УДК 347.4
DOI https://doi.org/10.32782/2524-0374/2024-5/84

РЕГУЛЮВАННЯ КОНФІДЕНЦІЙНОСТІ У ЕПОХУ БЛОКЧЕЙНУ: ПРАВОВІ АСПЕКТИ ТА ПЕРСПЕКТИВИ

PRIVACY REGULATION IN THE ERA OF BLOCKCHAIN: LEGAL ASPECTS AND PERSPECTIVES

Смірнов І.С., аспірант
Навчально-науковий інститут права Київського національного університету імені Тараса Шевченка

Стаття аналізує вплив технології блокчейн на правові аспекти конфіденційності, особливо зосереджуючись на взаємодії з Загальним регламентом захисту даних (GDPR). Розглядаються такі основні особливості блокчейну, як децентралізація та незмінність даних, та їх вплив на захист особистої інформації у цифровому просторі. Обговорюється актуальність адаптації чинних правових рамок до технологічних інновацій, необхідність розробки нових законодавчих норм та перспективи створення єдиних міжнародних стандартів.

Стаття зосереджує основну увагу на потенційних конфліктах, які виникають через незмінність даних, яку забезпечує блокчейн, та законодавство про конфіденційність, зокрема на «право на забуття», закріплене у GDPR. Розглядається складність цього питання, аналізується, як незмінний характер даних блокчейну може створювати виклики для видалення особистих даних, що є ключовим аспектом «права на забуття». Також висвітлюються можливості та виклики інтеграції блокчейну в правові системи та пропонуються підходи для гармонізації технологічних інновацій з вимогами конфіденційності.

Проводиться ретельний та детальний аналіз складних правових аспектів взаємодії блокчейну з GDPR, включно з складними питаннями, пов'язаними з юридичною силою та юрисдикцією блокчейн-рішень. Також детально аналізується роль держав у регулюванні цих технологій та вплив міжнародного законодавства на розвиток блокчейн-ініціатив.

Стаття наголошує, що блокчейн має потенціал радикально трансформувати підходи до конфіденційності та захисту даних. Однак також підкреслюється теперішня потреба у розробці детального правового механізму, який візьме до уваги специфіку цієї технології, для повної реалізації потенціалу блокчейну.

Ключові слова: блокчейн, конфіденційність, GDPR, правове регулювання, захист даних, технологічні інновації, міжнародні стандарти.

The article analyzes blockchain technology's impact on legal aspects of privacy, with a particular focus on its interaction with the General Data Protection Regulation (GDPR). It examines how blockchain's core features, such as decentralization and data immutability, influence personal information protection in the digital space. The relevance of adapting existing legal frameworks to technological innovations, the necessity of developing new regulations, and the prospects for creating unified international standards are discussed.

The article places primary attention on the potential conflicts that arise from the immutability provided by blockchain and privacy legislation, particularly the 'right to be forgotten' as enshrined in the GDPR. It delves into the complexities of this issue, discussing how the permanent nature of blockchain data can pose challenges to the erasure of personal data, a key aspect of the 'right to be forgotten'. The article also highlights the opportunities and challenges of integrating blockchain into legal systems and suggests approaches for harmonizing technological innovations with privacy requirements.

A meticulous and comprehensive analysis of the intricate legal aspects of blockchain's interaction with GDPR is conducted, including nuanced issues related to the legal strength and jurisdiction of blockchain solutions. The role of states in regulating these technologies and the impact of international legislation on the development of blockchain initiatives are also meticulously analyzed.

The article strongly emphasizes the belief that blockchain has the potential to radically transform approaches to privacy and data protection. However, it also underscores the urgent need for developing a comprehensive legal mechanism that takes into account the specifics of these technologies in order to fully realize these transformative potentials.

Key words: blockchain, privacy, GDPR, legal regulation, data protection, technological innovations, international standards.

Блокчейн-технології, здавалося б, перевернули уявлення про безпеку та прозорість у цифровому світі, вносячи кардинальні зміни у багато сфер людської діяльності, зокрема у захист інформації та обробку даних. Їхні особливості, такі як децентралізація, незмінність записів та високий ступінь криптографічного захисту, надають унікальні можливості для створення систем, де інформація захищена від зовнішніх втручань та фальсифікацій. Однак, разом із багатьма перевагами, блокчейн пропонує також і низку викликів для правових систем, особливо у контексті регулювання конфіденційності.

