

РЕГУЛЮВАННЯ ПЕРСОНАЛЬНИХ ДАНИХ В УКРАЇНІ: НОВІ ВИКЛИКИ ТА ПЕРСПЕКТИВИ В УМОВАХ ЦИФРОВИХ ТЕХНОЛОГІЙ

Стрімкий розвиток цифрових технологій, зростання обсягів обробки персональних даних та активне впровадження електронних сервісів в Україні актуалізують потребу у сучасному та ефективному правовому регулюванні цієї сфери. В умовах цифрової трансформації держави, розвитку е-урядування, електронної комерції, хмарних сервісів, штучного інтелекту та великих даних значно розширюються ризики втручання у приватне життя, несанкціонованого доступу до інформації про особу та зловживань із боку як приватних компаній, так і державних органів.

Водночас українська правова система перебуває на етапі гармонізації із стандартами ЄС, зокрема з положеннями GDPR, що зумовлює необхідність оновлення національного законодавства, удосконалення механізмів контролю та відповідальності, а також формування культури захисту персональних даних у суспільстві. Нові цифрові інструменти створюють низку викликів — від забезпечення кібербезпеки до урегулювання алгоритмічної обробки інформації та автоматизованого прийняття рішень.

Таким чином, дослідження проблем і перспектив регулювання персональних даних в Україні є надзвичайно актуальним, адже воно дозволяє визначити прогалини чинного законодавства, оцінити ризики цифрового середовища та запропонувати шляхи вдосконалення правових механізмів захисту прав і свобод людини.

Метою дослідження є всебічний аналіз сучасного стану правового регулювання персональних даних в Україні в умовах цифрових технологій, виявлення ключових викликів та ризиків, а також визначення перспектив і напрямів удосконалення національного законодавства з урахуванням міжнародних стандартів та європейських практик. Для досягнення вказаної мети слід буде виконати наступні завдання:

- проаналізувати сучасний стан правового регулювання персональних даних в Україні та визначити його відповідність міжнародним стандартам, зокрема вимогам GDPR;

- виявити основні виклики та загрози, пов'язані з обробкою персональних даних у цифровому середовищі (вплив штучного інтелекту, великих даних, онлайн-платформ, електронних сервісів тощо);

- окреслити ключові проблеми у сфері забезпечення права на приватність, включно з прогалинами законодавства, недоліками механізмів контролю та відповідальності;

- дослідити особливості функціонування системи захисту персональних даних в Україні в умовах цифрової трансформації та розвитку е-урядування;

- проаналізувати європейські та міжнародні практики регулювання персональних даних для виявлення можливостей їх імплементації в українське законодавство;

- запропонувати напрями вдосконалення національної системи захисту персональних даних, включно з правовими, організаційними та технологічними заходами.

Здійснюючи аналіз сучасного стану правового регулювання персональних даних в Україні слід зазначити, що національне законодавство у даній сфері перебуває у процесі модернізації та поступового наближення до європейських стандартів. Закон України «Про захист персональних даних» від 01.06.2010 року [1] залишається базовим актом, однак його норми значною мірою потребують оновлення у зв'язку зі зміною технологічного середовища, збільшенням масштабів цифрових сервісів та новими моделями обробки інформації. Чинні механізми контролю та відповідальності, на думку багатьох вчених, не повною мірою забезпечують ефективний захист прав суб'єктів даних.

Ідентифікація основних викликів та загроз, пов'язаних із цифровізацією, демонструє, що стрімке впровадження новітніх технологій значно ускладнює забезпечення належного рівня захисту персональних даних. Передусім, широке використання штучного інтелекту та алгоритмічної обробки даних створює ризики автоматизованого збирання, аналізу та профілювання осіб без їх поінформованої згоди. Алгоритми здатні обробляти великі масиви інформації, встановлювати кореляції та прогнозувати поведінку суб'єктів даних, що відкриває можливості для дискримінаційних рішень, маніпуляцій і непрозорого використання даних у комерційних або політичних цілях.

Зростання популярності хмарних платформ, на яких дуже часто зберігаються персональні та чутливі дані, посилює ризики несанкціонованого доступу через кібератаки, недоліки налаштування безпеки або передачу даних третім сторонам. У свою чергу, масштабування технологій Big Data дозволяє об'єднувати дані з різних джерел, що збільшує ризики ідентифікації осіб навіть тоді, коли інформацію подано у знеособленому вигляді.

Не менш проблемним є стрімке поширення мобільних застосунків, які збирають надмірні обсяги інформації: геолокацію, контакти, дані про активність користувачів, медійні файли тощо. Часто користувачі навіть не усвідомлюють, які саме дані збираються та з якою метою.

Використання біометричної ідентифікації (відбитки пальців, розпізнавання обличчя, голосу, райдужної оболонки ока) створює особливо високі ризики, адже біометричні дані є унікальними та незмінними. Їх витік або маніпулятивне використання може спричинити серйозне порушення приватності та загрозу безпеці особи.

