УДК 341.17:342.7:004.056.5

Олексій ТЕРЛЮК
фізична особа-підприємець,
доктор філософії за спеціальністю 081 «Право»
oleeksiy2807@gmail.com
ORCID: 0000-0003-4594-0517

Іван ТЕРЛЮК
Львівський національний університет ветеринарної
медицини та біотехнологій ім. С.З. Ґжицького,
професор кафедри права,
доктор юридичних наук, професор
i.terlyuk2406@gmail.com
ORCID: 0000-0002-0900-4388

БЛОКЧЕЙН, АВТОМАТИЗАЦІЯ Й ОСНОВОПОЛОЖНІ ПРАВА: ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КОНФІДЕНЦІЙНОСТІ ТА ПЕРСОНАЛЬНИХ ДАНИХ У ПРАВІ ЄВРОПЕЙСЬКОГО СОЮЗУ

http://doi.org/10.23939/law2025.48.461

Досліджується взаємодія новітніх цифрових технологій, зокрема блокчейну (Blockchain) та штучного інтелекту, з правом Європейського Союзу у сфері захисту персональних даних. У процесі дослідження застосовано методи юридичного аналізу норм права ЄС, порівняльного правознавства (зокрема у контексті практики Ради Європи та інших юрисдикцій). Акцентовано увагу на правових та етичних викликах, що виникають у зв’язку із незворотністю блокчейн-записів, відсутністю централізованого контролера та використанням автоматизованих рішень без людського втручання. Розглянуто, наскільки чинне регулювання, зокрема Загальний регламент про захист даних (GDPR) та Регламент про штучний інтелект (AI Act), забезпечують реалізацію основоположного права на конфіденційність в умовах цифрової трансформації. На основі аналізу рішень Суду ЄС, позицій EDPB і практики національних органів обґрунтовано потребу в адаптації правових механізмів до особливостей децентралізованих і високоризикових систем. Запропоновано шляхи удосконалення правового регулювання через поєднання технологічних і нормативних рішень, зокрема впровадження концепцій «Privacy by Design» і міждисциплінарного етичного комплаєнсу − системи заходів, правил та процедур, спрямованих на забезпечення відповідності діяльності організації вимогам встановлених правил і норм. Зроблено висновок про необхідність переосмислення цифрових прав людини як комплексної категорії, що охоплює не лише юридичні гарантії, але й демократичний контроль над алгоритмами та прозорість технологій. При цьому наголошено, що у центрі цифрового правопорядку має залишатися людина як носій прав і автономної гідності, а не лише об’єкт обробки даних.

Ключові слова: право Європейського Союзу, GDPR, конфіденційність, персональні дані, блокчейн, штучний інтелект, автоматизоване рішення, цифрові права людини, децентралізовані технології, AI Act.

Постановка проблеми. Проблема захисту конфіденційності та персональних даних в сучасних умовах майже суцільної цифровізації суспільних відносин набуває особливої актуальності. Це зумовлено щонайменше одним ключовим фактором − стрімким розвитком цифрових технологій XXI століття. Зокрема, технології блокчейн (Blockchain) і штучного інтелекту не лише радикально трансформували способи обробки, зберігання й передачі персональних даних, але й змінили саму парадигму конфіденційності в цифровому середовищі. Децентралізовані реєстри, автоматизоване прийняття рішень, алгоритмічне профілювання особи − усе це ставить під сумнів ефективність традиційних правових механізмів захисту приватності, сформованих у межах правового поля Європейського Союзу. Відтак, за таких умов постає необхідність проаналізувати, наскільки чинне право Європейського Союзу здатне забезпечити ефективний і водночас етично вмотивований захист персональних даних в умовах автоматизації та децентралізації. Особливе значення у цьому контексті має встановлення відповідності чинного нормативного регулювання викликам, зумовленим незворотністю записів у блокчейн-системах, непрозорістю алгоритмічного прийняття рішень та відсутністю чіткого суб'єкта відповідальності (контролера) в розподілених цифрових мережах.

У вищезазначеному контексті дослідження особливостей забезпечення захисту конфіденційності у праві Європейського Союзу відповідає актуальним викликам сучасного цифрового правопорядку, а також має безпосереднє практичне значення для країн, які прагнуть нормативного зближення з правом ЄС, зокрема України. Аналіз здатності права Європейського Союзу адаптуватися до новітніх технологічних трансформацій і водночас зберігати баланс між інноваціями та захистом прав людини створює підґрунтя для подальшого вдосконалення політики цифрової конфіденційності на національному рівні. Водночас це відкриває перспективу для міждисциплінарного діалогу між правом, технологіями та етикою в умовах поступового переформатування публічного простору в цифрову площину.

Аналіз дослідження проблеми. Порушена в заголовку проблема викликає значний інтерес у зарубіжній та українській юридичній, а також міждисциплінарній науці. Насамперед йдеться про взаємодію цифрових технологій − зокрема блокчейну та штучного інтелекту − з правом на конфіденційність і персональні дані.

У зарубіжній доктрині вже з 2017–2018 рр. активно досліджуються конфлікти між незмінністю блокчейн-реєстрів і правами суб'єкта даних. На наш погляд, однією із знакових праць, що ґрунтовно розглядає цю проблематику, є монографія ***Blockchain and the Law: The Rule of Code*** (2018) французьких дослідників Прімавери де Філіппі та Аарона Райта, опублікована у видавництві Гарвардського університету [див.: 1]. Це дослідження, що доступне у відкритому доступі, пропонує широку концептуалізацію блокчейну як нової нормативної інфраструктури, що кидає виклик усталеним правовим моделям.

