https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

5. Інформаційна довідка щодо правових та інституційних засад організації та розвитку медіаграмотності в Україні, Європейському Союзі та окремих державах-членах Європейського Союзу* URL: https://research.rada.gov.ua/uploads/documents/33489.pdf

6. Заславська Л.В. Нормативно-правове та інституційне забезпечення інформаційної культури в умовах цифрової трансформації. Інформація і право. № 1(56)/2026. 2026. С. 96-106. URL: https://doi.org/10.37750/2616-6798.2026.1(56).357248

7. Індекс медіаграмотності українців: 2020–2025 (шоста хвиля) URL: https://detector.media/infospace/article/248278/2026-03-13-indeks-mediagramotnosti-ukraintsiv-20202025-shosta-khvylya/.

8. Про громадську організацію «Сегалор» URL: https://scanarixmediagame.com/about.

9. Горбань, Ю., & Олійник, О. (2024). Медіаграмотність як чинник захисту інформаційного простору від ворожої дезінфомації в час війни. Український інформаційний простір, (1(13), 194–205. https://doi.org/10.31866/2616-7948.1(13).2024.300896

**Заярний Олег Анатолійович**
доктор юридичних наук, професор, головний науковий співробітник наукової лабораторії інформаційних прав та безпеки людини Державної наукової установи «Інститут інформації, безпеки і права Національної академії правових наук України»

## ІНФОРМАЦІЙНА ДЕЛІКТОЛОГІЯ ЯК МЕТОДОЛОГІЧНА ОСНОВА КВАЛІФІКАЦІЇ ПРАВОПОРУШЕНЬ В ІМЕРСИВНИХ ЦИФРОВИХ СЕРЕДОВИЩАХ

Стрімке впровадження імерсивних технологій у сферах освіти, культури, публічних послуг і електронної комерції формує якісно новий простір соціальної взаємодії людини. Особливістю такого простору є безперервне зчитування з користувача біометричних і поведінкових даних та можливість впливу на його сприйняття й волевиявлення засобами імерсивного дизайну Такі перетворення часто мають наслідком виникнення нового виду інформаційних правопорушень, об’єктом яких є інформаційні права особи, її персональні дані та кібербезпека. Водночас існуючі на практиці галузеві підходи кваліфікують ці діяння

фрагментарно, не охоплюючи їхньої інформаційно-правової природи. Поряд з цим гармонізація законодавства України з правом Європейського Союзу, зокрема з Актом про штучний інтелект та Загальним регламентом про захист даних, потребує узгодженого методологічного інструментарію кваліфікації таких діянь. За цих умов актуалізується потреба проаналізувати придатність вітчизняної концепції інформаційної деліктології як методологічної основи для кваліфікації правопорушень в імерсивних середовищах.

**Метою цієї роботи** є обґрунтування придатності методологічного апарату інформаційної деліктології для кваліфікації правопорушень, що вчиняються в імерсивних цифрових середовищах, та визначення напрямів його адаптації до особливостей таких середовищ.

Інформаційна деліктологія сформувалася у вітчизняному правознавстві як комплексний міждисциплінарний напрям, предметом якого є інформаційні правопорушення (інформаційні делікти), їх склад, причини та засоби запобігання [1]. Її понятійний апарат — поняття інформаційного делікту, його складу та деліктоздатності суб'єктів — було розроблено передусім стосовно традиційного інформаційного простору [3, с. 295]. Перенесення цього апарату в імерсивні середовища супроводжується виникненням трьох основних проблем.

Перша проблема — методологічна фрагментація. Шкідливі діяння в імерсивних середовищах (несанкціоноване зчитування біометрії, виведення емоцій, маніпулятивний імерсивний вплив, привласнення цифрової особистості) одночасно мають ознаки адміністративних, цивільних і кримінальних правопорушень, у зв'язку з чим кваліфікуються розрізнено, а їх спільна інформаційно-правова сутність - посягання на інформаційні права та безпеку особи — залишається поза увагою. Саме інформаційна деліктологія, яка об'єднує ці делікти за спільним об'єктом, дає змогу подолати цю фрагментацію [2, с. 124].

Друга проблема — понятійний розрив. Класичні елементи складу інформаційного делікту потребують адаптації під імерсивний контекст. Йдеться, зокрема, про ускладнення категорії суб'єкта делікту (користувач, оператор платформи, розробник системи штучного інтелекту, автономний програмний агент), розширюється об'єкт (біометричні та поведінкові дані, цифрова ідентичність, свобода волевиявлення), видозмінюється об'єктивна сторона, оскільки діяння опосередковане імерсивним інтерфейсом і алгоритмічним обробленням даних у реальному часі.