Ця тема є актуальною з огляду на потребу в адаптації законодавчих рамок до новітніх технологій. Зокрема, Загальний регламент захисту даних (GDPR) [1] в Європейському Союзі ставить перед блокчейн-технологіями нові виклики, такі як вимоги до «права на забуття», що можуть бути в антагонізмі до основних принципів блокчейну. Вивчення цих взаємодій є критично важливим для формування ефективного і справедливого правового середовища, яке б захищало права осіб і водночас розвивало технологічний прогрес.

Блокчейн, як технологія розподіленого реєстру, стала визначальним фактором у численних інноваційних рішеннях, змінюючи підходи до безпеки, прозорості та довіри у цифровому світі. Ця технологія забезпечує незмінність і відкритість даних без необхідності централізованого управління, що робить її ідеальною для реалізації заходів забезпечення конфіденційності та захисту персональних даних [2]. Проте, сама її структура викликає питання сумісності з такими правовими нормами, як GDPR, прийнятий Європейським Союзом.

Конфіденційність у сучасному розумінні тотожна персональним даним або відомостям про фізичну чи юридичну особу, якщо особа має бажання вважати таку інформацію конфіденційною [3]. Це право індивіда контролювати інформацію про себе та вирішувати, коли, як і в якому обсязі така інформація може бути розголошена або використана іншими особами. GDPR, як один із найбільш впливових правових актів у цій сфері, встановлює строгі вимоги до обробки персональних даних, включаючи право на забуття, яке може вступати у конфлікт з незмінністю даних у блокчейні.

Взаємодія блокчейну та законів про конфіденційність, особливо у контексті GDPR, вимагає глибокого аналізу потенційних конфліктів та розробки нових підходів для їх вирішення.

GDPR, який набув чинності у травні 2018 року, став основним документом, що регулює обробку персональних даних у Європейському Союзі. Основні принципи GDPR включають вимоги до прозорості, обмеження цілей обробки даних, мінімізацію даних, точність, обмеження зберігання, цілісність і конфіденційність. Однією з клю-

чових особливостей GDPR є право суб'єкта даних на «забуття», що передбачає можливість вимагати видалення своїх персональних даних з систем, що може суперечити незмінності даних у блокчейні.

Крім GDPR, країни по всьому світу розробляють власні закони, які визначають підходи до конфіденційності та захисту даних. У США, наприклад, не існує єдиного федерального закону, аналогічного GDPR; замість цього, є ряд законів штатів, таких як Закон Каліфорнії про конфіденційність споживачів (CCPA), який надає споживачам право знати, як їхні особисті дані збираються, обробляються та діляться [4, с. 123–169].

У Бразилії загальний закон про захист даних (LGPD) визначає правила обробки особистих даних у всіх секторах країни, вимагаючи від компаній впровадження жорстких заходів безпеки [5, с. 38–57]. У Південній Африці також існують суворі закони, які регулюють захист даних, аналогічно до GDPR [6, с. 58–74].

Застосування блокчейну варіюється в різних країнах залежно від локального законодавства. Наприклад, в Естонії блокчейн-технології активно використовуються урядом для забезпечення безпеки державних цифрових сервісів, зокрема, в системах охорони здоров'я та національних реєстрів. Це стало можливим завдяки прогресивному регулюванню, яке враховує технологічні особливості [7].

З іншого боку, у Китаї, де контроль за даними є суворішим, блокчейн використовується також активно, але переважно в державних проєктах, де уряд може гарантувати дотримання політик конфіденційності, що відповідають національному законодавству [8].

Однією з фундаментальних характеристик блокчейну є незмінність даних, що означає, що після додавання інформації до блокчейну, її не можна змінити або видалити. Ця особливість забезпечує високий рівень довіри та безпеки в мережі. Однак, це створює конфлікт з такими законами, як GDPR, де передбачено право на «забуття» або видалення особистих даних на вимогу суб'єкта. Цей конфлікт викликає необхідність розробки нових технологічних рішень, які б дозволяли блокчейн-мережам відповідати вимогам конфіденційності, наприклад, через механізми шифрування або створення приватних блокчейнів, де доступ до даних обмежений.

Блокчейн часто використовується для створення відкритих, децентралізованих баз даних, де інформація доступна всім учасникам мережі. Ця відкритість може вступати в конфлікт з правилами конфіденційності, які вимагають захисту особистих даних від непотрібного або неконтрольованого доступу. Це вимагає від розробників блокчейну інтеграції додаткових заходів безпеки, таких як псевдонімізація або анонімізація даних, щоб зберегти приватність, не втрачаючи при цьому переваг децентралізації [9, с. 1–34].

