УДК 342.7
DOI https://doi.org/10.24144/2307-3322.2024.86.1.25

ЗАБЕЗПЕЧЕННЯ ПРАВА НА ПРИВАТНІСТЬ У КОНТЕКСТІ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ: ПОТЕНЦІЙНІ ЗАГРОЗИ ТА ШЛЯХИ ЇХ ПОДОЛАННЯ

Гудзь Л.В.,
кандидатка юридичних наук, доцентка,
доцентка кафедри конституційного і муніципального права
юридичного факультету
Харківського національного університету
імені В.Н. Каразіна,
ORCID: 0000-0002-2064-014X
e-mail: l.v.gudz@karazin.ua

Гудзь Л.В. Забезпечення права на приватність у контексті використання штучного інтелекту: потенційні загрози та шляхи їх подолання.

У статті проаналізовано потенційні загрози для права на приватність (privacy), що виникають у контексті використання штучного інтелекту, а також запропоновано шляхи їх подолання через удосконалення законодавчих механізмів захисту приватних даних в Україні.

Захист права на приватність набуває особливого значення через стрімкий розвиток технологій у світі. Масовий збір персональних даних через інтернет і мобільні додатки, аналіз даних із використанням ШІ, застосування біометричних технологій, а також зростання кіберзлочинності та незаконного стеження створюють серйозні ризики для приватності особи. Тому, виникає нагальна потреба в подальших наукових дослідженнях забезпечення права на приватність у контексті використання штучного інтелекту.

Право на приватність закріплено як в універсальних, так і в регіональних міжнародних угодах, таких як: Загальна декларація прав людини, Міжнародний пакт про громадянські і політичні права, Конвенція про захист прав людини і основоположних свобод, Хартія основних прав Європейського Союзу тощо.

Суспільство все більше усвідомлює значущість захисту конфіденційності (приватності) та потенційні ризики у разі її порушення. Використання персональних даних у державних чи комерційних цілях порушує етичні питання щодо меж допустимого та недоторканного.

Зростаюча глобалізація вимагає узгоджених підходів до захисту приватності на міжнародному рівні. Прийняття таких нормативних актів, як GDPR і Закон про штучний інтелект у Європі, а також CCPA та CPRA у Каліфорнії, свідчить про важливість захисту персональних даних і права на конфіденційність.

Безумовно, Закон України «Про захист персональних даних» не відповідає викликам сьогодення і потребує доповнень, а саме: визначення понять штучного інтелекту, прозорість алгоритмів ШІ, інформована згода громадян та механізми її відкликання, обмеження доступу до персональних даних громадян, гарантії прав громадян на корекцію й видалення даних, контроль автоматизованих рішень, створення органу нагляду за ШІ та санкцій за порушення.

Ключові слова: право на приватність, штучний інтелект, конфіденційність, персональні дані.

Gudz L.V. Ensuring the right to privacy in the context of artificial intelligence: potential threats and ways to overcome them.

The article analyzes the potential threats to the right to privacy arising in the context of artificial intelligence and suggests ways to overcome them by improving the legislative mechanisms for protecting private data in Ukraine.

The protection of the right to privacy is of particular importance due to the rapid development of technology in the world. Massive collection of personal data via the Internet and mobile applications,

data analysis using AI, the use of biometric technologies, as well as the growth of cybercrime and illegal surveillance pose serious privacy risks. Therefore, there is an urgent need for further research on ensuring the right to privacy in the context of the use of artificial intelligence.

The right to privacy is enshrined in both universal and regional international agreements, such as the following: Universal Declaration of Human Rights, International Covenant on Civil and Political Rights, Convention for the Protection of Human Rights and Fundamental Freedoms, Charter of Fundamental Rights of the European Union, etc.

Society is increasingly aware of the importance of protecting confidentiality (privacy) and the potential risks in case of its violation. The use of personal data for governmental or commercial purposes raises ethical questions about the limits of what is permissible and inviolable.

Increasing globalization requires coordinated approaches to privacy protection at the international level. The adoption of regulations such as the GDPR and the Artificial Intelligence Act in Europe, as well as the CCPA and CPRA in California, demonstrate the importance of protecting personal data and the right to privacy.

Undoubtedly, the Law of Ukraine "On Personal Data Protection" does not meet the challenges of today and needs to be supplemented, namely: definition of artificial intelligence, transparency of AI algorithms, informed consent of citizens and mechanisms for its withdrawal, restriction of access to personal data of citizens, guarantees of citizens' rights to correct and delete data, control of automated decisions, creation of an AI supervisory body and sanctions for violations.