Для цілісного осягнення проблематики для нас важливим виявився «Посібник з європейського права у сфері захисту персональних даних» (2018), підготовлений під егідою низки дотичних європейських інституцій з метою надання допомоги практикам, які не спеціалізуються у сфері захисту персональних даних, включаючи адвокатів, суддів та представників інших юридичних професій [2]. Серед найновіших українських праць, присвячених зазначеній тематиці, привертають увагу статті О. Гиляки [3, с. 15–30] та Л. Тарасенка [4, с. 123–133]. Перша зосереджена на особливостях захисту персональних даних у цифровому середовищі, друга − на правовому аналізі феномену цифрових прав. Окремі аспекти цієї проблематики вже порушувалися в наукових публікаціях авторів, зокрема в контексті аналізу правових викликів і наслідків для публічного управління в умовах інформаційного суспільства [5, с. 258–265], а також одним із нас − у межах дослідження правового регулювання блокчейн-технології [див.: 6].

Водночас, фундаментом цього дослідження є чинна нормативно-правова база Європейського Союзу. Усі необхідні для аналізу документи − зокрема регламенти, директиви, рішення, керівні принципи та судову практику − було отримано через офіційний портал ЄС ***EUR-Lex − Access to European Union Law***, який забезпечує зручний доступ до актуального правового масиву ЄС, хоча ці

матеріали доступні й на інших офіційних ресурсах. Вказаний портал забезпечує відкритий доступ до: нормативних актів (регламентів, директив, рішень), документів інституцій (Європейської комісії, Ради ЄС, Європейського парламенту), судової практики Суду ЄС (CJEU), матеріалів публічних консультацій, «білих» і «зелених» книг, підготовчих документів (COM, SWD тощо). Зручна система пошуку за ключовими словами, датами, тематиками та типами документів дозволяє здійснювати повноцінний і цілеспрямований аналіз джерел [див.: 7].

Мета статті − окреслити сучасне законодавство Європейського Союзу у сфері захисту конфіденційності та персональних даних і здійснити комплексний аналіз його здатності реагувати на виклики, зумовлені впровадженням новітніх цифрових технологій, зокрема блокчейн-платформ та систем штучного інтелекту. У цьому контексті досліджується: (1) нормативне закріплення основоположного права на захист персональних даних у праві ЄС; (2) суперечності між технологією блокчейн та вимогами GDPR, включно з правом на забуття і визначенням відповідального суб'єкта; (3) правові та етичні дилеми, пов'язані з автоматизованим прийняттям рішень і використанням алгоритмів штучного інтелекту; (4) інституційна архітектура та практика правозастосування у сфері захисту даних, зокрема роль CJEU, EDPB та національних органів нагляду; (5) перспективи подальшої адаптації правового регулювання до умов децентралізації, автоматизації та високотехнологічної трансформації цифрового середовища.

Виклад основного матеріалу. Першим міжнародним юридично зобов'язальним документом у Європі, який стосувався виключно питань захисту персональних даних була *Конвенція Ради Європи* від 28 січня 1981 р. № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» [8]. У праві Європейського Союзу першим документом, який регулював захист персональних даних, стала *Директива про захист персональних даних* 1995 року [9]. Однак статусу окремого й самостійного основоположного права у Європейському Союзі право на захист персональних даних набуло щойно на початку XXI ст. з прийняттям *Хартії основних прав Європейського Союзу* (2000). У ст. 8 останньої [див.: 10], а також у статті 16 *Договору про функціонування ЄС* (ДФЄС) чітко закріплено нормативне підґрунтя права захисту конфіденційності та персональних даних [див.: 11]. Згідно з цими нормами, кожна особа має право на захист своїх персональних даних, а їхнє збирання, зберігання та обробка має здійснюватися відповідно до чітко визначених принципів, включаючи законність, справедливість, прозорість, обмеження мети та мінімізацію даних.

Директива про захист персональних даних (1995) втратила чинність під впливом швидких технологічних змін 2000-х. З метою адаптування правил захисту персональних даних до ери цифрових технологій Європейський Союз у 2016 році прийняв *Загальний регламент про захист даних* (GDPR, Регламент (ЄС) 2016/679. Набувши чинності 2018 року цей документ став головним інструментом реалізації цих прав у правозастосовній площині) [див.: 12]. Він створив у межах ЄС уніфіковану систему захисту персональних даних та передбачив конкретні зобов'язання як для приватних, так і для публічних суб'єктів, які обробляють такі дані.

Передовсім, ст. 5 GDPR встановлює низку фундаментальних принципів обробки персональних даних, зокрема: законність, справедливість і прозорість обробки; обмеження мети – обробка лише з чітко визначеною метою; мінімізація даних − збір лише необхідного мінімуму; точність – актуальність і точність даних; обмеження зберігання − зберігання лише протягом необхідного періоду; цілісність і конфіденційність − технічний і організаційний захист; підзвітність − обов'язок доводити дотримання усіх принципів.

