

ХАРАКТЕРНІ РИСИ ПРОЯВУ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

CHARACTERISTICS OF PERSONAL DATA PROTECTION

Дяковський О.С., к.ю.н.,

викладач кафедри інформаційного, господарського та адміністративного права

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Дослідження присвячене ключовим аспектам забезпечення захисту персональних даних в умовах сучасних інформаційних загроз. Розкрито концептуальні засади міжнародно-правового регулювання захисту персональних даних. Детерміновано зміст «стану захищеності персональних даних», обґрунтовано важливість дотримання правових норм та стандартів у сфері захисту даних, а також аналізуються основні методи та засоби, що застосовуються для захисту інформації. Особливу увагу приділено характеристиці типових загроз конфіденційності та методів їх запобігання, зокрема за допомогою новітніх технологій й процедур управління ризиками. Зроблено акцент на важливості дотримання загальних принципів конфіденційності, таких як законність, прозорість, цілісність, захист від несанкціонованого доступу, а також на дотриманні міжнародних стандартів. Розглянуто різні підходи до забезпечення конфіденційності та безпеки даних, включаючи організаційні і технічні заходи.

Систематизовано характерні риси захисту персональних даних. Наведено різні класифікаційні групи персональних даних, що фігурують у вітчизняному та іноземному законодавстві. Автор розглядає приклади сучасних кіберзагроз, таких як фішинг, DDoS-атаки, зломи баз даних, а також вразливості в хмарних системах, які можуть поставити під загрозу персональні дані. Обговорено рекомендації щодо побудови системи захисту персональних даних на рівні підприємств та організацій, що передбачають регулярні аудити безпеки, навчання персоналу, запровадження політик доступу до даних і управління правами користувачів. Вказано на особливе значення консолідації зусиль для досягнення стану максимальної захищеності персональних даних, що включає в себе персональну безпеку володільця даних; заходи (організаційні і правові), які впроваджує держава; діяльність громадських організацій.

Ключові слова: захист даних, персональні дані, конфіденційна інформація, кіберзагроза, міжнародні стандарти, нормативно-правове регулювання, інформація.

The study is devoted to the key aspects of personal data protection in the context of modern information threats. The conceptual foundations of international legal regulation of personal data protection are revealed. The content of the "state of personal data protection" is determined, the importance of compliance with legal norms and standards in the field of data protection is substantiated, and the main methods and means used to protect information are analyzed. Particular attention is paid to the characterization of typical privacy threats and methods of their prevention, in particular, with the help of the latest technologies and risk management procedures. Emphasis is placed on the importance of adherence to general principles of confidentiality, such as legality, transparency, integrity, protection against unauthorized access, as well as compliance with international standards. Various approaches to ensuring data confidentiality and security, including organizational and technical measures, are considered.

The characteristic features of personal data protection are systematized. Various classification groups of personal data appearing in domestic and foreign legislation are presented. The author examines examples of modern cyber threats, such as phishing, DDoS attacks, database hacking, and vulnerabilities in cloud systems that can jeopardize personal data. Recommendations for building a personal data protection system at the level of enterprises and organizations, including regular audits of personal data security, are discussed. The author emphasizes the special importance of consolidating efforts to achieve the state of maximum personal data protection, which includes personal security of the data owner; measures (organizational and legal) implemented by the State; and activities of public organizations.

Key words: data protection, personal data, confidential information, cyber threat, international standards, regulatory and legal regulation, information.

Актуальність теми. Баланс між правом людини на конфіденційність, приватність у співвідношенні із суспільними інтересами як складна проблематика завжди перебував у полі наукового інтересу. Найбільша кількість дослідницьких робіт в даному аспекті належить сфері права, адже саме в їх світлі відображається поточний стан ефективності нормотворення і правозастосування. Що найбільш досконалий підхід нормативного та організаційного забезпечення захисту персональних даних безперечно зміцнює систему інформаційних відносин, тим самим де-юре і де-факто роблячи її стійкою до внутрішніх й зовнішніх загроз.

