

Література:

1. Церковник С. І. Теоретико-правовий аналіз дії права під час воєнного стану в Україні. *Аналітично-порівняльне правознавство*. 2024. № 10. С. 100-104. URL: <http://journal-app.uzhnu.edu.ua/article/view/303011/295030>
2. Хила І. Ю. Конституційно-правові обмеження особистих прав і свобод людини: Україна та зарубіжний досвід: дис ... доктора філософії з галузі знань: 08 Право за спеціальністю 081 Право. Ужгород, 2021. 235 с. URL: <https://www.uzhnu.edu.ua/uk/infocentre/get/41360>
3. Чорнолуцький Р. В. Порушення прав людини та громадянина в умовах воєнного стану. *Права людини і громадянина в умовах воєнного стану: виклики та механізми захисту* : зб. матеріалів наук. практ. конф. (м. Харків, 6 груд. 2024 р.). С. 150-153.
4. Слінько Т. М. Міжнародно-правові стандарти в галузі прав людини та їх відображення в Конституції України. *Права людини і демократія* : зб. наук. ст. за матеріалами наук. конф., (м. Харків, 15 трав. 2018 р.). С. 30–34.
5. Керівництво з демократичного законотворення для вдосконалення законодавства. Бюро ОБСЄ. 2024. С. 11 200 с. URL: <https://www.osce.org/files/f/documents/1/d/570906.pdf>

DOI <https://doi.org/10.36059/978-966-397-501-6-7>

СОЦІАЛЬНІ МЕРЕЖІ ЯК ОБ'ЄКТ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Гавалешко П. С.

кандидат юридичних наук

*суддя Шевченківського районного суду м. Чернівці
м. Чернівці, Україна*

Колотило Марія Юрївна

*аспірант кафедри конституційного та адміністративного права,
Запорізький національний університет
м. Запоріжжя, Україна*

Соціальні мережі, зокрема такі глобальні платформи, як Instagram, Facebook і TikTok, виступають значущим об'єктом адміністративно-правового регулювання у сфері захисту персональних даних. У процесі функціонування вони здійснюють масову обробку персональної

інформації користувачів, включно з ідентифікаційними даними (ім'я, прізвище), контактною інформацією (номер телефону, адреса електронної пошти), візуальними матеріалами (фотографії), а також цифровими слідами активності (лайки, коментарі) [1]. Адміністративно-правові норми покликані забезпечити належний захист цих даних з метою запобігання правопорушенням у вигляді шахрайства, порушення права на приватність та несанкціонованого використання персональної інформації. Порушення встановлених вимог щодо обробки персональних даних тягне за собою адміністративну відповідальність як для суб'єктів господарювання – операторів платформ, так і для окремих користувачів [2].

В Україні адміністративне регулювання захисту персональних даних у соціальних мережах здійснюється відповідно до Закону України «Про захист персональних даних». Цей закон покладає на операторів соціальних мереж адміністративні обов'язки щодо отримання згоди користувачів на обробку даних, надання інформації про цілі обробки та забезпечення права на видалення даних. Україна також враховує Загальний регламент про захист даних (GDPR), який встановлює жорсткі адміністративні санкції, зокрема штрафи або обмеження діяльності, за порушення норм [3]. С. В. Глянько наголошує, що недотримання адміністративних вимог користувачами та платформами сприяє зростанню витоків даних, які можуть мати серйозні наслідки, як-от шантаж чи крадіжка особистих даних [2, с. 18-20].

Адміністративне право гарантує користувачам соціальних мереж право на інформацію про те, які дані збираються, кому вони передаються та як довго зберігаються. Порушення цих прав є підставою для адміністративних скарг до уповноважених органів, як зазначає К. С. Мельник [5, с. 64-68]. Основні адміністративні загрози включають: хакерські атаки через слабкі паролі, що свідчать про неналежне виконання платформами адміністративних обов'язків щодо захисту даних; фішинг, який вимагає від платформ адміністративних заходів для запобігання шахрайським повідомленням; соціальну інженерію, коли зловмисники використовують дані профілів для шахрайства, що може вказувати на недостатній адміністративний контроль; а також несанкціоновану передачу даних рекламодавцям, що є прямим адміністративним правопорушенням [5, с. 64-69].