Окрему увагу приділено *правам суб'єкта даних* (тут і далі курсив наш – *Авт.*), серед яких: право на доступ, виправлення, обмеження обробки, заперечення проти автоматизованого прийняття рішень, т. зв. *право на забуття* − багатогранне поняття, вперше закріплене у ЄС в травні 2014 р. (ст. 17 GDPR), що дозволяє людині вимагати за певних умов видалення своїх особових даних із загального доступу через пошукові системи, тобто посилань на ті дані, які, на її думку, можуть завдати їй шкоди, а також право на перенесення даних (ст. 20). Ці права особливо важливі в умовах цифрових трансформацій, де дані обробляються без прямого втручання людини.

Ключову роль у тлумаченні обсягу і змісту прав суб'єктів даних відіграє Суд Європейського Союзу. Уперше Суд ЄС визнав право особи на видалення даних з результатів пошуку у справі ***Google Spain SL v. Agencia Española de Protección de Datos*** (C-131/12) [13]. Тим самим фактично закріпив *«право на забуття»* в європейському правопорядку. У подальшому, в рішеннях ***Schrems I*** (C-362/14) [14] та ***Schrems II*** (C-311/18) [15], Суд розширив розуміння прав на конфіденційність, поставивши під сумнів законність передачі персональних даних у треті країни за відсутності адекватних гарантій.

Та попри фактичне сформування правом ЄС юридично зобов'язального та унікального у світовому вимірі наднаціонального стандарту захисту даних, сьогодні виникає потреба у його перегляді або уточненні деяких ключових понять − зокрема, контролера, мети обробки, принципу «data minimisation» та можливості реалізації права на забуття. А головна причина цього − інтенсивний розвиток децентралізованих систем з обмеженою керованістю (як-от блокчейн) і автоматизованого прийняття рішень (ШІ).

Технологія блокчейн, як складова частина децентралізованих систем обробки інформації, демонструє значний потенціал для підвищення прозорості, безпеки та достовірності цифрових транзакцій. Водночас такі її фундаментальні технічні характеристики як *незмінність* (immutability), *розподіленість* (distributed architecture) та *відсутність єдиного контролера* [див. докл.: 6, с. 53-61], вступають у пряму або опосередковану суперечність із низкою вимог *Загального регламенту про захист даних* (GDPR). Суть цього конфлікту зводиться до необхідності вирішення трьох ключових проблем: визначення статусу контролера в децентралізованому середовищі, незмінності записів у поєднанні з правом на забуття, а також кваліфікації персональних даних у контексті блокчейн-мереж.

GDPR виходить із припущення про існування чіткого суб'єкта, який визначає мету та засоби обробки персональних даних − т. зв. *контролера* (controller) (ст. 4(7) GDPR) [12]. Однак у випадку публічних блокчейн-мереж (наприклад, Bitcoin або Ethereum) відсутній єдиний орган чи особа, яка б відповідала цим критеріям. На практиці це ускладнює, а в деяких випадках унеможливлює визначення контролера в розумінні GDPR. У приватних або консорціумних блокчейнах ця проблема частково вирішується завдяки фіксації відповідальності між учасниками мережі, однак навіть тоді залишаються відкритими питання спільної відповідальності та рівня контролю [1, pp. 33-58]. У своїх *поясненнях* з цього приводу (Opinion 05/2014, Opinion 4/2019) *Європейська рада з питань захисту даних* (EDPB) зазначає, що у децентралізованих системах критерієм для визначення контролера може виступати фактичний вплив на обробку даних, навіть за відсутності централізованого оператора [16].

Одним із ключових принципів GDPR є право на стирання персональних даних (ст. 17), також відоме як *право на забуття*. Воно перебуває в прямій суперечності з технічною природою блокчейну, адже дані, один раз внесені до реєстру, не підлягають зміні або видаленню. Це ставить під сумнів можливість практичної реалізації згаданого права. Серед можливих рішень цієї проблеми: зберігання лише хешів або псевдонімізованих даних у блокчейні, а самих персональних даних − поза мережею (off-chain); використання «приватних ланцюгів» із контрольованим доступом і можливістю редагування або стирання; застосування криптографічних методів, які дозволяють зробити дані недоступними, наприклад, шляхом знищення ключа шифрування. Втім, навіть такі підходи не гарантують повної відповідності принципам GDPR, зокрема щодо прозорості, контролю з боку суб'єкта даних і пропорційності обробки [1, pp. 33-58].

GDPR також широко тлумачить поняття «персональні дані» як будь-яку інформацію, що прямо або опосередковано дозволяє ідентифікувати фізичну особу. У блокчейн-контексті це можуть бути навіть псевдонімізовані елементи - хеші транзакцій, криптогаманці, токени тощо − якщо їх можна зіставити з конкретною особою. Оскільки транзакції в публічних блокчейн-мережах є відкритими та доступними для аналізу, зберігається високий ризик повторної ідентифікації користувача [1, pp. 33-58]. Це, у свою чергу, підвищує вимоги до захисту конфіденційності та дотримання принципів права на приватність.

Так само суттєво ускладнює реалізацію гарантій, передбачених правом Європейського Союзу у сфері конфіденційності, стрімка інтеграція систем штучного інтелекту в процеси обробки персональних даних. Особливо гострими є етичні, правові та практичні виклики, пов'язані із застосуванням алгоритмів

машинного навчання, прогнозування ризиків, оцінки поведінки особи чи прийняття рішень без безпосередньої участі людини. Один із ключових механізмів захисту прав суб'єктів персональних даних у такому контексті міститься у статті 22 *Загального регламенту про захист даних* (GDPR), яка забороняє піддавати особу виключно автоматизованому прийняттю рішень, що тягне за собою правові наслідки або має істотний вплив на її становище. Винятки з цього правила дозволяються лише за дотримання конкретних умов, зокрема за наявності явної згоди суб'єкта даних, необхідності для виконання договору або у разі спеціального передбачення в законодавстві ЄС чи держав-членів із відповідними гарантіями [12].