Розподілена природа блокчейну означає, що дані розподілені між безліччю користувачів по всьому світу, що може ускладнити визначення юрисдикції та застосування національних законів. Наприклад, якщо дані користувача з ЄС зберігаються на серверах, розташованих поза ЄС, це може порушувати GDPR, який вимагає, щоб експорт даних з ЄС контролювався та відповідав встановленим стандартам. Також, це ставить питання про відповідальність за захист даних та виконання вимог законодавства. Це може призвести до юридичних спорів та необхідності розробки міжнародних угод або стандартів для регулювання таких операцій.

Ці аспекти підкреслюють складність взаємодії між блокчейн-технологіями та чинними законами про конфіденційність. Вони вимагають додаткових досліджень, юридичної креативності та технологічних інновацій, щоб знайти баланс між інноваціями та правами на конфіденційність.

Для інтеграції блокчейну з законами про конфіденційність використовуються різні підходи, які допомагають збалансувати потреби в технологічних інноваціях та вимоги законодавства. Однією з ключових стратегій є застосування шифрування даних на блокчейні, що дозволяє виконувати обчислення над зашифрованими даними без необхідності їх розкриття. Це насамперед гомоморфне шифрування, яке підтримує виконання операцій над шифрованими даними, забезпечуючи їхню конфіденційність при обробці [10].

Також існує підхід федеративного навчання, який дозволяє кільком сторонам спільно тренувати модель машинного навчання без необхідності обміну власними даними. Це рішення використовується в розподілених системах, як Інтернет речей, де датчики та пристрої збирають велику кількість даних. Інтеграція федеративного навчання з блокчейном дозволяє забезпечувати приватність при тренуванні моделей, обмінюючись лише параметрами даних, а не самими даними [11, с. 203].

Ці методи вирішують деякі з юридичних та технічних викликів, пов'язаних із забезпеченням конфіденційності на блокчейні, але також вимагають глибокого розуміння як технологій, так і юридичних рамок, в яких вони застосовуються.

Для забезпечення конфіденційності у блокчейні розробники використовують ряд технологічних новацій, кожна з яких спрямована на подолання специфічних викликів, пов'язаних із захистом даних. Серед таких інновацій: зеро-знання докази (Zero-Knowledge Proofs, ZKP), кільцеві підписи (Ring Signatures), гомоморфне шифрування (Homomorphic Encryption), обчислення з багатосторонньою безпекою (Secure Multi-party Computation, SMPC) [10].

Зеро-знання докази – це метод, який дозволяє одній стороні довести іншій, що вона знає певну інформацію без необхідності розкривати саму цю інформацію. Це як показати, що ви знаєте секретний пароль, не кажучи сам пароль. У юридичному контексті, це може допомогти підтверджувати важливі угоди або права без розкриття конфіденційної інформації.

Кільцеві підписи працюють за принципом, що дозволяє виконати транзакцію, яка виглядає так, ніби вона могла бути здійснена будь-ким з групи людей, не розкриваючи, хто саме її здійснив. Це трохи схоже на голосування в бюлетені, де ваш голос є анонімним, але береться до уваги у загальному підрахунку.

Гомоморфне шифрування дозволяє проводити розрахунки на зашифрованих даних без необхідності їх дешифрування. Це можна порівняти з тим, як ви могли б платити в ресторані через закритий конверт, щоб ніхто не знав суму, але платіж був би точним.

Обчислення з багатосторонньою безпекою дозволяє кільком сторонам об'єднати свої дані для обчислень, не розкриваючи їх один одному. Це як якби кожен давав загадку, рішення якої могло б бути знайдено лише тоді, коли всі загадки були б зібрані разом, але без того, щоб кожен знав загадки інших.

Ці технології допомагають не лише захищати приватні дані в блокчейні, але й забезпечують дотримання юридичних норм щодо конфіденційності та захисту особистих даних.

Для вдосконалення регуляторного середовища в контексті застосування блокчейн-технологій, особливо в аспектах конфіденційності та захисту даних, необхідно розглядати два основні напрямки: розробка нових законопроєктів та адаптація чинних законів.