Поширення систем відеоспостереження та технологій розпізнавання облич у публічних просторах формує ризик масового контролю та стеження без належного правового балансу між безпекою і приватністю. Крім того, значний масив персональних даних накопичується у державних реєстрах, які нерідко стають об'єктами кібератак чи внутрішніх зловживань. Концентрація інформації про громадян у цифрових системах держави збільшує кількість потенційних векторів доступу та можливостей для неправомірної обробки.

Усі зазначені виклики засвідчують, що сучасні технологічні процеси потребують комплексних і системних правових гарантій, включно з удосконаленням законодавства, посиленням контролю за обробкою даних, прозорістю алгоритмів, підвищенням стандартів кібербезпеки та чітким регламентуванням практик цифрової взаємодії. Без адаптації правових механізмів до нових технологічних реалій неможливо забезпечити належний захист прав людини на приватність у цифровому суспільстві.

Зазначені вище виклики та загрози дозволяють окреслити головні проблеми у забезпеченні права на приватність та виділити низку системних прогалин. Йдеться, перш за все, про нестачу спеціальних норм щодо обробки даних алгоритмами штучного інтелекту, недостатню захищеність електронних реєстрів, неврегульованість багатьох практик цифрової комунікації, низький рівень цифрової обізнаності населення та слабку інституційну спроможність уповноваженого органу. І, нарешті, наявні санкції та механізми контролю не завжди є ефективними для цифрової економіки.

Дослідження функціонування системи захисту персональних даних в умовах цифрової трансформації показує, що активне впровадження е-урядування та цифрових державних сервісів з одного боку полегшує доступ громадян до адміністративних послуг, але з іншого — концентрує великі масиви персональної інформації в одних інформаційних системах, що підвищує ризики неправомірного доступу. Формування цифрової держави потребує нових підходів до безпеки, а також прозорих, чітко регламентованих процедур обробки даних.

Аналіз міжнародних та європейських практик регулювання, насамперед Загального регламенту про захист даних (англ. *General Data Protection Regulation*, GDPR; Regulation (EU) 2016/679)[2], свідчить про важливість принципів мінімізації даних, прозорості обробки, забезпечення права на переносимість, стирання та обмеження обробки. Значний потенціал для України становить імплементація підходів щодо оцінки впливу на захист даних Data Protection Impact Assessment (DPIA), посилення наглядових повноважень та відповідальності операторів і процесорів даних. Аналіз впровадження на практиці зазначених документів дозволяє стверджувати, що європейська практика демонструє ефективність поєднання правових, організаційних та технічних стандартів.

Розроблення пропозицій щодо вдосконалення системи захисту персональних даних в Україні вимагає комплексного підходу: оновлення законодавства відповідно до стандартів ЄС, запровадження єдиних правил щодо алгоритмічної обробки та використання штучного інтелекту, посилення кібербезпеки реєстрів, створення сучасних інструментів моніторингу та аудиту обробки даних. Важливо також підвищувати цифрову грамотність громадян, формувати культуру захисту приватності та зміцнювати інституційні можливості державних органів, відповідальних за захист персональних даних.

Отож, проведене дослідження засвідчує, що в умовах стрімкої цифровізації суспільства питання захисту персональних даних набуває ключового значення як для національної безпеки, так і для забезпечення фундаментальних прав людини. Аналіз чинного законодавства та сучасних практик обробки даних показав, що українська система захисту персональних даних перебуває у стані активної трансформації і потребує всебічного оновлення з урахуванням викликів, які породжують штучний інтелект, великі дані, хмарні технології, біометричні системи та цифрові державні сервіси.

Виявлені виклики — від непрозорої алгоритмічної обробки до загроз кібератак і витоків інформації — підтверджують необхідність суттєвого посилення правових та технічних гарантій. Значні обсяги персональних даних, що накопичуються як у приватному секторі, так і в державних реєстрах, створюють підвищений ризик зловживань, особливо за умови недостатньої

інституційної спроможності органів контролю та прогалин у законодавстві.

Європейський досвід, насамперед стандарти GDPR, демонструє ефективність комплексного підходу, що поєднує чіткі правові норми, організаційні процедури та сучасні технічні механізми захисту. Імплементация таких підходів в Україні є важливою умовою підвищення рівня безпеки обробки даних, а також кроком до зміцнення довіри громадян до цифрової держави.

Здійснений аналіз дозволяє дійти висновку, що для ефективного захисту персональних даних Україні необхідно: оновити законодавство відповідно до європейських вимог; встановити чіткі правила алгоритмічної обробки даних; посилити кібербезпеку державних реєстрів; удосконалити нагляд і відповідальність суб'єктів обробки; забезпечити прозорість цифрових процесів; а також сприяти формуванню культури приватності серед громадян.

Таким чином, модернізація системи захисту персональних даних має здійснюватися комплексно — на законодавчому, інституційному, технічному й освітньому рівнях. Лише за умов системного підходу можливе створення безпечного, правового та людиноцентричного цифрового середовища, здатного забезпечити належний рівень захисту прав і свобод особи в сучасну епоху технологічних трансформацій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI. Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481
2. Загальний регламент про захист даних (англ. *General Data Protection Regulation*, GDPR; Regulation (EU) 2016/679). <https://www.gdpr.org.ua/>
3. Data Protection Impact Assessment (DPIA). <https://legalaid.ua/ua/data-protection-impact/>