Попри це, у практиці приватного та публічного секторів автоматизовані рішення поширюються швидше, ніж розвивається правове регулювання. Прикладами є використання алгоритмів у кредитному скорингу, онлайн-рекрутингу чи навіть у сфері розподілу соціальних послуг. При цьому одним із центральних викликів залишається ефект «чорної скриньки», або непрозорість логіки алгоритмічного прийняття рішень. Хоча стаття 15(1)(h) GDPR гарантує право суб'єкта даних на отримання інформації про логіку прийняття рішення, у випадку застосування глибоких нейронних мереж така логіка часто є або технічно незрозумілою, або захищеною як комерційна таємниця [12]. Вважаємо, що це істотно обмежує реалізацію принципу прозорості, закріпленого у статті 5(1)(a) GDPR, і знижує ефективність права на оскарження автоматизованого рішення, передбаченого статтею 22(3).

У сфері етики ШІ право ЄС поки що спирається переважно на акти «м'якого права» (soft law). Зокрема, в опублікованих у 2019 році «Етичних настановах щодо надійного ШІ» (Ethics Guidelines for Trustworthy AI), розроблених Європейською комісією, було запропоновано сім основоположних принципів етичного використання таких систем: людський контроль, технічна надійність, конфіденційність та управління даними, прозорість, недискримінація та справедливість, соціальне благополуччя і підзвітність [17]. Хоча ці принципи не є обов'язковими, вони стали підґрунтям для прийняття повноцінного нормативного акта − *Регламенту ЄС про штучний інтелект* (AI Act), ухваленого у 2024 році (Regulation (EU) 2024/1689) [18]. Цей документ запроваджує рівневу модель регулювання, що передбачає різні вимоги до систем ШІ залежно від ступеня ризику, і встановлює окремі стандарти для високоризикових систем, які обробляють біометричні та персональні дані.

Нарешті, важливо враховувати, що автоматизовані рішення можуть відтворювати або навіть посилювати дискримінаційні практики, якщо тренувальні дані систем ШІ містять упередженість або відображають соціальну нерівність. Це безпосередньо зачіпає права людини, включно з правом на гідність, рівність та недискримінацію, що гарантуються статтею 21 *Хартії основних прав Європейського Союзу* [див.: 10]. Водночас суб'єкти даних у багатьох випадках не мають реального контролю над тим, як саме використовуються їхні дані та як ці дані впливають на їхнє соціальне становище, що становить серйозний виклик як у контексті забезпечення інформованої згоди, так і з точки зору гарантування інформаційної автономії особи в цифрову епоху.

Водночас слід зважати на те, що ефективна реалізація прав суб'єктів персональних даних у Європейському Союзі залежить не лише від змісту правових норм, а й від здатності інституцій забезпечувати їх належне застосування. У сфері цифрової конфіденційності та етики критично важливим є наявність дієвого інституційного механізму контролю, координації та забезпечення відповідальності. Одним із центральних органів у цій сфері виступає *Європейська рада з питань захисту даних* (European Data Protection Board, EDPB) − незалежна структура, створена відповідно до статті 68 GDPR. До її складу входять представники національних органів із захисту даних та *Європейського наглядового органу з питань захисту даних* (European Data Protection Supervisor, EDPS). EDPB виконує важливі консультативно-координаційні функції: роз'яснює положення GDPR (зокрема щодо ролі контролера в децентралізованих системах), ухвалює керівні настанови (наприклад, Guidelines 05/2020 on consent), координує розгляд транскордонних справ, а також формулює рекомендації щодо новітніх технологій, таких як блокчейн, штучний інтелект та великі дані [19].

Поряд із EDPB вагому роль відіграють *національні органи захисту даних* (Data Protection Authorities, DPA), які функціонують у кожній державі-члені ЄС. Вони є незалежними наглядовими органами, уповноваженими здійснювати розслідування, розглядати скарги, видавати приписи про

припинення порушень та накладати адміністративні штрафи. GDPR (ст. 83) надає таким органам можливість накладати значні санкції − до 20 мільйонів євро або до 4 % від загального світового річного обороту компанії. Одним із прикладів ефективного правозастосування стало рішення DPA Ірландії у справі проти Meta Platforms Ireland Ltd (2023), коли компанію було оштрафовано на понад 1,2 мільярда євро за незаконну передачу персональних даних до США - на підставі висновків CJEU у справі Schrems II [15].

Ключову роль у забезпеченні єдності тлумачення й застосування положень GDPR відіграє *Суд Європейського Союзу* (Court of Justice of the European Union, CJEU). Через механізм попереднього запиту (ст. 267 ДФЄС) національні суди звертаються до CJEU для тлумачення норм Регламенту, що гарантує узгодженість у межах усіх держав-членів. Серед ключових рішень CJEU у сфері цифрової конфіденційності слід виокремити вже вище згадувані: справу ***Google Spain SL v. AEPD*** (C-131/12) [13], яка вперше визнала право на забуття; справи ***Schrems I*** (C-362/14) [14] і ***Schrems II*** (C-311/18) [15], у яких було скасовано механізми передачі даних до США через їх невідповідність стандартам захисту. А також: ***La Quadrature du Net*** (C-511/18), що визначила обмеження на масове зберігання даних з мотивів національної безпеки [20]; ***Digital Rights Ireland*** (C-293/12), у якій було визнано недійсною директиву про зберігання даних як таку, що суперечить основоположним правам [21].