Key words: right to privacy, artificial intelligence, confidentiality, personal data.

Постановка проблеми. Захист права на приватність набуває особливої важливості в умовах сучасного технологічного розвитку, зростання кіберзагроз, появи нових законодавчих вимог та підвищення суспільної обізнаності про значення і охорону персональних даних. Забезпечення конфіденційності потребує постійного оновлення законодавчих норм, впровадження сучасних технологічних рішень і дотримання високих етичних стандартів.

Серед ключових причин актуальності захисту права на приватність можна виділити такі аспекти: по-перше, стрімке поширення інтернету, соціальних мереж і мобільних додатків сприяє масовому збору та обробці персональних даних; по-друге, розвиток штучного інтелекту (ШІ) дозволяє аналізувати великі масиви даних, створюючи детальні профілі користувачів, що може призводити до дискримінації та загроз приватності; по-третє, впровадження технологій розпізнавання облич і біометричних даних піднімає питання щодо безпеки та використання чутливої інформації; по-четверте, зростання кіберзлочинності, включаючи хакерські атаки, фішингові схеми, витоки інформації, а також незаконне стеження з боку державних і приватних структур, значно посилює необхідність захисту персональних даних.

Метою дослідження є аналіз потенційних загроз для права на приватність, що виникають у контексті використання штучного інтелекту, а також розробка рекомендацій та шляхів їх подолання через удосконалення законодавчих механізмів захисту приватних даних в Україні.

Стан опрацювання цієї проблематики. Дослідження права на недоторканність приватного життя (приватності) розпочалися наприкінці XX століття і пов'язані з іменами західних конституціоналістів і соціологів, зокрема А. Вестіна, А. Етціоні, Дж. Іннеса, Д. О'Брайєна, Д. Солова та інших. Питання тлумачення і забезпечення права на приватність (недоторканність приватного і сімейного життя) стало предметом досліджень багатьох вітчизняних та зарубіжних науковців, серед яких Н. Бєляєва, Д. Гудима, Т. Дудаш, С. Ільченко, І. Касперський, А. Ковбан, А. Марущак, І. Михайленко, С. Мішуровська, Б. Недєлек, М. Пальчик, С. Погребняк, П. Рабінович, С. Рабінович, Ю. Разметаєва, М. де Сальвія, В. Серьогін, Т. Фулей, Г. Христова, Ж. Чевичалова, С. Шевчук та інші. Проте, зважаючи на складність і багатогранність цих проблем, виникає нагальна потреба в подальших наукових дослідженнях забезпечення права на приватність у контексті використання штучного інтелекту.

Виклад основного матеріалу. Навіть після тридцяти трьох років незалежності Українська держава все ще стикається з тим, що поняття прайвесі (від англ. privacy – таємниця, усамітнення, приватне життя) як політичний і правовий феномен залишається в значній мірі незвіданим, своєрідною terra incognita (від лат. – невідома земля).

Згідно з думкою відомого українського дослідника В. Серьогіна, «все розмаїття існуючих концепцій прайвесі можна умовно поділити на дві групи в залежності від їхнього ставлення до цього

політико-правового феномену: ті, що визнають його самостійність (абстрактні), і ті, що заперечують його незалежність (редукціоністські)».

Серед різноманітних наукових концепцій, що визнають прайвесі як самостійний політико-правовий феномен, найбільш поширеними є такі підходи: 1) прайвесі як право на усамітнення (С. Уоррен, Л. Брандейс); 2) прайвесі як обмежений доступ до особистої інформації (Д. О'Брайєн, Е. Ван Ден Хааг, Р. Гавізон); 3) прайвесі як секретність (Р. Позер, С. Джерард, А. Етціоні); 4) прайвесі як контроль над персональними даними (А. Вестін, Р. Паркер, Р. Мерфі); 5) прайвесі як захищена індивідуальність (С. Бенн, Е. Блюштейн, Л. Хенкін); 6) прайвесі як інтимність (Т. Джереті, Д. Фарбер, Дж. Рейчелс). [1; с. 537].

