СЛОВО МОЛОДОМУ НАУКОВЦЮ

Переможці конкурсу на кращу наукову роботу студентів, аспірантів, молодих та провідних вчених України на тему:
«Технології & Право» 2024[1]

ПЕРШЕ МІСЦЕ

Куліш Марія
студентка 2-го курсу Навчально-наукового інституту права Сумського державного університету

Науковий керівник: Михайловська Євгенія
докторка філософії права (PhD), заступниця завідувача кафедри адміністративного, господарського права та фінансово-економічної безпеки Навчально-наукового інституту права Сумського державного університету

УДК 347
https://doi.org/10.69724/2786-8834-2025-4-1-201-204

ЦИФРОВА ПРИВАТНІСТЬ В УМОВАХ МАСОВОГО СПОСТЕРЕЖЕННЯ: ПРАВОВІ ТА ЕТИЧНІ АСПЕКТИ

Kulish Maria. Digital Privacy in the Context of Mass Surveillance: Legal and Ethical Aspects

Сучасні технології, зокрема інтернет, мобільні додатки та соціальні мережі, опрацьовують великі масиви даних та аналізують значні обсяги інформації про користувачів, що створює серйозні виклики для захисту права на приватність і цифрових прав. Суперечність між національною безпекою та правом на приватність є однією з основних проблем сучасності, і дискусії щодо балансу між безпекою та приватністю стають дедалі актуальнішими на тлі терористичних загроз. Важливо знайти такий баланс, що дасть змогу забезпечити національну безпеку, одночасно дотримуючись права людини на приватність.

Правові аспекти цифрової приватності охоплюють захист персональних даних, право на інформовану згоду, право на забуття, конфіденційність у комунікаціях, цифрові права і свободи, а також кібербезпеку.

[1] Роботи оформлені відповідно до Вимог конкурсу на кращу наукову роботу студентів, аспірантів, молодих та провідних вчених України на тему «Технології & Право» 2024.

Цифрові технології стали невід'ємною частиною сучасного життя, що призвело до нових викликів у сфері захисту приватності. Міжнародне право відіграє визначальну роль у регулюванні цих питань, забезпечуючи захист прав людини в цифровому середовищі. Зокрема, ст. 12 Загальної декларації прав людини та ст. 17 Міжнародного пакту про громадянські і політичні права гарантують право на приватність, захищаючи особу від втручання в її особисте життя [3; 4].

Конвенція про кіберзлочинність, відома як Будапештська конвенція, є першим міжнародним договором для боротьби з кіберзлочинами. Вона встановлює стандарти для захисту даних і приватності, сприяючи співпраці між державами [5].

Національні закони, як-от GDPR в ЄС, визначають принципи захисту даних, включаючи законність, прозорість і конфіденційність. Водночас закони про національну безпеку, такі як Закон PATRIOT у США, викликають суперечки через їхній вплив на приватність [6; 7].

Регулювання цифрової приватності в країнах СНД має свої специфічні особливості. У деяких із цих країн законодавство надає державним органам широкі повноваження для моніторингу, що може порушувати права людини [8].

В Україні, натомість, розробляються закони, спрямовані на захист цифрових прав, включаючи право на приватність та доступ до інформації, розвивається співпраця з міжнародними організаціями для покращення законодавчих стандартів, Україна бере участь у різних проєктах Ради Європи, спрямованих на підвищення рівня захисту персональних даних та цифрових прав громадян.

Етичні аспекти масового спостереження є складними та викликають багато дискусій. Одним із ключових питань є інформована згода: «чи усвідомлюють люди, які дані збираються та як вони використовуються?» Прозорість у цьому контексті має важливе значення, адже дає змогу приймати обґрунтовані рішення щодо захисту приватності.

Принцип пропорційності передбачає, що спостереження має відповідати рівню загрози. Надмірний контроль може призводити до порушень прав громадян та їхньої приватності. Приклади, такі як програма PRISM у США або системи спостереження в Китаї, демонструють зловживання технологіями з метою контролю та порушення прав людини.

Штучний інтелект може посилювати дискримінацію через алгоритмічні упередження, що робить технології ще більш етично спірними. Отже, потрібно враховувати прозорість, пропорційність і запобігання зловживанням при впровадженні масового спостереження, щоб зберегти баланс між безпекою та правами людини.

Технологічні засоби захисту цифрової приватності включають шифрування даних та VPN. Шифрування перетворює дані у формат, який можна прочитати лише за допомогою спеціального ключа, що захищає інформацію від зловмисників. VPN створює зашифрований канал передачі даних між користувачем і сервером, приховуючи IP-адресу та забезпечуючи анонімність в інтернеті. Анонімні мережі, такі як Tor, також допомагають підвищити безпеку в мережі. Tor маршрутизує трафік

через серію серверів, додаючи шари шифрування, що ускладнює відстеження користувача. Інші інструменти, такі як анонімні проксі-сервери та приватні браузери, також сприяють захисту особистих даних [9].