У системі забезпечення правової відповідності важливу функцію виконує також інститут *Європейського омбудсмана*, який контролює дотримання прав людини у діяльності органів ЄС, зокрема у сфері застосування автоматизованих рішень у публічному управлінні. До прикладу, 2020 року Європейський омбудсман ініціював розслідування щодо використання систем штучного інтелекту в адміністративній практиці Європейської комісії (SI/4/2024/MIK), акцентуючи на необхідності прозорості алгоритмів та забезпечення їх аудитованості [22].

Зростає також роль Європейського агентства з кібербезпеки (ENISA), яке розробляє рекомендації щодо забезпечення безпеки персональних даних у цифровому середовищі, протидії кіберзагрозам і впровадження етичних стандартів у сфері кіберзахисту [див.: 23]. У сукупності всі ці органи формують інституційну архітектуру, здатну забезпечувати як належне впровадження норм, так і гнучку адаптацію до технологічного прогресу.

У світлі викликів, які створюють децентралізовані технології, автоматизовані рішення та алгоритмічна обробка даних, стає очевидним, що наявна нормативна база ЄС − попри її прогресивність − не вичерпує всіх аспектів цифрової етики та правового забезпечення конфіденційності. Необхідною є подальша адаптація підходів, які поєднували б стабільність правових стандартів із технологічною гнучкістю та міждисциплінарною чутливістю до новітніх викликів.

Передусім такої адаптації потребує регулювання децентралізованих технологій. *Загальний регламент про захист даних* (GDPR) наразі не охоплює повною мірою особливості функціонування блокчейну, Web3-інфраструктур та розподілених цифрових середовищ. У зв'язку з цим на рівні *Європейської ради з питань захисту даних* (EDPB), а також у дослідницьких спільнотах тривають обговорення необхідності запровадження спеціального регулювання, яке б передбачало оновлені визначення понять «контролер» і «процесор» у мережах без централізованого управління, формалізацію статусу «співконтролерів» у консорціумних блокчейнах, а також моделі захисту прав суб'єктів даних в умовах незмінності блокчейн-записів (наприклад, через off-chain зберігання або криптографічну псевдонімізацію) [19].

Другим напрямом є гармонізація положень GDPR із *Регламентом про штучний інтелект* (AI Act), ухваленим у 2024 році. Цей документ запроваджує нову регуляторну архітектуру, зосереджену на оцінці ризиків, контролі за високоризиковими системами ШІ та забезпеченні прозорості, що лише частково перетинається з положеннями GDPR про захист персональних даних. На стику цих двох нормативних масивів виникають як питання узгодження механізмів інформованої згоди, так і потенційні дублювання або прогалини в системі відповідальності [2, с. 379-389]. У перспективі доцільним видається формування єдиного нормативного комплексу − умовного «*Кодексу цифрових прав*» (Digital Rights Code), що охоплював би конфіденційність, алгоритмічну етику, права користувачів, відповідальність цифрових платформ і захист від дискримінаційних практик.

Важливим інструментом оновлення підходів є впровадження техніко-правових концепцій Privacy by Design і Privacy by Default, закріплених у статті 25 GDPR [12]. Хоча ці принципи задекларовано, їх практична імплементація здебільшого залишається фрагментарною. Пріоритетними завданнями тут є створення механізмів етичного комплаєнсу, запровадження обов'язкових аудитів алгоритмічних систем, розбудова регуляторних пісочниць (regulatory sandboxes) у взаємодії з наглядовими органами, а також включення принципів цифрової етики у професійні стандарти фахівців у сфері IT, права і технологій.

Окремого значення набуває посилення освітньо-наукової взаємодії. Формування нормативної цифрової культури неможливе без залучення академічної спільноти, розвиток якої має спиратися на міждисциплінарні освітні програми, поєднуючи право, етику, інформаційні технології та філософію [1, pp. 205-210]. Перспективними формами такої взаємодії можуть бути розвиток юридичних клінік із цифрових прав людини, створення постійних наукових консорціумів для підготовки рекомендацій до інституцій ЄС (на кшталт Reclaim Your Face чи MyData Europe), а також посилення участі молодих дослідників у формуванні політики відкритих даних, штучного інтелекту та цифрової справедливості.

Висновки. Підсумуємо вищевикладене декількома пунктами.

1. Право ЄС сформувало наднаціональний стандарт захисту даних, який є юридично зобов'язальним та унікальним у світовому вимірі. Проте з розвитком децентралізованих систем з обмеженою керованістю (як-от блокчейн) і автоматизованого прийняття рішень (ШІ) виникає потреба у перегляді або уточненні деяких ключових понять – зокрема, контролера, мети обробки, принципу «data minimisation» та можливості реалізації *права на забуття*.

2. Технологія блокчейн відкриває нові можливості у сфері цифрової трансформації, але водночас створює системні виклики для реалізації прав суб'єктів даних, які гарантує право ЄС. Поки що GDPR не містить спеціальних положень, що враховують особливості децентралізованих мереж, і вирішення конфліктів часто покладається на інтерпретації та практичні рекомендації органів нагляду. У перспективі необхідним є розроблення техніко-правових рішень, які поєднають інновації з вимогами прав людини.