Третя проблема — відсутність достатнього нормативного регулювання. Право Європейського Союзу вже встановлює заборони, безпосередньо відповідні імерсивним середовищам: Акт про штучний інтелект забороняє

застосування систем, що виводять емоції особи у сферах праці та освіти (ст. 5(1)(f)), біометричну категоризацію для встановлення чутливих ознак (ст. 5(1)(g)) і маніпулятивні підсвідомі практики, здатні спотворити поведінку та заподіяти шкоду (ст. 5(1)(a)) [4]; режим біометричних даних визначає Загальний регламент про захист даних [5]. У законодавстві України загальні засади обігу інформації встановлено Законом «Про інформацію» [7], а оброблення персональних даних — Законом «Про захист персональних даних» [6], проте жоден із них не оперує деліктологічними категоріями стосовно імерсивних середовищ, що унеможливлює переведення наведених заборон у кваліфіковані склади правопорушень із чітким розподілом відповідальності.

Серед можливих шляхів розв'язання окреслених проблем можна запропонувати наступні: По-перше, методологічний апарат інформаційної деліктології доцільно використати як комплексну модель, яка класифікує імерсивні шкідливі діяння за їх інформаційним об'єктом, а не за галузевою належністю санкції. По-друге, елементи складу інформаційного делікту потребують істотної адаптації. Так, зокрема, об'єкт інформаційних правопорушень може бути розширений шляхом включення до нього біометричних і поведінкових даних та свободи волевиявлення. У свою чергу, об'єктивна сторона вимагає врахування виведення емоцій, імерсивної маніпуляції та зчитування даних у реальному часі. cОсновний вектор удосконалення категорії «суб'єкт інформаційного правопорушення» має бути зосереджений на розподілі деліктоздатності між користувачем, оператором платформи й розробником системи штучного інтелекту з урахуванням обов'язку людського нагляду. По-третє, понятійний апарат інформаційної деліктології доцільно гармонізувати із заборонами ст. 5 Акта Європейського Союзу про штучний інтелект та режимом біометричних даних Загального регламенту про захист даних, побудувавши на цій основі типологію імерсивних інформаційних деліктів. По-четверте, для відмежування правомірної обробки даних від протиправної варто розробити сценарні критерії оцінювання, придатні для застосування у правозастосовній і нормотворчій практиці.

На підставі проведеного дослідження можна сформулювати такі основні висновки і рекомендації:

1. Інформаційна деліктологія створює необхідну методологічну основу кваліфікації правопорушень в імерсивних середовищах, оскільки об'єднує різнорідні діяння за спільним інформаційно-правовим об'єктом і усуває фрагментарність галузевих підходів.

2. Склад інформаційного делікту потребує адаптації до імерсивної специфіки — розширення об’єкта (біометричні та поведінкові дані, свобода волевиявлення), уточнення об’єктивної сторони та розподілу деліктоздатності між кількома суб’єктами.

3. Доцільно сформувати типологію імерсивних інформаційних деліктів, узгоджену із заборонами ст. 5 Акта Європейського Союзу про штучний інтелект та режимом біометричних даних Загального регламенту про захист даних, що може стати підґрунтям подальшихнаукових досліджень і змін до законодавства.

4. Категорію людського нагляду, на нашу думку, слід запровадити у вітчизняну доктрину як критерій деліктоздатності за правопорушення, вчинені за опосередкування систем штучного інтелекту в імерсивних середовищах.

**Список використаних джерел:**

1. Заярний О. А. Правове забезпечення розвитку інформаційної сфери України: адміністративно-деліктний аспект : монографія. Херсон : Видавничий дім «Гельветика», 2017. 700 с. URL: https://ippi.org.ua/sites/default/files/zayarnii_monografiya_tv_pereplet_0.pdf (дата звернення: 03.06.2026).

2. Заярний О. А. Публічно-правові засади розвитку науки інформаційної деліктології на сучасному етапі цифрової трансформації України. Концептуальні засади розвитку вітчизняного адміністративного права та процесу : колективна монографія / за заг. ред. П. Діхтієвського, В. Пашинського. Рига : Baltija Publishing, 2022. С. 123–149.

3. Zaiarnyi O. A. Information Delictology as a New Legal Science: Issues of the Principal Sense-Making Elements Formation. Legal scholarly discussions in the XXI century : collective monograph. Lviv ; Toruń : Liha-Pres, 2019. P. 295–318.

4. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj (дата звернення: 03.06.2026).

5. 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 (Загальний регламент про захист даних). URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 03.06.2026).

6. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 03.06.2026).