Савка С.
студентка юридичного факультету
Західноукраїнського національного університету.
Науковий керівник: доктор юридичних наук, доцент,
професор кафедри теорії права та конституціоналізму
Західноукраїнського національного університету
Колесніков А. П.

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В УМОВАХ ЦИФРОВІЗАЦІЇ СУСПІЛЬСТВА: КРИМІНАЛЬНО-ПРАВОВИЙ АСПЕКТ

Стрімкий развитие інформаційних технологій, глобальна цифровізація суспільних відносин та масштабне впровадження систем штучного інтелекту докорінно змінили архітектуру взаємодії між державою, суспільством та особою. Переведення більшості сфер життєдіяльності у віртуальний простір зумовило не лише оптимізацію управлінських та побутових процесів, а й виникнення принципово нових, високотехнологічних загроз для фундаментальних прав людини. Серед них особливе місце посідає право на недоторканність приватного життя, яке в умовах цифрової трансформації трансформувалося у критичну потребу забезпечення надійного захисту персональних даних. Масовий збір, автоматизована обробка, систематизація та зберігання колосальних масивів інформації про особу (Big Data) створюють сприятливе підґрунтя для зловживань та протиправних посягань, що вимагає своєчасного, системного та ефективного кримінально-правового реагування.

Традиційні інструменти забезпечення інформаційної безпеки та цивільно-правової чи адміністративної відповідальності за порушення законодавства про захист персональних даних у сучасних реаліях часто виявляються недостатніми та неефективними. Масштабність витоків конфіденційної інформації, поява тіньових ринків купівлі-продажу баз даних (так званого «даркнету»), використання технологій соціальної інженерії та фішингу для несанкціонованого доступу до приватних профілів громадян свідчать про високий рівень суспільної небезпеки цих діянь. Кримінально-правовий аспект захисту персональних даних полягає у необхідності чіткої кваліфікації новітніх форм злочинних посягань, модернізації диспозицій існуючих норм Кримінального кодексу України та розробки дієвих механізмів розслідування кіберзлочинів, що пов’язані з незаконним обігом інформації з обмеженим доступом.

Основним матеріально-правовим підґрунтям захисту інформаційних прав особи в Україні є стаття 32 Конституції України, яка прямо забороняє збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім визначених законом випадків в інтересах національної безпеки,

економічного добробуту та прав людини. Ця конституційна гарантія кореспондує з міжнародними стандартами, зокрема з Конвенцією про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція 108) та Загальним регламентом про захист даних Європейського Союзу (GDPR), які визначають персональні дані як будь-яку інформацію, що дає змогу прямо чи опосередковано ідентифікувати фізичну особу. У кримінально-правовому контексті суспільна небезпека порушення цих положень полягає у підриві довіри громадян до цифрових державних та приватних інститутів, а також у створенні реальних ризиків для їхньої майнової та особистої безпеки.

Чинний Кримінальний кодекс України містить низку статей, покликаних забезпечувати охорону інформаційної сфери. Ключовою у контексті досліджуваної проблеми є стаття 182, яка передбачає відповідальність за порушення недоторканності приватного життя, а саме за незаконне збирання, зберігання, використання, знищення чи поширення конфіденційної інформації про особу. Разом із тим, практична реалізація цієї норми стикається з серйозними теоретичними та прикладними проблемами. Специфіка цифрового середовища полягає в тому, що персональні дані часто виступають не лише безпосереднім об'єктом злочину, а й засобом або інструментом для вчинення інших кримінальних правопорушень, таких як шахрайство (стаття 190), несанкціоноване втручання в роботу інформаційних систем (стаття 361) або викрадення грошових коштів з банківських рахунків.

Однією з найгостріших проблем сучасного кримінального права є бланкетний характер більшості норм, що регулюють відповідальність за кіберзлочини та порушення інформаційної безпеки. Диспозиція статті 182 КК України відсилає правоохоронця до регуляторного законодавства, зокрема до Закону України «Про захист персональних даних». Проте понятійно-категоріальний апарат кримінального закону суттєво відстає від темпів технологічного прогресу. Наприклад, такі поняття, як «цифровий слід»,

«метадані», «біометрична ідентифікація», «динамічна IP-адреса» або

«профайлінг», які активно використовуються у сфері інформаційних технологій і можуть містити критично важливі персональні дані, досі не мають чіткого відображення та правової оцінки у кримінально-правовій доктрині України. Це створює труднощі при визначенні предмету злочину та встановленні меж кримінальної відповідальності.