3. Регулювання автоматизованих систем в ЄС перебуває на перехідному етапі: з одного боку – жорсткі вимоги GDPR, з іншого – гнучкі підходи AI Act. Проблема полягає в тому, що алгоритмічна обробка персональних даних відбувається швидше, ніж розвивається судова та нормативна практика. Етичні рамки, хоч і проголошені, часто не мають обов'язкової сили, а отже, право суб'єкта даних на автономію, інформованість і контроль не завжди реалізоване повною мірою.

4. Інституційна система ЄС загалом забезпечує високий рівень правозастосування у сфері захисту даних, хоча потребує вирішення проблема забезпечення технічної адекватності та оперативного реагування на інноваційні виклики. Водночас розрив між регуляторною спроможністю та темпами розвитку цифрових технологій вимагає зміцнення співпраці між органами нагляду, впровадження інноваційного комплаєнсу та активної участі академічної спільноти у формуванні техніко-правових стандартів.

5. Правове регулювання в ЄС стоїть на порозі нового етапу: від реактивного реагування до проактивного супроводу технологічних змін. Для цього потрібні не лише нові норми, але й нові інститути, механізми комунікації та розуміння етики як невід'ємної частини правового ландшафту. Відтак, подальша адаптація права ЄС повинна охоплювати такі напрями як: розроблення спеціалізованих норм для децентралізованих технологій; інтеграцію принципів етичного комплаєнсу в цифрову економіку; узгодження між GDPR та AI Act; посилення міждисциплінарної співпраці на рівні освіти, науки та політики. Але при цьому, основним орієнтиром змін права у цій сфері має залишатися людина – її гідність, автономія й право на контроль над особистою інформацією в цифрову добу.

Подяки. Немає.

Фінансування. Автори заявляють про відсутність фінансової підтримки для проведення досліджень, написання або публікації цієї статті.

Внесок авторів: Терлюк Олексій – 50 %, Терлюк Іван – 50 %. Автори схвалюють цю роботу і беруть на себе відповідальність за її цілісність.

Конфлікт інтересів. Автори заявляють про відсутність конфлікту інтересів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. De Filippi, P., Wright, A. (2018). Blockchain and the Law: The Rule of Code. Harvard University Press. 312 p. DOI: https://doi.org/10.2307/j.ctv2867sp (Дата звернення: 12.07.2025)
2. Посібник з європейського права у сфері захисту персональних даних. Видання 2018 року / Агенція Європейського Союзу з питань основоположних прав; Рада Європи; Європейський Суд з прав людини; Європейський інспектор із захисту персональних даних. Б.м., 2018, 432 с.
3. Гиляка О. (2023). Право на приватність та захист персональних даних в умовах цифровізації. *Вісник Національної академії правових наук України*. Том 30. № 1. С. 15-30.
4. Тарасенко Л. (2024). Цифрові права: правова природа та еволюція. *Вісник Львівського університету. Серія юридична*. Випуск 79. С. 123–133.
5. Терлюк О., Терлюк І. (2025) Розвиток інформаційного суспільства: правові наслідки та виклики для публічного управління. *Вісник Національного університету «Львівська політехніка». Серія: "Юридичні науки"* . Том. 12, № 1 (45), С. 258-265. DOI: https://doi.org/10.23939/law2025.45.258
6. Терлюк Олексій (2024). Правове регулювання блокчейн-технології у публічному управлінні: аспекти міжнародного та українського досвіду використання. [Монографія]. Львів: Растр-7, 260 с.
7. EUR-Lex – Access to European Union Law (Доступ до законодавства Європейського Союзу). URL: https://eur-lex.europa.eu/homepage.html (Дата звернення: 15.07.2025)
8. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981. URL: http://zakon4.rada.gov.ua/laws/show/994_326 (Дата звернення: 01.07.2025)
9. Директива 95/46/ЄС Європейського парламенту і Ради про захист осіб у зв'язку з обробкою персональних даних і вільним обігом цих даних від 24.10.1995. URL: https://zakon.rada.gov.ua/laws/show/994_242 (Дата звернення: 01.07.2025)
10. Хартія основних прав Європейського Союзу. (2007/C 303/01). URL: https://eur-lex.europa.eu/eli/treaty/char_2007/oj (Дата звернення: 09.12.2024)
11. Договір про функціонування Європейського Союзу (консолідована версія 2016 року). URL: https://eur-lex.europa.eu/collection/eu-law/treaties/treaties-force.html#new-2-52 (Дата звернення: 08.03.2025)
12. Регламент Ради ЄС 2016/679 про захист фізичних осіб щодо обробки персональних даних та про вільний рух таких даних, а також про скасування Директиви 95/46/ЕС (Загальний регламент захисту даних) від 27.04.2016. URL: https://eur-lex.europa.eu/ legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN (Дата звернення: 02.07.2025)
13. Google Spain SL, Google Inc.v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González. Judgment of the Court (Grand Chamber) of 13 May 2014. URL: https:// eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0131&from=EN (Дата звернення: 13.07.2025)
14. Рішення Суду ЄС у справі Шремс I. URL: https://www.datawo.org/schrems-i/ (Дата звернення: 13.07.2025)
15. Шремс II: короткий зміст – все, що вам потрібно знати. URL: https://www.gdprsummary.com/schrems-ii/ (Дата звернення: 13.07.2025)
16. Європейській комісії пояснили блокчейн та розподілену логістику згідно з GDPR. 4 червня 2019 р. Сільван Йонгеріус. URL: https://techgdpr.com/blog/blockchain-dlt-under-the-gdpr-explained-to-the-european-commission/ (Дата звернення: 01.07.2025)
17. Ethics Guidelines for Trustworthy AI. URL: https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1 (Дата звернення 10.07.2025)
18. Регламент (ЄС) 2024/1689 Європейського Парламенту та Ради від 13 червня 2024 року, що встановлює гармонізовані правила щодо штучного інтелекту […]. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (Дата звернення: 05.07.2025)