Так, відповідно до інформації, представленої на офіційному сайті National Cybersecurity Index, у 2023 році Україна посіла 12 місце у переліку держав за рейтингом кіберзахисту [16]. Щорічне поліпшення вітчизняних позицій обумовлено очевидним покращенням цифрового і технологічного потенціалу країни на міжнародній арені. Разом з цим спостерігається збільшення кількості правопорушень у даній сфері. Усвідомлюючи потенційні загрози, спричинені такою ситуацією, для України, як демократичної держави, захист персональних даних являє собою пріоритетне питання в розрізі інформаційної політики.

На зазначеному наголошено у наукових дослідженнях таких вчених як Біла-Кисельова А. А., яка в контексті ана-

лізу міжнародного законодавства про права людини вивчає нормативно-правове забезпечення захисту персональних даних [1]. Важливу роль для теоретичного аналізу окремих положень відіграло монографічне дослідження Гужій Т. О., яке присвячено розкриттю досягнень вітчизняної юриспруденції та зарубіжного досвіду, аналізу чинного законодавства, нормотворчої та правозастосовної практики. У результаті сформовано комплекс теоретичних засад і практичних рекомендацій, спрямованих на підвищення ефективності правового регулювання та організаційного забезпечення захисту персональних даних [2]. З точки зору класифікаційних підходів, взято за основу специфіку розподілу і систематизації, запропоновану Різак М. В. [12]. Окреслення проблематики та формування пропозицій щодо врегулювання проблемних аспектів правового і організаційного забезпечення захисту персональних даних здійснювалось із урахуванням рекомендацій, наданих юристами-практиками Фісун В. [13], Панченко О. А. [8].

Мета дослідження – ідентифікувати та класифікувати основні риси захисту персональних даних, розглядаючи їх як комплексний правовий та технічний процес, який відповідає сучасним вимогам конфіденційності та безпеки інформації.

Виклад основної інформації. У міжнародно-правовій доктрині чинне місце відведено питанню забезпечення

й захисту персональних даних. Так, один із ключових документів світового масштабу – Конвенція про захист прав людини і основоположних свобод у ст. 8 фіксує, що кожен має право на повагу до приватного і сімейного життя, а також до свого житла і кореспонденції [5]. У примітках зазначено досить чіткий аналіз того, що саме має забезпечити держава задля дотримання перед людиною і громадянином зазначених прав. Зокрема, зі сторони органів публічного управління заборонено втручання у приватне і сімейне життя особи за виключенням тих випадків, коли подібного роду дії мають законне підґрунтя та є необхідним із позиції забезпечення демократичних засад і захисту національних інтересів. Більш детально механізми реалізації вказаного права фіксуються у вітчизняному законодавстві.

Так, в Україні, суспільні відносини із захисту персональних даних регулюються більше як двадцятьма різними законодавчими актами. Відповідальність за делікти у вказаній сфері закріплена у КК України [6], ЦК України [14], КУпАП [7]. Попри значну кількість нормативно-правових актів, за більш ґрунтовного аналізу їх змісту все ж виявляємо, що вони врегульовують лише окремі аспекти захисту [2, с. 64], відповідно, законодавче регулювання позбавлене комплексності і цілісного підходу. Складність практичного втілення окресленої ідеї зумовлена тим, що безпосередньо сам процес захисту персональних даних включає як правові, так і технічні аспекти, перебуває в залежності від мір і заходів, котрі вживає держава, а також особа як володілець і розпорядник персональних даних.

Так, держава є найбільшим володільцем персональних даних, тому цілком закономірно, що саме до неї висуваються щонайбільш суворі вимоги стосовно забезпечення захисту [13]. Органи публічної влади зобов'язані вживати всіх заходів, коли не передбачено надання згоди на обробку персональних даних. За таких умов, витік відомостей із державних баз даних лише посилює недовіру до управлінських інституцій зі сторони громадськості. На зазначене вказує і судова практика. До прикладу, Касаційний цивільний суд Верховного Суду України своєю постановою від 28.05.2024 по справі № 127/13877/19 задовольнив вимогу щодо видалення персональних даних АТ «Укрпошта» та зобов'язав відповідача відшкодувати збитки. При цьому, суд приходить до важливого висновку: ідентифікація особи під час надання їй послуг може здійснюватися за паспортними даними без необхідності використання засобів автоматизації. Незважаючи на те, що позивачі у цій справі не надавали згоду на обробку їхніх персональних даних та внесення до електронних баз даних, відповідач не довів, що він не здійснював такої обробки [10].

