Савело Мар'яна Сергіївна,
здобувачка ступеня вищої освіти бакалавра Навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Тригубенко Галина Василівна,
доцент кафедри конституційного права Навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук, доцент

ПРАВО НА ПРИВАТНІСТЬ У ЦИФРОВУ ЕПОХУ: ВИКЛИКИ ЦИФРОВИХ ПЛАТФОРМ ТА ШТУЧНОГО ІНТЕЛЕКТУ

Сучасне інформаційне суспільство характеризується прискореним розвитком цифрових технологій, що трансформує традиційні правові уявлення про особисте життя, конфіденційність та автономію особи. Право на приватність, закріплене в міжнародних правозахисних актах та конституціях багатьох держав, включаючи Конституцію України (ст. 32), зазнає нових викликів, спричинених масовим збором, обробкою та аналізом персональних даних цифровими платформами та системами штучного інтелекту (ШІ). Ці технології, хоча й сприяють інноваціям та ефективності, водночас несуть загрозу фундаментальним правам людини, зокрема до ризиків масового спостереження, дискримінації, алгоритмічної маніпуляції та втрати контролю над власною інформацією. У цьому контексті актуалізується необхідність розробки адекватних правових механізмів, які б забезпечували ефективний захист права на приватність у цифровому середовищі [1].

Одним із ключових викликів для України, пов'язаних із діяльністю цифрових платформ, є їхня роль як «цифрових воротарів», які, володіючи надзвичайною владою над потоками інформації, формують цифрову ідентичність користувачів. Платформи, такі як: Meta (Facebook, Instagram), Google, TikTok чи Amazon, здійснюють постійний моніторинг поведінки користувачів, аналізуючи їхні кліки, геолокацію, час перебування на сторінці, соціальні зв'язки та навіть емоційну реакцію. Така практика, хоча й виправдовується комерційною логікою персоналізації контенту та реклами, порушує принцип інформаційної самоідентифікації, закладений у теорії про «інформаційне самовизначення» (вперше сформульований у рішенні Федерального конституційного суду Німеччини 1983 року). Цей принцип

передбачає, що особа має право вирішувати, коли, у якому обсязі та кому вона хоче передати свої особисті дані. Однак у реальності користувачі часто не мають реального вибору: прийняття умов обробки даних стає необхідною передумовою доступу до послуг, що створює дисбаланс у відносинах між особою та платформою [7].

Проблемою є те, що більшість цифрових платформ повноцінно не підпадають під регулювання державних органів України, оскільки не мають офіційних представництв в нашій державі.

Крім того, цифрові платформи часто оперують непрозорою архітектурою своїх алгоритмів, що підриває можливість контролю за їхнім використанням. Так звана «чорна скринька» алгоритмів приховує від користувачів механізми прийняття рішень, які впливають на їхні права — від показу реклами до модерації контенту чи кредитного скорингу. Це порушує принципи передбачуваності, обґрунтованості та справедливості, які є основоположними в адміністративному та цивільному праві. Більше того, масштабні порушення конфіденційності, як-от скандал з Cambridge Analytica, продемонстрували, як персональні дані можуть бути використані не лише з комерційною, а й з політичною метою — для формування маніпулятивних медіастратегій, спрямованих на вплив на вибори або суспільну думку [8].

Паралельно з цим, розвиток штучного інтелекту посилює виклики для права на приватність. Системи ШІ, зокрема на основі машинного навчання, потребують великих обсягів даних для тренування моделей. Ці дані часто містять чутливу інформацію — біометричні характеристики, медичні записи, дані про сексуальну орієнтацію чи політичні погляди. Обробка таких даних без явної, вільної та інформованої згоди особи є прямою загрозою її недоторканості. Особливо небезпечними є системи розпізнавання обличчя, які все частіше впроваджуються в сфері правоохоронної діяльності, транспорту чи торгівлі. Вони можуть призводити до масового спостереження (surveillance capitalism), коли кожен рух, вираз обличчя чи місце перебування особи фіксується, аналізується та архівується без її відома. Рада Європи неодноразово зазначала, що такі практики можуть створювати суспільство страху та самоцензури, де особа утримується від висловлювання поглядів або участі в громадському житті через страх бути «поміченою» [5-6].