19. European Data Protection Board, EDPB. URL: https://www.edpb.europa.eu/edpb_en (Дата звернення: 05.07.2025)

20. Суд ЄС - C-511/18 - La Quadrature du Net та інші. URL: https://gdprhub.eu/index.php?title=CJEU_-_C-511/18_-_La_Quadrature_du_Net_and_Others (Дата звернення: 01.07.2025)

21. Plenty to retain? Opinion of the Advocate General in Joined Cases C-293/12 and 594/12, Digital Rights Ireland ltd and Seitlinger and others by Orla Lynskey. URL: https://www.europeanlawblog.eu/pub/plenty-to-retain-opinion-of-the-advocate-general-in-joined-cases-c-29312-and-59412-digital-rights-ireland-ltd-and-seitlinger-and-others/release/1 (Last accessed 02.07.2025)

22. Як Європейська комісія приймає рішення щодо штучного інтелекту та використовує його. URL: https://www.ombudsman.europa.eu/en/case/en/65545 (Дата звернення: 01.07.2025)

23. Європейське агентство з кібербезпеки (ENISA). URL: https://www.enisa.europa.eu/ (Дата звернення: 02.07.2025)

REFERENCES

1. De Filippi, P., Wright, A. (2018). ***Blockchain and the Law: The Rule of Code.*** Harvard University Press. 312 r. DOI: https://doi.org/10.2307/j.ctv2867sp (Accessed: 12.07.2025)

2. ***Posibnyk z yevropeiskoho prava u sferi zakhystu personalnykh danykh***. Vydannia 2018 roku / Ahentsiia Yevropeiskoho Soiuzu z pytan osnovopolozhnykh prav; Rada Yevropy; Yevropeiskyi Sud z prav liudyny; Yevropeiskyi inspektor iz zakhystu personalnykh danykh. B.m., 2018, 432 p. [In Ukrainian].

3. Hyliaka O. (2023). ***Pravo na pryvatnist ta zakhyst personalnykh danykh v umovakh tsyfrovizatsii***. Visnyk Natsionalnoi akademii pravovykh nauk Ukrainy. Tom 30. № 1. P. 15-30. [In Ukrainian].

4. Tarasenko L. (2024). ***Tsyfrovi prava: pravova pryroda ta evoliutsiia***. Visnyk Lvivskoho universytetu. Seriia yurydychna. Vypusk 79. P. 123–133. [In Ukrainian].

5. Terliuk O., Terliuk I. (2025) ***Rozvytok informatsiinoho suspilstva: pravovi naslidky ta vyklyky dlia publichnoho upravlinnia.*** Visnyk Natsionalnoho universytetu «Lvivska politekhnika». Seriia: "Iurydychni nauky" . Tom. 12, № 1 (45), P. 258-265. DOI: https://doi.org/10.23939/law2025.45.258 [In Ukrainian].

6. Terliuk Oleksii (2024). ***Pravove rehuliuvannia blokchein-tekhnolohii u publichnomu upravlinni: aspekty mizhnarodnoho ta ukrainskoho dosvidu vykorystannia***. [Monohrafiia]. Lviv: Rastr-7, 260 s. [In Ukrainian].

7. ***EUR-Lex*** – Access to European Union Law (Dostup do zakonodavstva Yevropeiskoho Soiuzu). Retrieved from: https://eur-lex.europa.eu/homepage.html (Accessed: 15.07.2025)

8. ***Konventsiia pro zakhyst osib u zviazku z avtomatyzovanoiu obrobkoiu personalnykh danykh*** vid 28.01.1981. Retrieved from: http://zakon4.rada.gov.ua/laws/show/994_326 (Accessed: 01.07.2025) [In Ukrainian].

9. ***Dyrektyva 95/46/IeS Yevropeiskoho parlamentu i Rady pro zakhyst osib u zviazku z obrobkoiu personalnykh danykh i vilnym obihom tsykh danykh*** vid 24.10.1995. Retrieved from: https://zakon.rada.gov.ua/laws/show/994_242 (Accessed: 01.07.2025) [In Ukrainian].

10. ***Khartiia osnovnykh prav Yevropeiskoho Soiuzu***. (2007/C 303/01). Retrieved from: https://eur-lex.europa.eu/eli/treaty/char_2007/oj (Accessed: 09.12.2024) [In Ukrainian].

11. ***Dohovir pro funktsionuvannia Yevropeiskoho Soiuzu*** (konsolidovana versiia 2016 roku). Retrieved from: https://eur-lex.europa.eu/collection/eu-law/treaties/treaties-force.html#new-2-52 (Accessed: 08.03.2025) [In Ukrainian].