Розробка нових законопроєктів передбачає створення спеціалізованих нормативних актів, які безпосередньо визначають використання і стандарти блокчейну. Це може включати встановлення правил для операцій, здійснюваних за допомогою блокчейну, вимоги до безпеки та конфіденційності даних. Нові законопроєкти можуть також визначити процедури верифікації та валідації транзакцій

на блокчейн-платформах, а також законодавчі рамки для використання смарт-контрактів.

Адаптація чинних законів зосереджується на перегляді та модифікації законодавчих актів з метою їх актуалізації до новітніх технологій. Такий підхід може включати внесення змін до законів про захист персональних даних, цивільного права та законодавства про інтелектуальну власність, щоб забезпечити їхню сумісність з технологією блокчейн. Важливо, щоб такі зміни враховували особливості незмінності, децентралізації та прозорості блокчейну, щоб не обмежити його потенціал, але при цьому забезпечити належний захист користувачів і даних.

В обох випадках важливо забезпечити широке громадське обговорення та залучення всіх зацікавлених сторін: від розробників технологій і бізнесу до правових експертів і звичайних користувачів. Такий підхід дозволить створити збалансоване та ефективне регуляторне середовище, яке сприятиме інноваціям і одночасно захищатиме основні права та свободи осіб.

Для гармонізації технологічних інновацій і законодавчих рамок у контексті використання блокчейн-технологій, необхідно розглянути кілька ключових аспектів, які дозволять забезпечити ефективну взаємодію між новітніми технологіями та чинними правовими стандартами.

Перш за все, важливо створити правові механізми для визначення та регулювання технологічних процесів, які використовують блокчейн. Це може включати визначення правил щодо використання смарт-контрактів, вимог до прозорості блокчейн-операцій та стандартів безпеки даних. Такі механізми дозволять не тільки захистити користувачів, але й надати юридичну ясність для бізнесу, що сприятиме його розвитку.

Також потрібно враховувати потреби у захисті особистих даних. Розробка правил, що дозволять блокчейн-платформам виконувати операції з даними, не порушуючи правил приватності, є критично важливою. Це може включати розробку нових технологічних рішень, які дозволяють забезпечити анонімність та безпеку даних.

Також, як вже зазначалося, важливо забезпечити участь усіх зацікавлених сторін у процесі регулювання, включно з технологічними експертами, юристами, бізнесом та громадськістю. Це дозволить врахувати різні погляди та потреби, що сприятиме створенню ефективного і справедливого регуляторного середовища.

Окрема увага повинна бути приділена міжнародній координації та співпраці, оскільки блокчейн часто використовується в транснаціональних контекстах [12]. Гармонізація законодавчих норм між країнами може допомогти уникнути правової невизначеності та сприяти міжнародній торгівлі та співпраці.

Імплементація цих рекомендацій вимагатиме часу та ресурсів, але вони є ключовими для того, щоб технологічні інновації, такі як блокчейн, залишалися відповідними та інтегрованими в чинні правові рамки, гарантуючи при цьому безпеку, прозорість та захист прав користувачів. Впровадження цих змін потребує балансу між інноваціями та регуляторним контролем, щоб забезпечити, що нові технології не лише вдосконалюють бізнес-процеси, але й сприяють соціальному добробуту та захисту особистих прав.

Отже, блокчейн пропонує значні переваги з погляду безпеки та прозорості, але його основні характеристики, такі як незмінність та децентралізація, створюють виклики для виконання норм щодо конфіденційності, зокрема GDPR, особливо щодо права на забуття. Розробка та адаптація законодавства для інтеграції блокчейну є критичною задачею. Це містить в собі створення правових рамок, що дозволяють гармонізувати інноваційні технології з чинними вимогами до захисту даних. Різні підходи до регулювання конфіденційності в різних країнах, такі як відмінності між GDPR в Європі та інші закони про персональні дані інших країн, підкреслюють потребу в уніфікації міжнародних норм.

Блокчейн-технології мають значний потенціал для зміцнення безпеки та прозорості у цифровому світі. Вони впроваджують децентралізацію та незмінність записів, що може забезпечити більш надійний захист інформації від несанкціонованих втручань і фальсифікацій.

Розвиток регулювання блокчейну та захисту конфіденційності буде залежати від кількох ключових факторів. Перш за все, необхідно розвивати та впроваджувати міжнародні стандарти, які дозволять координувати дії різних країн та забезпечити єдиний підхід до регулювання блокчейн-технологій. Це допоможе уникнути юридичної розрізненості та спростить використання блокчейну в міжнародних проєктах.