Право на приватність було закріплене як в універсальних, так і в регіональних міжнародних договорах. Зокрема, відповідно до ст. 12 Загальної декларації прав людини, ніхто не може зазнавати безпідставного втручання в його особисте та сімейне життя, посягань на недоторканність його житла, таємницю листування та кореспонденції, а також на його честь і репутацію. Кожна особа має право на захист від такого втручання або посягання відповідно до закону [2].

Міжнародний пакт про громадянські і політичні права (ст. 17) проголошує: «1. Ніхто не повинен зазнавати свавільного або незаконного втручання в його особисте та сімейне життя, свавільних чи незаконних посягань на недоторканність його житла, таємницю кореспонденції чи незаконних посягань на його честь і репутацію. 2. Кожна особа має право на захист від такого втручання чи посягань відповідно до закону» [3].

Конвенція про захист прав людини і основоположних свобод 1950 року (ЄКПЛ) у статті 8 формулює право таким чином: «1. Кожна особа має право на повагу до свого приватного і сімейного життя, житла та кореспонденції. 2. Органи державної влади не можуть втручатись у реалізацію цього права, за винятком випадків, коли втручання є законним і необхідним у демократичному суспільстві для забезпечення національної та громадської безпеки, економічного добробуту, запобігання заворушенням чи злочинам, захисту здоров'я або моралі, а також для захисту прав і свобод інших осіб» [4].

Хартія основних прав Європейського Союзу 2000 року у ст. 7 проголошує право на повагу до приватного і сімейного життя, недоторканність житла і таємницю кореспонденції, що фактично збігається з формулюванням ст. 8 ЄКПЛ. Важливою новацією Хартії є стаття 8, яка конкретно захищає персональні дані, підтверджуючи, що основою права на приватність є питання здобуття та поширення інформації про особу [5].

У Конституції України право на приватність регулюється кількома статтями (28, 30–32). Зокрема, ст. 28 гарантує, що ніхто не може бути підданий медичним, науковим чи іншим експериментам без добровільної згоди, захищаючи фізичну приватність. Ст. 30 забезпечує недоторканність житла, що стосується територіальної приватності. Ст. 31 охороняє таємницю листування, телефонних розмов, телеграфної та іншої комунікації, захищаючи комунікаційну приватність. А ст. 32 забороняє збір, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, охоплюючи інформаційну приватність [6].

Основною серед цих статтей є ст. 32 Конституції України, яка в ч. 1 визначає, що ніхто не може зазнавати втручання в його особисте та сімейне життя, за винятком випадків, передбачених Конституцією. Друга частина цієї статті забороняє збір, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, за винятком ситуацій, визначених законом, і лише в інтересах національної безпеки, економічного добробуту або захисту прав людини.

У Рішенні Конституційного Суду України № 2-рп/2012 від 20.01.2012 зазначено, що «право на приватне та сімейне життя є основною цінністю, яка необхідна для повного розвитку особистості в демократичному суспільстві, і розглядається як право фізичної особи на незалежне існування, не залежно від держави, органів місцевого самоврядування, юридичних та фізичних осіб» (п. 3.1) [7].

Варто зазначити, що в Національній стратегії у сфері прав людини (далі – Стратегія) право на приватність розглядається вужче, ніж це трактують Конституційний Суд України, Парламентська Асамблея Ради Європи та ЄСПЛ. Це суперечить заявленій стратегічній меті щодо «забезпечення встановлених стандартів захисту права на приватність», оскільки її формулювання не уточнює, хто саме визначає ці стандарти [8].

У зв'язку з розвитком технологій в Україні запроваджено заходи щодо захисту даних у кіберпросторі, зокрема контроль за діяльністю операторів мобільного зв'язку, інтернет-провайдерів та

соціальних платформ. З початком російської агресії питання захисту приватного життя в Україні набули нових аспектів.

В Україні запроваджуються нові програми моніторингу та безпеки, для захисту країни, які також потребують балансу між національною безпекою та правами громадян. Як приклад, можна навести створення Ситуаційного центру у місті Харкові, який був ініційований Харківською міською радою у співпраці з Агентством США з міжнародного розвитку (USAID), а підтримку в його реалізації забезпечив Kharkiv IT Cluster. Це інноваційний проєкт, спрямований на модернізацію системи оповіщення та реагування у надзвичайних ситуаціях. В умовах постійних обстрілів міста Харкова швидке реагування на будь-які загрози набуває критичного значення. Ситуаційний центр працює цілодобово, забезпечуючи оперативне інформування населення про потенційні небезпеки. Він розпочав свою роботу навесні 2024 року і одним із головних елементів проєкту є комплексна модернізація системи оповіщення населення про потенційні ракетні удари, що включає технічне розмежування сигналів оповіщення і оптимізує роботу служб, скорочує кількість тривог у місті.

