УДК 342.951:004.056
DOI https://doi.org/10.32782/pyuv.v2.2024.14

В. О. Кравчук
orcid.org/0009-0003-6660-2952
аспірантка кафедри конституційного і адміністративного права
Національного авіаційного університету

ЗАВДАННЯ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СОЦІАЛЬНИХ МЕРЕЖАХ

Захист персональних даних у соціальних мережах є одним із найбільш актуальних питань сучасності, що потребує ґрунтовного вивчення та ефективного правового регулювання. Стрімкий розвиток інформаційно-комунікаційних технологій та розширення використання соціальних мереж створили нові виклики у сфері забезпечення конфіденційності та безпеки особистих даних користувачів.

Багатогранність поняття «захист персональних даних» обумовлює його дослідження з різних ракурсів. На думку Л. Кожури, «захист» не є тотожним загальному користуванню правами, а виникає лише у реакції на конкретні правопорушення або оспорювання. Відповідно, дослідниця трактує дане поняття як сукупність дій державних органів, передбачених законодавством та спрямованих на: 1) відновлення порушеного права на персональні дані; 2) припинення правопорушень у даній сфері; 3) забезпечення юридичної відповідальності винних осіб за шкоду, заподіяну правам та інтересам суб'єктів [1, с. 120].

Одним з ключових підходів до розв'язання проблеми захисту персональних даних у соціальних мережах є адміністративно-правовий захист.

У своїй роботі Н. Коломоєць вказує на те, що адміністративно-правовий захист прав є комплексним правовим явищем. Воно охоплює права та правовий статус, механізми захисту і сукупність адміністративно-правових норм, що регулюють правовий статус та повноваження органів влади та неурядових організацій щодо захисту прав [2, с. 56].

Отже, адміністративно-правовий захист прав людини є важливою гарантією оперативного та ефективного відновлення порушених прав. Він забезпечує функціонування механізмів, спрямованих на припинення правопорушень, усунення їх наслідків та притягнення винних осіб до відповідальності згідно з чинним законодавством. У сфері захисту персональних даних користувачів соціальних мереж зазначений інструмент набуває особливої значущості. Його головна мета полягає у встановленні правових норм, які гарантують право на приватне життя та забезпечують конфіденційність інформації. Такі норми дають можливість оперативно реагувати на випадки несанкціонованого доступу або розголошення персональних даних.

Ефективний адміністративно-правовий захист персональних даних у соціальних мережах передбачає комплексне регулювання на законодавчому рівні, встановлення чітких норм та правил збору, обробки та використання персональних даних, а також створення механізмів контролю та нагляду за діяльністю соціальних мереж у зазначеній сфері. Адміністративно-правове регулювання у галузі захисту персональних даних спрямоване на формування правового поля, в якому діяльність соціальних мереж щодо обробки даних користувачів буде чітко врегульована та підконтрольна відповідним державним органам. Зазначене сприятиме забезпеченню належного рівня безпеки та конфіденційності персональних даних, а також дотриманню прав і свобод людини в інформаційному просторі.

У рамках адміністративно-правового регулювання найважливішу роль відіграє саме юридична основа захисту персональних даних. На наш погляд, вона полягає у встановленні чітких законодавчих норм, які визначають права та обов'язки всіх учасників процесу збору та обробки персональної інформації. Основне завдання такої системи полягає у створенні безпечного інформаційного середовища на глобальному рівні та забезпеченні належного рівня кібербезпеки як для окремих осіб, так і для їхніх персональних даних у соціальних мережах.

К. Токарєва вважає, що ефективний захист персональних даних у соціальних мережах вимагає комплексного підходу, що поєднує належне правове регулювання та впровадження технічних засобів безпеки [3, с. 91].

Ми поділяємо зазначену позицію та вважаємо, що створення захищеного інформаційного середовища ґрунтується на низці ключових елементів. По-перше, воно передбачає формування відповідної нормативно-правової бази, яка б чітко регламентувала правила та принципи обробки персональних даних, встановлювала вимоги до соціальних мереж щодо забезпечення безпеки та конфіденційності інформації, визначала повноваження контролюючих органів та відповідальність за порушення. В Україні діють закони, що регулюють сферу захисту персональних

даних, зокрема стаття 32 Конституції України гарантує захист персональних даних [4]; Закон України «Про інформацію» визначає основні принципи інформаційних відносин щодо створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації [5]; Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» регулює відносини у сфері захисту інформації в таких системах [6]. Крім того, Типовий порядок обробки персональних даних, затверджений наказом Уповноваженого Верховної Ради України №1/02-14 від 08.01.2014 року [7], визначає загальні вимоги до організації обробки персональних даних та забезпечення їх захисту.