Штучний інтелект та великі бази даних створюють нові можливості, водночас підвищують ризики для приватності. Алгоритми ШІ можуть обробляти величезні обсяги персональних даних, що загрожує витоками або неправильним використанням інформації. Тому важливо впроваджувати шифрування, анонімізацію та дотримуватись етичних стандартів задля мінімізації ризиків [11; 12].

Приватні технологічні компанії, такі як Google, Facebook і Amazon, відіграють важливу роль у захисті або порушенні приватності користувачів. З одного боку, вони використовують технології захисту, як-от шифрування і багатофакторну аутентифікацію, але з іншого, їхні бізнес-моделі передбачають збір і аналіз великих обсягів персональних даних, що може призводити до порушень приватності, як це сталося у випадках з витоками даних у Facebook.

Шифрування, VPN та анонімні мережі є важливими для захисту цифрової приватності, але з розвитком штучного інтелекту та великих баз даних необхідно постійно вдосконалювати методи захисту інформації та дотримуватися етичних норм. Технологічні компанії мають не тільки нести відповідальність за захист персональних даних своїх користувачів, а й бути підзвітними за будь-які порушення права на приватність та конфіденційність.

Цифрова приватність в умовах масового спостереження є складною і багатогранною проблемою, що потребує ретельного аналізу як правових, так і етичних аспектів. Сучасні технології дають безпрецедентні можливості для збору та опрацювання даних, що, з одного боку, сприяє зміцненню безпеки, а з іншого, навпаки, загрожує правам людей на приватність та конфіденційність.

Для забезпечення цифрової приватності в умовах масового спостереження важливо досягти балансу між безпекою та захистом прав людини. Потрібно впроваджувати прозорі та пропорційні заходи спостереження, забезпечувати інформовану згоду користувачів і уникати зловживання технологіями. Водночас важливо враховувати етичні виклики, зокрема ризики алгоритмічної дискримінації та неправильного використання даних, і розробляти правові механізми, що дозволять ефективно захищати приватність у цифрову епоху.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Романова А., Русаль Л. Етичні норми та свобода людини у праві: інтегративний аспект. *Вісник Національного університету «Львівська політехніка». Серія: «Юридичні науки»*. 2020. №4(28). С. 89–93. http://doi.org/10.23939/law2020.28.089
2. Петришин О. В., Гиляка О. С. Права людини у цифрову епоху : виклики, загрози та перспективи. *Вісник Національної академії правових наук України*. 2021. Т. 28, №1. С. 7–35. http://doi.org/10.31359/1993-0909-2021-28-1-17

3. Загальна декларація прав людини від 10.12.1948. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text (дата звернення: 10.10.2024).
4. Міжнародний пакт про громадянські і політичні права від 16.12.1966. URL: https://zakon.rada.gov.ua/laws/ show/995_043#Text (дата звернення: 10.10.2024).
5. Конвенція про кіберзлочинність від 23.11.2001. URL: https://zakon.rada.gov.ua/laws/show/994_575# Text (дата звернення:10.10.2024).
6. 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, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) від 27.04.2016 № 2016/679. URL: https://zakon.rada.gov.ua/ laws/show/984_008-16#Text (дата звернення: 10.10.2024).
7. USA Patriot Act (назва з екрану). URL: https://www.fincen.gov/resources/ statutes-regula tions/usa-patriot-act (дата звернення: 10.10.2024).
8. Братасюк О. Б., Ментух Н. Ф. Поняття та класифікація цифрових прав в Україні. *Юридичний науковий електронний журнал*. 2021. №10. С. 58–61. https://doi.org/10.32782/2524-0374/2021-10/12
9. Для чого потрібен Tor Browser (назва з екрану). URL: https://foxminded. ua/shcho-take-tor/ (дата звернення: 10.10.2024).
10. Що таке VPN, і як ним безпечно користуватись (назва з екрану). URL: https://csirt.csi.cip.gov.ua/uk/posts/what-is-a-vpn-and-how-to-use-it-safely (дата звернення: 10.10.2024).
11. AI Risk: як штучний інтелект формує нові горизонти корпоративної безпеки (назва з екрану). URL: https://blog.liga.net/user/ishevtsov/article/54473 (дата звернення: 10.10.2024).
12. Бєлова М. В., Бєлов Д. М. Виклики та загрози захисту персональних даних у роботі зі штучним інтелектом. *Науковий вісник Ужгородського національного університету*. 2023. Т. 2, №79. С. 17–22. https://doi.org/10.24144/2307-3322.2023.79.2.2