Ситуаційний центр, що займається моніторингом і реагуванням на надзвичайні ситуації теж може потенційно порушувати право на приватність. Наприклад, у разі недосконалості системи кібербезпеки або недбалого поводження з інформацією, конфіденційність особистих даних може бути порушена або якщо громадськість не має доступу до інформації про те, які дані збираються, як вони використовуються і хто має до них доступ, також підвищує ризик зловживань.

Для мінімізації цих ризиків, на нашу думку важливо, щоб діяльність Ситуаційного центру регулювалася прозорими нормативно-правовими актами, а доступ до даних був обмежений чіткими правилами, відповідно до законодавства про захист персональних даних, такого, наприклад, як GDPR у ЄС або Законом «Про захист персональних даних».

Інші країни теж сьогодні стикаються з такою проблематикою. У США такі технологічні гіганти, як Google та Facebook, активно застосовують штучний інтелект для обробки даних користувачів, що породжує дискусії про захист приватності та потребує регулювання як з боку самих компаній, так і державних органів. Суспільство дедалі більше усвідомлює важливість збереження конфіденційності та ризики, які виникають у разі її порушення. Використання персональних даних у комерційних чи державних цілях викликає етичні запитання щодо меж допустимого і непорушного.

У Китаї, на відміну від США, держава активно застосовує штучний інтелект для контролю за населенням, зокрема через систему соціального кредиту. У країні діють закони, що надають уряду широкі повноваження у зборі та обробці даних, часто без врахування принципів приватності. Яскравим прикладом є китайська компанія ByteDance, яка володіє соціальною мережею TikTok — однією з найпопулярніших платформ, зокрема і в Україні. TikTok активно використовує штучний інтелект для обробки даних користувачів, що створює загрози для приватності. Серед таких ризиків: аналіз переглядів, лайків, коментарів і пошукових запитів користувачів для створення персоналізованої стрічки відео; зберігання й обробка даних, зокрема місцезнаходження, контактів, інформації про пристрої та інших метаданих, які використовуються для формування детальних профілів користувачів; застосування технології розпізнавання облич для фільтрів та ефектів у відео, що надає доступ до біометричних даних користувачів.

24 квітня 2024 року президент США Джо Байден підписав законопроєкт, який зобов'язує китайську компанію ByteDance продати TikTok, інакше цю соціальну мережу буде заборонено на території США. Це рішення було ухвалене через побоювання щодо національної безпеки, захисту приватності користувачів, а також через політичні та економічні фактори. На нашу думку, Україні також варто обмежити використання TikTok, адже Китай є союзником держави, яка здійснює агресію проти України. Існує ризик, що приватна інформація українських користувачів цієї платформи може потрапити до рук держави-агресора.

Зростаюча глобалізація потребує гармонізованих підходів до захисту приватності на міжнародному рівні. Прийняття таких нормативних актів, як GDPR [9] і Закон про штучний інтелект [10] у Європі, а також CCPA і CPRA [11] у Каліфорнії, підкреслює значущість захисту персональних даних і права на конфіденційність.

GDPR визначає правила збору, обробки та зберігання персональних даних у країнах ЄС і встановлює високі стандарти захисту приватності. Наприклад, компанія Clearview AI, яка розробляє програмне забезпечення для розпізнавання облич, була оштрафована у п'яти країнах за використання персональних даних без згоди користувачів. Французький регулятор (CNIL) заявив, що дії

Clearview AI порушують GDPR, оскільки особиста інформація використовувалася без законних підстав і згоди осіб. GDPR забезпечує високий рівень захисту даних, які застосовуються в роботі штучного інтелекту. Для інтеграції ШІ із вимогами GDPR необхідно дотримуватися принципів законності, прозорості, отримання згоди, обмеження обробки даних та інших положень регламенту. Це вимагає розробки алгоритмів і технологій, що враховують ці принципи, та відповідального використання ШІ згідно з правилами GDPR.