По-друге, необхідним є запровадження ефективних технічних та організаційних заходів безпеки, спрямованих на захист інформаційних систем та даних від несанкціонованого доступу, витоку чи пошкодження. Вважаємо, що на глобальному рівні дані заходи охоплюють:

1) технічні заходи, такі як використання сучасних криптографічних методів та протоколів для забезпечення конфіденційності та цілісності даних. Прикладами є використання шифрування з відкритим ключем (RSA, ECC), симетричного шифрування (AES, ChaCha20), хешування (SHA-256, SHA-3) та протоколів захищеного зв'язку (TLS, HTTPS);

2) впровадження надійних систем ідентифікації та автентифікації користувачів, таких як багатофакторна автентифікація, біометричні дані, технології безпечних токенів тощо, що допомагає запобігти несанкціонованому доступу до систем та даних;

3) використання брандмауерів, систем виявлення та запобігання вторгнень (IDS/IPS), антивірусного програмного забезпечення та інших засобів мережевої безпеки для захисту від зовнішніх загроз та кібератак;

4) регулярне оновлення програмного забезпечення та усунення виявлених проблем безпеки у програмному забезпеченні робить систему більш стійкою до кіберзагроз;

5) впровадження систем моніторингу та аудиту для виявлення підозрілої активності та своєчасного реагування на інциденти безпеки;

6) резервне копіювання та відновлення даних для захисту від їх втрати або пошкодження внаслідок збоїв, атак чи стихійних лих.

Натомість, організаційні заходи охоплюють розробку та впровадження комплексної політики інформаційної безпеки в організаціях. Вони також передбачають створення спеціалізованих підрозділів чи призначення відповідальних осіб для управління інформаційною безпекою, проведення регулярних навчань та підвищення обізнаності працівників, здійснення періодичних оцінок ризиків та аудитів безпеки, встановлення чітких процедур реагування на інциденти інформаційної безпеки, укладання угод про рівень обслуговування з постачальниками послуг та підрядниками, що визначають вимоги до безпеки та конфіденційності інформації.

Впровадження комплексу технічних та організаційних заходів безпеки на глобальному рівні істотно знижує ризики витоку або пошкодження персональних даних. Зазначені заходи створюють надійний захист для користувачів соціальних мереж та інших інформаційних систем.

Розглядаючи індивідуальний рівень захисту персональних даних у соціальних мережах, необхідно звернути увагу на емпіричні дані, які висвітлюють масштаби проблеми та підкреслюють важливість дотримання належних заходів безпеки. Результати загальнонаціонального дослідження «Безпека в інтернеті» свідчать про те, що в Україні широко поширені шахрайські дії в онлайн-середовищі, пов'язані з персональними даними. 30% респондентів дослідження стали жертвами різних видів онлайн-шахрайства [8]. На наш погляд, отримані результати опитування свідчать про те, що значна кількість користувачів соціальних мереж в Україні недостатньо обізнана про належні заходи безпеки або ж нехтує ними, що робить їх вразливими до різноманітних форм шахрайських дій. Серед таких дій можуть бути випадки: фішингових атак, розповсюдження шкідливого програмного забезпечення, крадіжки особистих даних або навіть фінансові махінації.

Враховуючи зазначені емпіричні дані, стає очевидною необхідність посилення зусиль щодо освіти та інформування користувачів соціальних мереж про важливість індивідуального захисту персональних даних. Необхідно розробляти та впроваджувати освітні програми, інформаційні кампанії та тренінги, спрямовані на підвищення рівня обізнаності громадян щодо потенційних ризиків, пов'язаних з розміщенням персональних даних в інтернеті, а також надавати практичні рекомендації щодо належних заходів безпеки.

Центральним елементом індивідуального захисту персональних даних є налаштування конфіденційності в соціальних мережах. Більшість популярних платформ, таких як Facebook, Instagram чи Twitter, пропонують своїм учасникам можливість контролювати рівень доступу до їхніх особистих даних та налаштовувати відповідні параметри конфіденційності. Наприклад, користувачі можуть обмежити коло осіб, які мають доступ до їхніх персональних відомостей, фотографій чи публікацій, скориставшись відповідними опціями в налаштуваннях конфіденційності.

