

Київського університету інтелектуальної власності та права. № 1 (2022). С. 3-8 DOI 10.32782/chasopyskiiivp/2022-1-1

7. Часник М. І. Міжнародні підходи до визначення і кримінальної відповідальності за колабораційну діяльність (на прикладі Австрії та Ліхтенштейну). *Часопис Київського університету права*. 2023. № 3. С. 251-255. <https://doi.org/10.36695/2219-5521.3.2023.51>

8. Vyhivskiy I. Countering collaborationism in the context of armed conflict. *Baltic Journal of Economic Studies*. 2024. No.10(3) pp.96-103. doi: 10.30525/2256-0742/2024-10-3-96-103.

9. Сьомін С. В., Комашко В. В. Сучасна парадигма колабораціонізму в умовах російського вторгнення в Україну: історико-правовий аналіз. *Право та державне управління*. 2023. № 4. С. 194-201.

10. Колабораціонізм у медицині: національна судова практика та вимоги міжнародного гуманітарного права. URL: <https://mipl.org.ua/kolaboraczionizm-u-medyczyni-naczionalna-sudova-praktyka-ta-vymogy-mizhnarodnogo-gumanitarnogo-prava/>

11. Ємельянов Р. О., Єлаєв Ю. Л. Кримінально-правова характеристика колабораційної діяльності. *Публічне право*. 2023. № 3 (51). С.100-108. DOI 10.32782/2306-9082/2023-51-11

DOI <https://doi.org/10.36059/978-966-397-557-3-22>

КІБЕРБЕЗПЕКА ТА ПРАВОВІ ГАРАНТІЇ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У ДЕРЖАВНИХ ЕЛЕКТРОННИХ СЕРВІСАХ

Морозова П. О.

*студентка факультету міжнародного та європейського права,
Національний юридичний університет імені Ярослава Мудрого
м. Харків, Україна*

Кібербезпека та захист даних громадян набувають особливого значення в умовах цифрового розвитку державного управління. Сьогодні електронні реєстри й застосунки, включно з платформою «Дія», виступають ключовим каналом комунікації та надання послуг між владою та громадянами. Під час війни ризики несанкціонованого доступу до інформаційних систем, кібератак і витоку персональних даних зростають, що ускладнює захист прав людини. Надійний захист персональної інформації вимагає не лише технічних рішень, а й ефективного адміністративно-правового регулювання, оскільки саме правові процедури формують систему захисту громадян у цифровому середовищі. Тому вивчення адміністративно-

правових способів захисту персональних даних у роботі державних електронних ресурсів під час воєнних загроз є особливо актуальним для посилення інформаційної безпеки та захисту прав людини.

Ст. 32 Конституції України гарантує право на приватність і недоторканність, але за певних умов ці права та інші права можуть тимчасово обмежуватися (ч. 2 ст. 64 Конституції України). Одна з ключових проблем, що постає перед органами державної влади у царині кібербезпеки, – знаходження балансу між інтересами національної безпеки та правами осіб. Основні нормативні акти, що регулюють відповідну сферу суспільних відносин: Закон України «Про захист персональних даних» № 2297-VI (2010), що встановлює правила обробки та захисту даних; Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII (2017), який визначає державні електронні ресурси як об'єкти критичної інфраструктури. Закон України «Про правовий режим воєнного стану» (2015) дозволяє обмежувати доступ до інформаційних ресурсів у надзвичайних умовах, що наразі здійснюється в умовах режиму воєнного стану [2, с.133–136]. Одним із важливих орієнтирів для України у сфері захисту персональних даних є дотримання європейських стандартів, зокрема Загального регламенту ЄС про захист даних (GDPR). Він визначає принципи, такі як мінімізація даних, обмеження цілей їх обробки, отримання згоди суб'єкта та право бути забутим. В. Теремецький та Д. Цвірюк наголошують, що ефективний захист персональних даних можливий лише за умов гармонізації українського законодавства з європейськими нормами, включаючи створення незалежного органу контролю – так званого "інформаційного омбудсмена" [3, с. 73–75]. Європейський суд з прав людини (ЄСПЛ) встановив низку важливих стандартів тлумачення статті 8 Конвенції про захист прав людини і основоположних свобод, яка закріплює право на повагу до приватного життя. У рішенні у справі *Leander v. Sweden* (1987) Суд визнав, що зберігання інформації у державних реєстрах та відмова у доступі до неї становлять втручання у приватне життя. У справі *Breyer v. Germany* (2020) ЄСПЛ підтвердив, що процедура збору та зберігання персональних даних також є втручанням у право на приватність. Однак таке втручання може бути допустимим лише за умови дотримання принципів пропорційності та законності [4, с. 612].