Адміністративне право зобов'язує користувачів дотримуватися правил безпеки для уникнення правопорушень. Д. І. Садовська рекомендує створювати складні паролі з комбінацією літер, цифр і символів, увімкнути двофакторну автентифікацію, налаштувати конфіденційність профілю для обмеження доступу, уникати публікації чутливих даних (адреса, номер телефону, банківські реквізити), ознайомлюватися з політикою конфіденційності платформ і перевіряти

несанкціонований доступ до акаунтів [7, с. 225-230]. Бліхар М. М. підкреслює, що соціальні мережі несуть адміністративну відповідальність за шифрування даних, оновлення систем безпеки та оперативне повідомлення користувачів про витоки. Недотримання цих вимог може призвести до адміністративних штрафів або заборони діяльності [1, с. 20-24].

Г. А. Прохазка зазначає, що великі компанії, такі як Meta, зазнають адміністративних санкцій за порушення GDPR, що підкреслює важливість дотримання адміністративних норм захисту даних [6, с. 151-155]. К. С. Мельник пропонує запровадити адміністративні освітні програми з кібербезпеки в навчальних закладах, щоб підвищити обізнаність молоді про адміністративні ризики в соціальних мережах, адже молодь часто ділиться даними, не враховуючи наслідків [5, с. 64-68].

Глобальне адміністративне регулювання захисту даних ускладнене через транскордонну передачу інформації. Наприклад, дані Instagram можуть зберігатися в США, де діють інші адміністративні норми, що створює виклики для компаній, таких як Google чи Meta, які зобов'язані адаптуватися до вимог кожної країни. Адміністративне право також регулює доступ додатків до особистих даних. Наприклад, додатки на кшталт Getcontact, які отримують доступ до контактів, можуть спричиняти адміністративні порушення, пов'язані з конфіденційністю. Право бути забутим, передбачене GDPR, дозволяє вимагати видалення даних, але в Україні його реалізація обмежена через невідповідність деяких платформ адміністративним стандартам, як зазначає Українська Гельсінська спілка.

Компанії, що обробляють дані, зобов'язані мати спеціалізовані підрозділи з захисту даних відповідно до Типового порядку обробки персональних даних 2014 року, затвердженого Омбудсменом. Д. І. Садовська звертає увагу на проблему геолокаційних даних, які автоматично додаються до публікацій, і пропонує запровадити адміністративні норми для обов'язкового попередження користувачів перед їх публікацією [7, с. 225-230]. О. С. Глянько вказує на непрозорість алгоритмів соціальних мереж і пропонує адміністративно вимагати від компаній розкриття їхніх методів для запобігання маніпуляціям і підвищення довіри [2, с. 18-20].

К. С. Мельник наголошує на необхідності використання штучного інтелекту для автоматичного виявлення адміністративних порушень, таких як розміщення персональних даних без згоди, що може оптимізувати адміністративний нагляд [5, с. 64-68]. Нові виклики, пов'язані зі штучним інтелектом, який аналізує дані для створення реклами чи фальшивих профілів, також потребують адміністративного регулювання. Д. І. Садовська зазначає, що користувачі повинні

перевіряти відповідність іноземних платформ адміністративним стандартам безпеки [7, с. 225-230].

Адміністративне право передбачає механізми притягнення до відповідальності за порушення у сфері захисту даних. Кодекс України про адміністративні правопорушення (стаття 188-39) встановлює штрафи за порушення законодавства про захист персональних даних, які можуть застосовуватися до фізичних чи юридичних осіб, що обробляють дані без згоди або не забезпечують їх належний захист. Органи виконавчої влади, Уповноважений Верховної Ради України з прав людини, здійснюють нагляд за дотриманням адміністративних норм у цій сфері, проводять перевірки та можуть ініціювати адміністративні провадження. Для підвищення ефективності захисту даних пропонується вдосконалити адміністративні процедури, зокрема запровадити електронні реєстри скарг і автоматизовані системи моніторингу обробки даних у соціальних мережах [4].