Як власне сама судова практика, так і зміст охоронної функції, що покладено на державу, апелює до потреби забезпечення стану захищеності у відношенні до персональних даних. Рівень захищеності персональних даних – це комплексний показник, який характеризує виконання вимог, котрі нейтралізують загрози безпеці інформаційних систем персональних даних [8]. У свою чергу, із правової точки зору під станом захищеності персональних даних прийнято розуміти юридично забезпечений рівень безпеки персональної інформації, при якому гарантується її конфіденційність, цілісність, доступність, а також дотримання прав суб'єктів даних щодо їх збору, обробки, зберігання та передачі. Він передбачає застосування належних організаційних та технічних заходів, спрямованих на запобігання несанкціонованому доступу, розголошенню, модифікації або знищенню персональних даних, відповідно до вимог чинного законодавства. Розглянемо ключові детермінанти такого явища:

Конфіденційність означає захист даних від несанкціонованого доступу. За умови конфіденційності доступ до персональних даних мають тільки ті особи, які наділені спеціальним правом, і лише в межах, необхідних для

виконання своїх обов'язків. Досягти такого стану можливо шляхом обмеження доступу до інформації, шифрування даних, контролю доступу через паролі, ідентифікацію та багатфакторну аутентифікацію.

Цілісність даних полягає у забезпеченні їхньої точності, повноти та актуальності. Будь-які зміни даних повинні бути санкціоновані та належно зафіксовані, щоб уникнути втрати чи спотворення інформації. Методи забезпечення цілісності включають: контроль версій даних, використання журналів змін, перевірку даних на відповідність встановленим критеріям.

Доступність даних означає, що інформація повинна бути доступною у потрібний час для уповноважених осіб. Такий підхід необхідний для забезпечення безперервності роботи організацій та надання послуг. Для підтримки доступності використовуються відповідні методи: резервне копіювання даних, розподілені системи зберігання, антивірусний захист і захист від атак типу DDoS.

Правове регулювання та відповідність. Важливою рисою захисту персональних даних є дотримання законодавства, що регулює збирання, зберігання, обробку і передачу персональних даних. Наприклад, в Україні це Закон «Про захист персональних даних» [11], у Європейському Союзі – Загальний регламент про захист даних (GDPR) [15]. Дотримання правових вимог передбачає: прозорість процесів збирання та обробки даних, інформування суб'єктів даних про їхні права, надання права на доступ до даних, їх зміну чи видалення.

Анонімізація та псевдонімізація – це методи, що допомагають зменшити ризики ідентифікації особи в разі витоку даних. Анонімізація повністю унеможливає ідентифікацію особи, тоді як псевдонімізація передбачає заміну іменних ідентифікаторів на інші, що дозволяє лише обмежене відновлення відомостей про особу при наявності спеціальних прав доступу.

Регулярний аудит і контроль заходів безпеки дозволяють вчасно виявити вразливості в системі захисту даних. Мова йде про перевірку доступів і повноважень, аналіз журналів подій, виявлення та усунення інцидентів безпеки.

Підвищення обізнаності персоналу. Захист персональних даних значною мірою залежить від обізнаності персоналу. Співробітники повинні знати, як обробляти персональні дані, дотримуватися політик конфіденційності та не допускати витоку інформації. Навчання персоналу та регулярні тренінги допомагають знизити ризик випадкових порушень.

Оцінка ризиків дозволяє ідентифікувати потенційні загрози та визначити заходи для їхнього мінімізації. Важливим є також управління інцидентами, що передбачає оперативну реакцію на будь-які порушення в системі захисту персональних даних та швидке усунення наслідків.