Крім того, важливо обережно ставитися до розміщення персональних даних у соціальних мережах. Користувачам слід уникати публікації надмірної кількості конфіденційної інформації, такої як номери кредитних карток, паспортні дані, адреси проживання чи інші відомості, які можуть бути використані зловмисниками для злочинних цілей. Замість цього, рекомендується надавати лише мінімальну кількість персональних даних, необхідних для використання соціальної мережі.

Особливу увагу привертає складна багатоетапна схема шахрайства, описана правоохоронними органами Сумської області. Зазначена схема поєднує методи соціальної інженерії, фішингові атаки та безпосередній контакт із жертвою з метою незаконного заволодіння конфіденційними даними та подальшого незаконного списання грошових коштів з банківських рахунків. Потерпіла отримала повідомлення в месенджері Viber з пропозицією отримати грошову допомогу в розмірі 6 500 гривень, нібито від державних органів. Перехід за шкідливим посиланням з повідомлення призвів до несанкціонованого списання коштів з банківського рахунку під виглядом благодійного внеску. Наступним кроком зловмисник видав себе за працівника банку, зателефонував потерпілій та запевнив її в технічній помилці й можливості повернення списаних коштів. Під приводом верифікації він вимагав розголосити конфіденційні дані. Внаслідок таких дій шахраї отримали повний доступ до рахунків та незаконно заволоділи 200 000 грн [9].

Важливо також регулярно оновлювати паролі доступу до соціальних мереж та використовувати складні, унікальні паролі для кожного облікового запису. Такі дії допоможуть запобігти несанкціонованому доступу до персональних даних у випадку компрометації паролів. Крім того, рекомендується використовувати двофакторну автентифікацію, яка додає додатковий рівень безпеки до облікового запису. Загалом, індивідуальний рівень захисту персональних даних у соціальних мережах вимагає від користувачів відповідального ставлення до власної інформаційної безпеки та дотримання певних правил та рекомендацій.

Висновок. Адміністративно-правовий захист персональних даних у соціальних мережах можна розуміти як сукупність адміністративно-правових засобів, спрямованих на забезпечення права особи на безпеку персональних даних у соціальних мережах, поновлення такого права у випадку його порушення, припинення порушення та притягнення до юридичної відповідальності осіб, винних у порушенні вимог захисту персональних даних у соціальних мережах.

Завданням адміністративно-правового захисту персональних даних у соціальних мережах є створення захищеного інформаційного середовища на глобальному рівні через формування належної нормативно-правової бази, впровадження технічних та організаційних заходів безпеки. На особистісному рівні – забезпечення інформаційної безпеки конкретної особи та її персональних даних у соціальних мережах шляхом підвищення обізнаності користувачів, налаштування конфіденційності, дотримання принципів безпечного використання соціальних мереж і обачності у розміщенні персональних даних.

Ефективний адміністративно-правовий захист персональних даних у соціальних мережах потребує комплексного підходу, що поєднує належне нормативно-правове регулювання, впровадження технічних і організаційних заходів безпеки, а також підвищення обізнаності та відповідальності користувачів. Лише систематична реалізація зазначених елементів забезпечить створення безпечного інформаційного середовища та гарантуватиме дотримання права на захист персональних даних у соціальних мережах.

Література

1. Кожура Л. Адміністративно-правовий захист та охорона: поняття та співвідношення. *Науковий вісник Ужгородського національного університету*. 2015. Т. 2, № 35. С. 119–122.

2. Коломоєць Н. Адміністративно-правовий захист прав дитини в Україні : монографія. Харків, 2019. 352 с.

3. Токарєва К. Забезпечення інформаційних прав людини в соціальних мережах. *Актуальні проблеми правознавства*. 2022. № 4(32). С. 88–93.

4. Конституція України : від 28.06.1996 р. № 254к/96-ВР : станом на 1 січ. 2020 р. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (дата звернення: 23.04.2024).

5. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII : станом на 27 лип. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 23.04.2024).

6. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР : станом на 4 квіт. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення: 23.04.2024).

7. Про затвердження документів у сфері захисту персональних даних : Наказ Уповноваж. Верхов. Ради України з прав людини від 08.01.2014 р. № 1/02-14. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text (дата звернення: 23.04.2024).

8. Понад 40% українців стикаються з кібербулінгом, третина – з шахрайством онлайн. *Укрінформ*. URL: https://www.ukrinform.ua/rubric-society/3281449-ponad-40-ukrainciv-stikautsa-z-kiberbulingom-tretina-z-sahrajstvom-onlajn.html (дата звернення: 25.04.2024).