Захист персональних даних у соціальних мережах залежить від чіткого адміністративного регулювання, відповідальності платформ і свідомості користувачів. Користувачі повинні знати свої адміністративні права, дотримуватися правил безпеки та уникати надмірного розголошення інформації. Соціальні мережі зобов'язані виконувати адміністративні вимоги щодо захисту даних, а органи влади – забезпечувати нагляд і санкції за порушення. Спільні зусилля зроблять соціальні мережі безпечнішим середовищем.

Література:

1. Бліхар М. М. Правові основи захисту персональних даних в Інтернеті [Електронний ресурс] // Науковий вісник Міжнародного гуманітарного університету. Серія: Юриспруденція. – 2023. – № 62. – С. 20–24. – Режим доступу: <https://www.vestnik-pravo.mgu.od.ua/archive/juspradenc62/4.pdf> (дата звернення: 30.04.2025).

2. Глянько О. С. Захист персональних даних в соціальних мережах [Електронний ресурс]. – Науково-дослідний інститут публічної політики і соціальних наук. – С. 18–20. – Режим доступу: <https://pp-ss.pro/wp-content/uploads/2020/06/%D0%93%D0%BB%D1%8F%D0%BD%D1%8C%D0%BA%D0%BE.pdf> (дата звернення: 30.04.2025).

3. Закон України «Про захист персональних даних» [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата звернення: 30.04.2025).

4. Кодекс України про адміністративні правопорушення [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/80731-10#Text> (дата звернення: 30.04.2025).

5. Мельник К. С. Обробка та захист персональних даних в соціальних мережах [Електронний ресурс]. – С. 64–68. – Режим доступу:

<https://ippi.org.ua/sites/default/files/14mksdsm.pdf> (дата звернення: 30.04.2025).

6. Прохазка Г. А. Захист персональних даних у сучасному світі [Електронний ресурс] // Науковий вісник Ужгородського національного університету. – 2018. – С. 151–155. – Режим доступу: <https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/30929/1/%D0%97%D0%90%D0%A5%D0%98%D0%A1%D0%A2%D0%9F%D0%95%D0%A0%D0%A1%D0%9E%D0%9D%D0%90%D0%9B%D0%AC%D0%9D%D0%98%D0%A5%D0%94%D0%90%D0%9D%D0%98%D0%A5%D0%A3%D0%A1%D0%A3%D0%A7%D0%90%D0%A1%D0%9D%D0%9E%D0%9C%D0%A3%D0%A1%D0%92%D0%86%D0%A2%D0%86.pdf> (дата звернення: 30.04.2025).

7. Садовська Д. І. Захист персональних даних дітей у соціальних мережах в контексті права на забуття [Електронний ресурс] // Науковий вісник Ужгородського національного університету. – 2024. – С. 225–230. – Режим доступу: <https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/03/37.pdf> (дата звернення: 30.04.2025).

DOI <https://doi.org/10.36059/978-966-397-501-6-8>

ЕЛЕКТРОННІ ДОКАЗИ ЯК СПОСІБ ЗАХИСТУ ПРАВ ЛЮДИНИ

Гарашенко Вадим Вікторович

<https://orcid.org/0009-0004-8389-0869>

аспірант відділу теорії держави і права,

напрямок підготовки 081 Право,

Науковий керівник: Пархоменко Наталія Миколаївна

доктор юридичних наук, професор,

завідувач відділу теорії держави і права

Інститут держави і права імені В.М. Корецького

Національної академії наук України

м. Київ, Україна

Права людини, що сформувались внаслідок тривалого еволюційного процесу, нині закріплені в міжнародно-правових актах та законодавстві провідних держав світу. Однак, в сучасних умовах цифровізації вони трансформуються, наповнюються новим змістом, вимагають осмислення та адекватного формулювання правового механізму регулювання, реалізації та захисту.

Відповідно до ст. 55 Конституції України кожному гарантується право на оскарження в суді рішень, дій чи бездіяльності органів