Окремої уваги заслуговує аналіз суб'єктивної сторони та суб'єкта досліджуваних злочинів. Особливу суспільну небезпеку становлять правопорушення, вчинені службовими особами або володільцями (розпорядниками) баз персональних даних, які мають легальний доступ до конфіденційної інформації громадян (співробітники банків,

мобільних операторів, державних реєстраційних органів тощо). Продаж або передача таких відомостей третім особам із корисливих мотивів має кваліфікуватися за сукупністю злочинів, включаючи зловживання владою або службовим становищем та несанкціонований збут інформації з обмеженим доступом (стаття 361-2 КК України). В умовах воєнного стану та підвищених гібридних загроз такі дії набувають ознак загрози національній безпеці, оскільки бази даних військовослужбовців, правоохоронців чи патріотично налаштованих громадян можуть стати об'єктом інтересу ворожих спецслужб.

Транскордонний характер кіберзлочинності створює додаткові виклики для національної системи кримінальної юстиції. Злочинці, які здійснюють викрадення чи незаконну обробку персональних даних українських громадян, можуть фізично перебувати під юрисдикцією іншої держави, а сервери з викраденою інформацією — розміщуватися у «хмарних» сховищах по всьому світу. Це актуалізує питання імплементації положень Будапештської конвенції про кіберзлочинність та налагодження ефективної міжнародної співпраці у сфері взаємної правової допомоги. Важливим кроком є також гармонізація українського кримінального законодавства із європейськими стандартами кібербезпеки, що дозволить оперативно блокувати протиправний контент та притягати винних осіб до відповідальності незалежно від місця їхнього перебування.

Процесуальний аспект розслідування злочинів проти персональних даних вимагає високого рівня професійної підготовки працівників правоохоронних органів та впровадження єдиних стандартів цифрової криміналістики (digital forensics). Збір, фіксація та дослідження електронних доказів (лог-файлів, трафіку, зашифрованих дискових масивів) мають свою специфіку, оскільки такі докази є надзвичайно динамічними, вразливими до модифікації та можуть бути дистанційно знищені за лічені секунди. Необхідно на законодавчому рівні вдосконалити процедуру тимчасового доступу до речей і документів, що містять електронну інформацію, та чітко регламентувати статус цифрових доказів у кримінальному процесі, забезпечивши баланс між ефективністю розслідування та невтручанням у приватне життя добропорядних громадян.

Підсумовуючи, слід зазначити, що ефективний захист персональних даних в умовах тотальної цифровізації суспільства неможливий без комплексної модернізації кримінально-правового інструментарію. Необхідно відійти від фрагментарного регулювання та розробити цілісну стратегію кримінально-правової охорони інформаційних прав особи. Це передбачає: по-перше, уточнення та розширення термінологічного апарату Кримінального кодексу України з урахуванням новітніх технологічних реалій; по-друге, посилення кримінальної відповідальності за масовий витік та комерційну

реалізацію персональних даних, особливо якщо вони вчинені службовими особами; по-третє, підвищення кваліфікації слідчих та суддів у сфері інформаційних технологій. Тільки за умови створення гнучкого, сучасного та адаптивного правового механізму держава зможе гарантувати безпеку особи у цифровому просторі та мінімізувати ризики, що супроводжують суспільний прогрес.

Список використаних джерел

1. Конституція України від 28 червня 1996 року № 254к/96-ВР. URL: https:// zakon.rada.gov.ua/laws/show/254к/96-вр (дата звернення: 31.05.2026).
2. Кримінальний кодекс України від 05 квітня 2001 року № 2341-III. URL: ht tps://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 31.05.2026).
3. Закон України «Про захист персональних даних» від 01 червня 2010 року № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 31.05.2026).
4. Конвенція про кіберзлочинність (Будапештська конвенція) від 3 листопада 2001 року. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 31.05.2026).
5. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 4th ed. London : Academic Press, 2020. 848 p.