Безперечно, специфіка захисту персональних даних багато в чому залежить від видової групи, про яку йде мова. До прикладу, біометричні персональні дані являють собою особливу та цілком специфічну категорію персональних даних, що характеризують фізіологічні особливості людини, на підставі яких можна встановити особу. До них належать: група крові, код ДНК, відбитки пальців, малюнок сітківки ока тощо. Ідентифікацію особистості за сукупністю біометричних ознак здавна практикують у криміналістиці – досить згадати в зв'язку з цим знаменитий метод бертильйонажа, який використовувала європейська поліція на початку ХХ ст., що давав змогу ідентифікувати злочинців.

Різні класифікації персональних даних містяться і в національному законодавстві європейських країн. Наприклад, Закон Франції «Про інформатику, картотеки і свободи» виокремлює в окрему категорію медичну інформацію про особу (за винятком даних, що накопичуються з метою терапевтичного або медичного контролю над пацієнтом та з дослідницькими цілями) та в окремі

главі виділяє порядок збирання й обігу такої інформації. Диференційовано також дані про здоров'я, накопичувані та оброблювані з метою розвитку профілактичної та опікунської діяльності [3]. Згідно з угорським законодавством, в окрему категорію публічних персональних даних виділено відомості про імена і посади фізичних осіб, які діють у центральних і місцевих органах влади.

Такими чином, усі персональні дані умовно можна розділити на три основні групи: персональні дані, збирання яких, за загальним правилом, заборонено (спеціальні категорії персональних даних); персональні дані, збирання яких здійснюються на підставі чинного законодавства (різні категорії персональних даних, зокрема біометричні та спеціальні категорії персональних даних); а також персональні дані, збирання та оброблення яких дозволено за згодою суб'єкта персональних даних [12].

Враховуючи той аспект, що захист персональних даних не обмежується виключно межами конкретної країни, а зачастую набуває інтеграційного характеру, Кабінет Міністрів України своєю постановою 16.08.2022 № 910 затвердив Перелік держав, які забезпечують належний захист персональних даних [9]. Незважаючи на те, що документ носить виключно рекомендаційний характер, його прийняття передувала ґрунтовна робота із аналізу та вивчення стану дотримання законодавства про захист персональних даних у різних країнах, відповідно, це є полегшеним посібником для представників бізнесу; фізичних осіб, які задіяні у систематичному міжнародному обміні даними тощо.

Позитивним вбачаємо активність громадських спільнот у вивченні та аналізі вітчизняного онлайн ринку, який обробляє персональні дані мільйонів користувачів. Зокрема, у 2022–2023 роках ГО «Інтерньюз-Україна» дослідила 10 застосунків і 20 сайтів великих приватних компаній, з-поміж яких Rozetka, Olx, «Нова Пошта», Ukr.net, Comfy, Foxtrot, Eldorado, Prom, Citrus, Allo, Kasta, MakeUp, Zakaz.ua, Silpo, Triolan, Data Group, Lanet, Kyivstar, Lifecell, Vodafone. Серед додатків – Bolt, Liki24, Uklon, Fishka, Tabletki.ua, Meest, Glovo, «Епіцентр» та Busfor. За результатами було встановлено, що 10 ресурсів отримали низькі бали, зокрема, виходячи із показників

дотримання європейських стандартів, зручності користування ресурсом, врахування принципів інклюзивності, технологічні аспекти тощо [4, с. 4–5]. На кінці дослідження було сформовано низку рекомендацій, які дали б змогу вдосконалити політику конфіденційності вказаних ресурсів, зокрема шляхом:

- чіткої детермінації строків зберігання даних;
- спрощення інформації, відносно засад обробки персональних даних, виклавши її таким чином, щоб це було доступно для розуміння будь-якому користувачу (мінімізація канцеляризму);
- викласти дані стосовно засад збереження даних, а також географічного розташування серверів;
- зафіксувати відомості стосовно даних, котрі передаються третім особам;
- дотримуватися засад мінімізації з позиції використання виключно тих даних, котрі дійсно необхідні в процесі реалізації профільної діяльності компаніями.

Висновки. Отже, підбиваючи підсумок буде доцільно зазначити, що захист персональних даних саме в цифрову епоху поки що мало чим відрізняється від звичних юридичних способів захисту. Цифрова епоха накладає відбитки більшою мірою на їх обіг, комодифікацію та, відповідно, подальшу обробку різноманітними суб'єктами. З'являються нові способи неправомірного отримання доступу до величезних масивів персональних даних громадян, зростає кількість резонансних справ, з'являються і нові оператори, які акумулюють у себе величезні масиви даних. З високою часткою очевидності можна констатувати, що законодавство потребує оновлення, а поточних способів правового захисту недостатньо ні як превентивного заходу, ні як компенсаторного.