Національні законодавства повинні бути гнучкими та здатними адаптуватися до технологічних інновацій. Важливо відмовитися від суворих норм, які обмежують розвиток новітніх технологій, і замість цього впроваджувати принципи, які підтримують інновації та одночасно захищають права користувачів. Це може включати розробку законів, які враховують особливості блокчейну, такі як незмінність і децентралізація, і надають юридичну ясність щодо використання смарт-контрактів та інших інноваційних технологій.

Також важливо створювати механізми для постійного діалогу між технологічними фахівцями, законодавцями, бізнесом та громадськістю. Відкрите обговорення допоможе сформувати стратегії, що враховують потреби різних сторін та забезпечують баланс між інноваціями та захистом прав. Інклюзивний підхід сприятиме розробці законодавства, яке відповідає реальним потребам суспільства і технологічного розвитку.

Окрім цього, перспективи розвитку регулювання блокчейну та захисту конфіденційності залежать від здатності законодавчих та регуляторних органів швидко реагувати на технологічні зміни. Це може вимагати від урядів збільшення інвестицій в юридичні дослідження та освіту, щоб законодавці та регуляторні органи мали глибоке розуміння технологій, які вони регулюють.

Таким чином, інтеграція блокчейну в різноманітні сфери вимагає від законодавців впровадження гнучких, прогресивних та ефективних правових рамок, які б сприяли інноваціям та забезпечували високий рівень захисту особистих даних та конфіденційності.

ЛІТЕРАТУРА

1. 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) : Регламент Європ. Союзу від 27.04.2016 р. № 2016/679. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 08.05.2024).

2. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. SSRN Electronic Journal. 2008. URL: https://doi.org/10.2139/ssrn.3440802 (дата звернення: 08.05.2024).

3. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI : станом на 27 квіт. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 08.05.2024).

4. THE CCPA. The California Consumer Privacy Act (CCPA). 2019. С. 123–169. URL: https://doi.org/10.2307/j.ctvjghvnn.15 (дата звернення: 08.05.2024).

5. De Lucca N., Martins G. M., Queiroz R. C. Z. Brazilian General Data Protection Law (LGPD) and California Consumer Privacy Act (CCPA). Brazilian Journal of Law, Technology and Innovation. 2023. Т. 1, № 1. С. 38–57. URL: https://doi.org/10.59224/bjlti.v1i1.38-57 (дата звернення: 08.05.2024).

6. Netshakhuma N. S. Assessment of a South Africa national consultative workshop on the Protection of Personal Information Act (POPIA). Global Knowledge, Memory and Communication. 2019. Т. 69, № 1/2. С. 58–74. URL: https://doi.org/10.1108/gkmc-02-2019-0026 (дата звернення: 08.05.2024).
7. Semenzin S., Rozas D., Hassan S. Blockchain-based application at a governmental level: disruption or illusion? The case of Estonia. Policy and Society. 2022. URL: https://doi.org/10.1093/polsoc/puac014 (дата звернення: 08.05.2024).
8. Wang Q., Su M., Li R. Is China the world's blockchain leader? Evidence, evolution and outlook of China's blockchain research. Journal of Cleaner Production. 2020. Т. 264. С. 121742. URL: https://doi.org/10.1016/j.jclepro.2020.121742 (дата звернення: 08.05.2024).
9. Zhang R., Xue R., Liu L. Security and Privacy on Blockchain. ACM Computing Surveys. 2019. Т. 52, № 3. С. 1–34. URL: https://doi.org/10.1145/3316481 (дата звернення: 08.05.2024).
10. An Overview of AI and Blockchain Integration for Privacy-Preserving / Z. Li та ін. Cryptography and Security. 2023. URL: https://doi.org/10.48550/arXiv.2305.03928 (дата звернення: 08.05.2024).
11. Al Asqah M., Moulahi T. Federated Learning and Blockchain Integration for Privacy Protection in the Internet of Things: Challenges and Solutions. Future Internet. 2023. Т. 15, № 6. С. 203. URL: https://doi.org/10.3390/fi15060203 (дата звернення: 08.05.2024).
12. Gürcan B. Application of Blockchain Technology to the International Trade and Customs Regulation. Central and Eastern European eDem and eGov Days. 2022. Т. 341. С. 409–417. URL: https://doi.org/10.24989/ocg.v341.30 (дата звернення: 08.05.2024).