Незважаючи на наявність базових норм щодо захисту персональних даних та кібербезпеки у національному законодавстві, існують значні прогалини, що суттєво знижують ефективність їх реалізації. Це, наприклад, відсутність чітко визначених процедур швидкого реагування на масові витоки даних із державних електронних реєстрів, що, у свою чергу, створює критичні виклики і загрози для нормального функціонування суспільства і держави. Законодавство здебільшого обмежується загальними

положеннями про зобов'язання розпорядників інформації забезпечувати її збереження, проте не передбачає конкретного алгоритму дій у випадках порушення конфіденційності. Це ускладнює оперативне відновлення прав громадян, що потрапили під вплив таких інцидентів. Крім того, залишається неврегульованим питання використання технологій блокчейн у державних електронних реєстрах. Хоча ці технології розглядаються як перспективний інструмент для забезпечення прозорості та незмінності даних, їхнє впровадження супроводжується конфліктами із правом на видалення інформації (так зване «право бути забутим»), закріпленим у європейському праві та частково імplementованим у законодавство України. Така правова невизначеність створює серйозні ризики для інтеграції інноваційних технологій у сферу електронного урядування. Варто зазначити, що Міністерство оборони України ухвалило новий перелік кризових ситуацій та розробило алгоритм оперативного реагування на них. Проте це рішення здебільшого зосереджене на організаційно-адміністративному аспекті оборонної системи, а його зв'язок із питаннями кібербезпеки залишився недостатньо деталізованим у публічних документах. Наприклад, у повідомленнях відсутній опис механізмів взаємодії цього алгоритму з процесами обробки персональних даних в контексті масових витоків або несанкціонованого доступу до інформації. Не зрозуміло, яким чином алгоритм оперативного реагування узгоджується із нормативним забезпеченням захисту даних, чи передбачено процедуру інформування суб'єктів даних про такі порушення, а також яка відповідальність запроваджується за недотримання відповідних заходів безпеки?. Таким чином, хоча державними органами сформовані базові нормативні рамки для реагування на кризові ситуації, відсутність деталізації механізмів захисту інформаційних систем свідчить про наявність значних прогалин у правовому регулюванні кібербезпеки в межах державних електронних сервісів.

Дослідження показують, що навіть при застосуванні криптографічного захисту та електронного підпису залишається проблема перевірки достовірності даних, які вносяться у реєстри [2, с.144]. Це пов'язано з тим, що відсутність цифрового підпису підтверджує лише технічну цілісність запису, але не його правдивість з точки зору змісту. Застосунок «Дія» (Єдиний портал державних послуг «Дія») став зручним інструментом для цифрової взаємодії, однак водночас він створив нові виклики у царині кібербезпеки. Наприклад, у 2024 році масштабна кібератака призвела до недоступності послуг програми для багатьох користувачів. У наступному році відбувся витік даних у мережу Інтернет, проте представники «Дії» заперечують, що ці дані походять саме з їх системи. Важливим є те, що в єдиній платформі концентрується значний обсяг конференційної інформації, що може призвести до ризиків масового витоку даних. У цьому

випадку доцільно застосовувати механізми токенізації доступу, трьохфакторної автентифікації та обов'язкового виконання принципу «Privacy by Design», який визначено як у європейському законодавстві (ст. 25 GDPR), так і в вітчизняних нормативах.