12. ***Rehlament Rady YeS 2016/679 pro zakhyst fizychnykh osib shchodo obrobky personalnykh danykh ta pro vilnyi rukh takykh danykh, a takozh pro skasuvannia Dyrektyvy 95/46/EC*** (Zahalnyi rehlament zakhystu danykh) vid 27.04.2016. Retrieved from: https://eur-lex.europa.eu/ legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679& from=EN (Accessed: 02.07.2025) [In Ukrainian].

13. ***Google Spain SL, Google Inc.v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González. Judgment of the Court (Grand Chamber) of 13 May 2014***. Retrieved from: https:// eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0131&from=EN (Accessed: 13.07.2025)

14. ***Rishennia Sudu YeS u spravi Shrems I.*** Retrieved from: https://www.datawo.org/schrems-i/ (data zvernennia: 13.07.2025) [In Ukrainian].

15. ***Shrems II: korotkyi zmist – vse, shcho vam potribno znaty***. Retrieved from: https://www.gdprsummary.com/schrems-ii/ (Accessed: 13.07.2025) [In Ukrainian].

16. ***Ievropeiskii komisii poiasnyly blokchein ta rozpodilenu lohistyku zghidno z GDPR***. 4 chervnia 2019 r. Silvan Yonherius. Retrieved from: https://techgdpr.com/blog/blockchain-dlt-under-the-gdpr-explained-to-the-european-commission/ (Accessed: 01.07.2025) [In Ukrainian].

17. ***Ethics Guidelines for Trustworthy AI.*** Retrieved from: https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1 (Last accessed 10.07.2025)

18. ***Rehlament (IeS) 2024/1689 Yevropeiskoho Parlamentu ta Rady*** vid 13 chervnia 2024 roku, shcho vstanovliuie harmonizovani pravyla shchodo shtuchnoho intelektu […]. Retrieved from: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (Accessed: 05.07.2025) [In Ukrainian].

19. *European Data Protection Board,* EDPB. Retrieved from: https://www.edpb.europa.eu/edpb_en (Accessed: 05.07.2025)

20. ***Sud YeS*** - C-511/18 - La Quadrature du Net ta inshi. Retrieved from: https://gdprhub.eu/index.php?title=CJEU_-_C-511/18_-_La_Quadrature_du_Net_and_Others (Accessed: 01.07.2025) [In Ukrainian].

21. ***Plenty to retain?*** Opinion of the Advocate General in Joined Cases C-293/12 and 594/12, Digital Rights Ireland ltd and Seitlinger and others by Orla Lynskey. Retrieved from: https://www.europeanlawblog.eu/pub/plenty-to-retain-opinion-of-the-advocate-general-in-joined-cases-c-29312-and-59412-digital-rights-ireland-ltd-and-seitlinger-and-others/release/1 (Accessed: 02.07.2025)

22. ***Iak Yevropeiska komisiia pryimaie rishennia shchodo shtuchnoho intelektu ta vykorystovuie yoho.*** Retrieved from: https://www.ombudsman.europa.eu/en/case/en/65545 (Accessed: 01.07.2025) [In Ukrainian].

23. ***Ievropeiske ahentstvo z kiberbezpeky*** (ENISA). Retrieved from: https://www.enisa.europa.eu/ (Accessed: 02.07.2025) [In Ukrainian].

Отримано: 24.07.2025
Прорецензовано: 09.09.2025
Схвалено до друку: 29.09.2025
Опубліковано (онлайн): 12.12.2025
Надруковано: 26.12.2025

Oleksii TERLYUK
Doctor of Philosophy, specialty 081 "Law"
oleeksiy2807@gmail.com
ORCID: 0000-0003-4594-0517

Ivan TERLYUK
Lviv National University of Veterinary
Medicine and Biotechnology named after S.Z. Grzycki,
Professor of the Department of Law
Dr. habil (Law), Professor
i.terlyuk2406@gmail.com
ORCID: 0000-0002-0900-4388

BLOCKCHAIN, AUTOMATION AND FUNDAMENTAL RIGHTS: ENSURING THE PROTECTION OF PRIVACY AND PERSONAL DATA IN EUROPEAN UNION LAW

This article explores the interaction between emerging digital technologies − particularly blockchain and artificial intelligence − and European Union law in the field of personal data protection. The research applies methods of legal analysis of EU legal norms and comparative law (notably in the context of Council of Europe practices and other jurisdictions). Particular attention is paid to the legal and ethical challenges posed by the immutability of blockchain records, the absence of a centralized data

controller, and the use of automated decision-making without human involvement. The study assesses how current regulations − especially the General Data Protection Regulation (GDPR) and the Artificial Intelligence Act (AI Act) − enable the realization of the fundamental right to privacy in the context of digital transformation. Drawing on case law of the Court of Justice of the European Union (CJEU), positions of the European Data Protection Board (EDPB), and national supervisory practice, the article substantiates the need to adapt legal mechanisms to the specificities of decentralized and high-risk systems. It proposes ways to improve legal regulation through a combination of technological and normative tools, including the implementation of Privacy by Design principles and interdisciplinary ethical compliance (a system of measures, rules, and procedures aimed at ensuring that an organization's activities conform to established legal and ethical standards). The conclusion emphasizes the need to reconceptualize digital human rights as a complex category encompassing not only legal safeguards but also democratic oversight of algorithms and technological transparency. Ultimately, it is underscored that human beings − as bearers of rights and autonomous dignity − must remain at the center of the digital legal order, not merely as objects of data processing.

Keywords: European Union law, GDPR, privacy, personal data, blockchain, artificial intelligence, automated decision-making, digital human rights, decentralized technologies, AI Act.