9. Втратила 200 тис. грн. На Сумщині поліцієнти з'ясовують обставини шахрайства. *Суспільне*. URL: https://suspilne.media/sumy/685062-hotila-otrimati-grosovu-dopomogu-ta-vtratila-200-tis-grn-na-

sumsini-policianti-zasovuut-obstavini-sahrajstva/ (дата звернення: 25.04.2024).

Анотація

Кравчук В. О. **Завдання адміністративно-правового захисту персональних даних у соціальних мережах.** – Стаття.

У статті розглянуто актуальну проблему захисту персональних даних у соціальних мережах та висвітлено роль адміністративно-правового захисту в забезпеченні інформаційної безпеки особистих відомостей користувачів. Проаналізовано поняття «захист персональних даних» та його різні аспекти. Визначено, що адміністративно-правовий захист є комплексним правовим явищем, яке охоплює права та правовий статус, механізми захисту та сукупність адміністративно-правових норм, що регулюють повноваження органів влади та неурядових організацій у даній сфері.

Наголошено на ключовому призначенні адміністративно-правового захисту персональних даних у соціальних мережах – створенні правових засад для забезпечення права на недоторканність приватного життя та конфіденційності інформації, а також оперативного реагування на випадки несанкціонованого доступу чи витоку даних. Окреслено основні елементи адміністративно-правового захисту на глобальному та індивідуальному рівнях.

На глобальному рівні запропоновано формування відповідної нормативно-правової бази, що регламентує правила збору, обробки та використання персональних даних, а також запровадження ефективних технічних та організаційних заходів безпеки. Наведено приклади технічних заходів, зокрема використання криптографічних методів, систем ідентифікації та автентифікації користувачів, брандмауерів, антивірусного програмного забезпечення тощо. Організаційні заходи включають розробку політики інформаційної безпеки, створення спеціальних підрозділів, навчання персоналу, проведення оцінок ризиків та аудитів.

На індивідуальному рівні акцентовано на важливості підвищення обізнаності користувачів, налаштування параметрів конфіденційності, дотримання принципів безпечного використання соціальних мереж та обачності у розміщенні персональних даних. Наведено рекомендації щодо використання складних паролів, двофакторної автентифікації, уникнення надмірного розголошення конфіденційної інформації.

Узагальнено, що ефективний адміністративно-правовий захист персональних даних у соціальних мережах потребує комплексного підходу з поєднанням належного правового регулювання, технічних і організаційних заходів безпеки, а також відповідальності користувачів. Лише систематична реалізація зазначених елементів забезпечить створення безпечного інформаційного середовища та гарантуватиме дотримання права на захист персональних даних.

Ключові слова: персональні дані, соціальні мережі, адміністративно-правовий захист, завдання захисту персональних даних, рівні захисту.

Summary

Kravchuk V. O. **Administrative-legal protection tasks of personal data in social networks.** – Article.

This article addresses the pressing issue of personal data protection in social networks and highlights the role of administrative-legal protection in ensuring the information security of users' personal information. The concept of «personal data protection» and its various aspects are analyzed. It is determined that administrative-legal protection is a comprehensive legal phenomenon encompassing rights and legal status, protection mechanisms, and a set of administrative-legal norms regulating the powers of government bodies and non-governmental organizations in this area.

Emphasis is placed on the key purpose of administrative-legal protection of personal data in social networks – establishing legal principles to safeguard the right to privacy and confidentiality of information, as well as promptly responding to instances of unauthorized access or data breaches. The main elements of administrative-legal protection at both global and individual levels are outlined.

At the global level, the formation of an appropriate regulatory framework regulating the rules for the collection, processing, and use of personal data is proposed, as well as the implementation of effective technical and organizational security measures. Examples of technical measures are provided, including the use of cryptographic methods, user identification and authentication systems, firewalls, antivirus software, etc. Organizational measures include developing information security policies, establishing specialized units, staff training, risk assessments, and audits.

At the individual level, the importance of increasing users' awareness, configuring privacy settings, adhering to principles of safe social media use, and exercising caution in sharing personal data is emphasized. Recommendations are provided for using complex passwords, two-factor authentication, and avoiding excessive disclosure of confidential information.

In conclusion, it is summarized that effective administrative-legal protection of personal data in social networks requires a comprehensive approach combining appropriate legal regulation, technical and organizational security measures, as well as user responsibility. Only the systematic implementation of these elements will ensure the creation of a secure information environment and guarantee compliance with the right to personal data protection.

Key words: personal data, social networks, administrative-legal protection, tasks of personal data protection, levels of protection.