13 березня 2024 року Європейський парламент ухвалив перший у світі Закон про штучний інтелект. Головна мета цього документа – забезпечити захист прав і свобод осіб, на яких впливають технології ШІ. Закон визначає принципи й правила обробки персональних даних, використання систем автоматизованого прийняття рішень та інших аспектів штучного інтелекту, наголошуючи на прозорості, справедливості та законності цих процесів. Особливий акцент зроблено на захисті приватності та персональних даних, включаючи заборону систем біометричної категоризації та розпізнавання емоцій. Закон також надає громадянам право подавати скарги на роботу систем ШІ та вимагати пояснень щодо рішень, які впливають на їхні права.

Ухвалення цього Закону матиме вплив і на регулювання штучного інтелекту в Україні, оскільки країни-кандидати на вступ до ЄС, включно з Україною, будуть зобов'язані адаптувати своє законодавство до цих норм. Україна вже розпочала підготовку до імплементації цього Закону. Зокрема, торік уряд України ухвалив рішення про створення регуляторної «пісочниці» (sandbox) для розробників штучного інтелекту. Це контрольоване середовище, у якому компанії-розробники зможуть створювати свої продукти відповідно до стандартів європейського законодавства.

2 грудня 2020 року була затверджена Концепція розвитку штучного інтелекту, в якій визначено ключові пріоритети, серед яких основним було створення національного Етичного кодексу для штучного інтелекту [12]. У вересні 2022 року Європейська комісія та Україна підписали угоду про приєднання до програми «Цифрова Європа», що відкриває можливості для отримання фінансування та підтримки з метою поширення використання технологій штучного інтелекту в різних сферах, зокрема в правозастосуванні.

Підсумовуючи викладене, вважаємо, що Закон України «Про захист персональних даних» потребує доповнення такими положеннями: чітке визначення штучного інтелекту, приватності персональних даних та інших ключових понять; вимоги щодо прозорості та підзвітності алгоритмів ШІ; забезпечення інформованої згоди користувачів на обробку їх персональних даних системами ШІ; механізми для відкликання згоди та видалення персональних даних; обмеження доступу до персональних даних і визначення чітких умов їх використання; гарантії прав громадян на доступ до своїх даних, їх корекцію, видалення та перенесення; право отримувати інформацію про автоматизовані рішення, прийняті за допомогою ШІ; створення спеціалізованого державного органу для нагляду за використанням ШІ та захистом приватності; відповідальність та санкції за порушення законодавства про захист приватності у контексті застосування ШІ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Серьогін В.О. Право на недоторканність приватного життя у конституційно-правовій теорії та практиці: монографія. Х.: ФІНН, 2010. 608 с.
2. Загальна декларація прав людини. URL: http://zakon2.rada.gov.ua/laws/show/995_015 (дата звернення 12.12.2024).
3. Міжнародний пакт про громадянські і політичні права. URL: http://zakon2.rada.gov.ua/laws/show/995043 (дата звернення 12.12.2024).
4. Конвенція про захист прав людини і основоположних свобод. URL: http://zakon3.rada.gov.ua/laws/show/995_004 (дата звернення 12.12.2024).
5. Charter of Fundamental Rights of the European Union, 2000. URL: https://www.europarl.europa.eu/charter/pdf/text_en.pdf (дата звернення 12.12.2024).
6. Конституція України від 28.06.1996 р. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-D0%B2%D1%80#Text (дата звернення 12.12.2024).
7. Рішення Конституційного Суду України від 20.01.2012 р. № 2-рп/2012. *Офіційний вісник України***.** 2012. № 9. Ст. 332.
8. Національна стратегія у сфері прав людини. Затверджено Указом Президента України від 25 серпня 2015 р. № 501/2015. *Урядовий кур'єр***.** 2015. № 160.

9. Загальний регламент про захист даних (GDPR). 10.01.2002. URL: https://gdpr-text.com/uk/ (дата звернення 12.12.2024).
10. Artificial Intelligence Act. European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 C9-0146/2021 2021/0106(COD)). URL: https://www.europarl. europa.eu/doceo/document/TA-9-2024-0138_EN.pdf (дата звернення 12.12.2024).
11. CALIFORNIA CONSUMER PRIVACY ACT OF 2018. effective 1/1/2024 – AB 947 and AB 1194 updates posted to cppa.ca.gov April 2024. URL: Law & Regulations – California Privacy Protection Agency (CPPA) (дата звернення 12.12.2024).
12. Про схвалення Концепції розвитку штучного інтелекту в Україні: розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (дата звернення 12.12.2024).