Однак немає жодних гарантій, що створення, наприклад, особливого *in sui generis*, юридичного способу захисту персональних даних сприятиме виправленню ситуації. Важливо розуміти, що цифрова епоха насамперед змінює саме концептуальні підходи до балансу публічних і приватних інтересів. Надавши згоду на обробку персональних даних один раз, з розвитком технологій особа має з кожним днем все менше як технологічних, так і правових можливостей для подальшого контролю за обігом власних даних.

ЛІТЕРАТУРА

1. Біла-Кисельова А. А. Зобов'язання за статтею 8 Конвенції про права людини і основоположні свободи щодо захисту персональних даних: міжнародний досвід і практика Європейського суду з прав людини. *Наукові праці Національного університету «Одеська юридична академія»*. Т. 26. голов. ред. Ю. В. Цуркан-Сайфуліна. МОН України, НУ «ОЮА». Одеса : Гельветика, 2020. с. 12-18
2. Гуржий Т. О. Правовий захист персональних даних: монографія. Київ: Київ. нац. торг.-екон. ун-т, 2019. 216 с.
3. Закон Франції «Захист персональних даних. Досвід правового регулювання». Фонд захисту права. Упорядник. О. К. Вовчинська. К., 2001. с. 92
4. Індекс захисту персональних даних: звіт за ред. В. Мороз. Громадська організація «Інтерньюз-Україна». 2024. 44 с. URL: https://drive.google.com/file/d/1yWb8txiL8xx6krJra6dD025qXfqY9OFA/view?fbclid=IwAR3mPud1P93gOLbkjd-barQlriDVRcuhtdwJHIDcr7Vv_8JNL5_L7EJePc
5. Конвенція про захист прав людини і основоположних свобод від 04.11.1950. Офіційний портал Верховної Ради України. 2010. №215. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text
6. Кримінальний кодекс України: Відом. Верховної Ради України. 2001. № 25–26. с. 131.
7. Кодекс України про адміністративні правопорушення: Відом. Верховної Ради Української РСР. 1984. Дод. до № 51. с. 1122.
8. Панченко О. А. Державне управління інформаційною безпекою в епоху турбулентності. дис... держ. упр. у сф. держ. безпеки та охорони громадського порядку. Національний університет цивільного захисту України. Харків, 2020. 521 с.
9. Перелік держав, які забезпечують належний захист персональних даних: постанова Кабінету Міністрів України від 16.08.2022 № 910 URL: <https://www.kmu.gov.ua/npras/deiaki-pytannia-peredachi-personalniy-a910>
10. Постанова Касаційного цивільного суду Верховного Суду України від 28.05.2022 по справі № 127/13877/19. Єдиний Реєстр судових рішень. URL: <https://reyestr.court.gov.ua/Review/91161361>
11. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
12. Різак М. В. Класифікація персональних даних як необхідний елемент введення ефективної комунікації в суспільстві. *Науковий вісник Міжнародного гуманітарного університету*. Серія: Юриспруденція. Вип. 6-3 (1). 2013. С. 91-96
13. Фісун В. Проблеми захисту персональних даних: досвід України та інших країн. *Юридична газета* Вип. № 10 (716). 2020. URL: <https://jur-gazeta.com/publications/practice/informatsiye-pravo-telekomunikaciyi/problems-zahistu-personalnih-danih-dosvid-ukrayini-ta-inshih-krayin.html>
14. Цивільний кодекс України. Відом. Верховної Ради України. 2003. № 40–44. с. 356. 138.
15. Directive 95/46/EC Of The European Parliament And Of The Council of 24 October 1995 «On the protection of individuals with regard to the processing of personal data and on the free movement of such data». Official Journal. L 281, 1995. p. 31–50
16. The National Cyber Security Index 2023. URL: <https://ncsi.ega.ee/ncsi-index/>