Слід також враховувати, що під час війни значно зростає кількість кібератак на державні системи. Державні реєстри, які зберігають дуже важливу інформацію, стають основною мішенню зловмисників. 19 грудні 2024 році російські хакери “зламали” сайти Національних інформаційних систем та Міністерства юстиції України, що на деякий час зробило неможливим доступ до них користувачів. У 2022 році було ухвалено Постанову Кабінету Міністрів України «Деякі питання забезпечення функціонування публічних електронних реєстрів в умовах воєнного стану», якою заборонено для обробки даних використовувати центри обробки даних та хмарні середовища, розташовані на тимчасово окупованих територіях України. Навпаки, для забезпечення додаткових гарантій безпеки і захисту даних, було рекомендовано перенести всі ресурси до закордонних центрів [1, с.79]. Реалізація відповідних вимог і обмежень істотно зменшує ризики витоків інформації. Вважаємо, що удосконалення система захисту персональних даних має здійснюватися одночасно у двох напрямках: технічному (використання шифрування, токенізації, гібридних блокчейн-моделей) та правовому (прийняття нових законопроектів, адаптованих до реалій воєнного стану).

Таким чином, забезпечення прав людини під час воєнного стану залежить від кібербезпеки та захисту персональних даних державних електронних послуг. Відсутність чітких процедур реагування на витoki даних і правова невизначеність щодо новітніх технологій, особливо блокчейн, створюють значні ризики і загрози. Узгодження вітчизняного законодавства і практики його застосування з міжнародними стандартами, зокрема GDPR, разом із комплексом технічних і юридичних процедур дозволить підвищити стійкість інформаційних систем і підвищити довіру громадян до державних електронних послуг.

Література

1. Худолей Я.Г., Загребельна Н.А. Захист персональних даних у період дії в Україні правового режиму воєнного стану: загальнотеоретичні аспекти. *Legal Bulletin*. 2023. № 8. С. 75–82. URL:<https://doi.org/10.31732/2708-339x-2023-08-75-82>.

2. Балацька В.С. Підвищення ефективності захисту персональних даних користувачів в умовах цифрової інформатизації державних реєстрів України: дис. ... д-ра філософії : 125/ Нац. ун-т “Львівська політехніка”. Львів, 2025. 231 с.

3. Теремецький В. І., Цвірюк Д. В. Застосування зарубіжного досвіду правового захисту персональних даних в Україні. Часопис Академії адвокатури України. 2014. Т. 7, № 2 (23). С. 73–82. URL:

4. Пашинський В. Й., Цюменко А. В. Захист персональних даних Європейським судом з прав людини. *Юридичний науковий електронний журнал*. 2024. № 10. С. 610–613.

5. Мізіна І. В. Особливості правового регулювання фінансування оборонної сфери в умовах воєнного стану. *Актуальні проблеми вітчизняної юриспруденції*. 2023. № 1. С. 141–145. DOI: <https://doi.org/10.32782/39221444>.

DOI <https://doi.org/10.36059/978-966-397-557-3-23>

РОЛЬ ПРАВА НА ЗАБУТТЯ В РЕАЛІЗАЦІЇ ОСОБИСТИХ ПРАВ ЛЮДИНИ

Мудрисівська Л. М.

*кандидат філософських наук, кандидат юридичних наук, доцент,
завідувачка кафедри теорії держави і права, конституційного права
та державного управління,*

*Дніпровський національний університет імені Олеся Гончара
м. Дніпро, Україна*

У зв'язку з повною зміною характеристик інформаційного простору і виникненням реального світового інформаційного суспільства виникають нові прояви вже давно існуючих прав людини, які надають нове розуміння сутності особистих прав людини. В науковій літературі є дискусійним питання віднесення нових прав, що виникають в постіндустріальному суспільстві, до четвертого або п'ятого покоління прав людини. Тому автор вирішив розглянути природу такого права, як права на забуття. Це право деякі автори відносять до четвертого покоління прав (О. Совгіря, В. Батиргарєєва), які пов'язані, в першу чергу, з виникненням інформаційних цифрових прав. На нашу думку, це право має подвійну природу: з одного боку, воно пов'язано з групою особистих прав людини – права на повагу до честі та гідності, особисту недоторканність, свободу слова і думки і т.д. З іншого, за своєю сутністю, воно, так би мовити, механізоване право, бо безпосередньо пов'язано з технічними можливостями та конфіденційною політикою світових і національних інформаційних платформ та месенджерів.

Також необхідно відзначити, що це право може бути пов'язано з багатьма аспектами персональної інформації: достовірність або неточність