Правове регулювання цих явищ потребує комплексного підходу. У Європейському Союзі таким інструментом стало Загальне положення про захист даних (GDPR), яке встановило високі стандарти захисту персональних даних, зокрема принципи мінімізації даних, цільової обмеженості, обов’язкової згоди та права бути забутим. Особливу увагу GDPR приділяє автоматизованому прийняттю рішень, передбачаючи право особи на пояснення алгоритмічних рішень (ст. 22). В Україні Закон «Про захист персональних даних» (2010 р.) ще не враховує специфіки ШІ та масових платформ, що створює регуляторний вакуум. Тому необхідна модернізація національного законодавства відповідно до європейських стандартів, з урахуванням рекомендацій Ради Європи, таких

як Guidelines on the protection of individuals with regard to the processing of personal data through AI (2024) [2,3,6].

Особливу увагу слід приділити інституціональному механізму контролю. У Європейському Союзі функції нагляду за дотриманням GDPR виконує Європейський комітет з захисту даних (EDPB), а також національні органи з захисту даних. В Україні такі повноваження здійснює Уповноважений Верховної Ради України з прав людини, однак його компетенція обмежена, а ресурси недостатні для ефективного контролю над глобальними технологічними гігантами. Таким чином, необхідне посилення надзорних повноважень, підвищення кваліфікації спеціалістів, а також тісна міжнародна співпраця у сфері цифрових прав.

Крім того, важливу роль у захисті приватності має освіта. Правова грамотність у сфері цифрових технологій повинна бути інтегрована в освітні програми, зокрема в юридичних вишах, оскільки майбутні юристи — адвокати, судді, прокурори — повинні знати не лише традиційні правові норми, а й розуміти специфіку цифрової екосистеми. Адміністративне право, яке регулює відносини між державою та особою, також має адаптуватися до нових реалій: адміністративні процедури, що використовують ШІ, мають бути прозорими, з можливістю оскарження автоматизованих рішень.

Важливою тенденцією є також розвиток «етичного ШІ», який передбачає закладання принципів прав людини безпосередньо в архітектуру алгоритмів («human rights by design»). Це означає, що розробники мають враховувати можливі негативні наслідки своїх систем на етапі проєктування, а регуляторні органи — впроваджувати обов’язкову оцінку впливу на права людини перед запуском нових цифрових систем. У цьому контексті перспективним є підхід ЄС, закладений у AI Act (2024), який встановлює ризик-орієнтовану модель регулювання ШІ: чим вищий потенційний негативний вплив системи на права людини, тим жорсткіші вимоги до її розробки, впровадження та контролю [4].

У висновку можна зазначити, що цифрова епоха вимагає переосмислення права на приватність не як пасивного права бути «залишеним у спокої», а як активного права на управління власною цифровою ідентичністю. Цифрові платформи та системи штучного інтелекту не можуть функціонувати за межами правового поля — навпаки, вони мають підпорядковуватися принципам верховенства права, недискримінації та захисту особи. Ефективний захист приватності в умовах цифрової трансформації є запорукою не лише індивідуальної свободи, а й самого демократичного порядку. Тому подальший розвиток правової системи має бути спрямований на створення балансу між інноваціями та правами людини, що вимагатиме постійного діалогу між законодавцями, суддями, технологічним сектором та громадянським суспільством.

Список використаних джерел:

1. Конституція України: Закон України від 28 червня 1996 року № 254к/96-ВР.

URL:https://zakon.rada.gov.ua/laws/show/254%D0%BA/96%D0%B2%D1%80#Text
2. Про захист персональних даних: Закон України від 14 червня 2025 року № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj
4. Proposal for a regulation of the European parliament and of the council laying down harmonized rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021PC0206
5. Protecting fundamental rights within the Union. URL: https://www.europarl.europa.eu/about-parliament/en/democracy-and-human-rights/fundamental-rights-in-the-eu
6. CM(2024)52-final - Committee on Artificial Intelligence (CAI) - Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. URL: https://search.coe.int/cm#{%22CoEIdentifier%22:[%220900001680afb11f%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}
7. HEADNOTES to the Judgment of the First Senate of 15 December 1983. URL: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html
8. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. URL: https://www.hbs.edu/faculty/Pages/item.aspx?num=56791