

КРИТЕРІЇ ТА МЕХАНІЗМИ ЗАХИСТУ ПРАВ У СФЕРІ ПЕРСОНАЛЬНИХ ДАНИХ ТА ІНФОРМАЦІЇ РІЗНИМИ СУБ'ЄКТАМИ

CRITERIA AND MECHANISMS FOR THE PROTECTION OF RIGHTS IN THE FIELD OF PERSONAL DATA AND INFORMATION BY VARIOUS SUBJECTS

Дяковський О.С., к.ю.н.,

старший викладач кафедри інформаційного, господарського та адміністративного права

Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»,

докторант кафедри публічного права

Державний податковий університет

Стаття присвячена висвітленню однієї з актуальних теоретико-методологічних проблем захисту прав у сфері персональних даних. Досліджено питання правових механізмів захисту прав та зазначено про суб'єктів котрі здійснюють відповідний захист, а також критерії конфіденційності, цілісності та доступності персональних даних. Розкрито термінологічну палітру. Зокрема, детально аналізується роль законодавства у встановленні стандартів та вимог щодо обробки особистої інформації, а також практичні аспекти застосування технологічних засобів для захисту даних. Вивчено заходи, котрі мають вживатися зі сторони володільців та розпорядників персональних даних та уникнення витоку інформації.

Надано пропозиції щодо напрямків і способів покращення вітчизняного нормативно-правового регулювання у сфері захисту персональних даних. Зосереджено увагу на потребі узгодження термінології та принципів галузевого закону з міжнародними стандартами, а також посилення відповідальності за його порушення, у тому числі за витік персональних даних; більш детально врегульовано права і обов'язки тих, хто обробляє персональні дані. Також зазначено про реалізацію механізму самозахисту шляхом направлення запиту із вимогою щодо отримання мети обробки персональних даних, отримання відповіді на вказаний запит, щодо змісту персональних даних, які підлягають обробці та заявляти в подальшому заперечення щодо обробки персональних даних, що є первинним етапом захисту прав та в подальшому звертатися до Уповноваженого Верховної Ради України з прав людини та суду.

В статті розглядаються актуальні проблеми та виклики, які з'являються у контексті забезпечення приватності у цифрову епоху, а також пропонуються рекомендації щодо подальших досліджень та вдосконалення законодавства у цій сфері. Результати, представлені у статті, спрямовані на розуміння та підвищення ефективності механізмів захисту персональних даних у різних секторах суспільства.

Ключові слова: персональні дані, технології, запит, обробка даних, інформація, право власності, реєстри, суд, захист, нерухоме майно, інформаційне суспільство, реалізація права.

The article is devoted to the coverage of one of the actual theoretical and methodological problems of the protection of rights in the field of personal data. The issue of legal mechanisms for the protection of rights has been studied, and the subjects that carry out appropriate protection, as well as the criteria of confidentiality, integrity and availability of personal data, have been indicated.

The terminological palette is revealed. In particular, the role of legislation in establishing standards and requirements for the processing of personal information, as well as the practical aspects of using technological means for data protection, are analyzed in detail. Measures to be taken by the owners and managers of personal data and to avoid information leakage have been studied.

Proposals regarding directions and ways to improve domestic legal regulation in the field of personal data protection have been provided. Attention is focused on the need to harmonize the terminology and principles of the industry law with international standards, as well as strengthening responsibility for its violation, including for the leakage of personal data; the rights and obligations of those who process personal data are regulated in more detail. It is also stated about the implementation of the self-protection mechanism by sending a request with the requirement to obtain the purpose of personal data processing, receiving an answer to the specified request, regarding the content of personal data to be processed and to state in the subsequent objection to the processing of personal data, which is the primary stage of rights protection and in further contact the Commissioner of the Verkhovna Rada of Ukraine for human rights and courts.

The article considers current problems and challenges that appear in the context of ensuring privacy in the digital age, and also offers recommendations for further research and improvement of legislation in this area. The results presented in the article are aimed at understanding and improving the effectiveness of personal data protection mechanisms in various sectors of society.

Key words: personal data, technologies, request, data processing, information, ownership, registers, court, protection, real estate, information society, implementation of law.

Актуальність теми. Стрімкий розвиток інформаційних технологій, які інтегрувались фактично у всі сфери суспільної діяльності, спричинив модифікацію взаємовідносин індивіда із соціумом. Цифровий прогрес створює все більшу кількість можливостей і підстав для збору, обробки, збереження персональних даних. Враховуючи тісний взаємозв'язок персональних даних із низкою суб'єктивних прав людини, з яких найбільш яскраво вираженим є право на приватність, – розвиток системи їх захисту не втрачає своєї актуальності. Особливо гостро дане питання постало для України в останні два роки, зважаючи на воєнний стан, введений Указом Президента України від 24.02.2022 № 64/2022 [6] та наявність бойових дій, знищення та пошкодження майна та інформаційних ресурсів.

На зазначеному наголошують у своїх дослідженнях такі науковці як Гуржій Т. О., що в рамках монографічної праці опрацьовує організаційно-правові механізми захисту персональних даних, зосереджуючи увагу, в тому числі, на державному примусі як одному із дієвих інстру-

ментів у даному напрямку [2]. В розрізі правового регулювання інформаційних відносин як одне із актуальних виділяє питання критеріїв і механізмів захисту персональних даних Виноградова Г. В. [1]. З позиції аналізу дефініцій та узагальнення напрямків удосконалення вітчизняного законодавства цінними були роботи Сокол М. В., Тимощук А. В. [11], Малімон В. І. [4] та ін.

Метою дослідження є диференціація критеріїв і механізмів захисту прав щодо персональних даних з огляду на поточні суспільно-правові реалії в Україні.

Виклад основного матеріалу. Питання термінологічного визначення концепту «персональні дані» у юриспруденції, не зважаючи на його закріплення у профільному Законі, залишається одним із чи не найбільш дискусійних у вітчизняному праві. Так, згідно статті 2 Закону України «Про захист персональних даних» законодавець зазначає дану категорію як відомість чи сукупність відомостей про особу із зазначенням, що дана особа ідентифікована або може бути конкретно ідентифікована [9].

Дискусія відносно коректності трактування зазначеного поняття обумовлена багатоаспектністю використання, а отже практичною неспроможністю окреслити його межі. До прикладу, персональні дані найманого працівника будуть необхідними його роботодавцю, якщо вони безпосередньо пов'язані із його трудовою діяльністю, навчанням, забезпеченням охорони праці на виробництві, підвищенням кваліфікації [11, с. 53]. Разом з цим, ідентичний суб'єкт, вступаючи у правовідносини із банківською установою, надасть право на обробку первинних персональних даних, а також тих, що стосуються інформації про рахунки, доходи (нарахування і витрати), кредитної історії тощо.

Особливість взаємозв'язку перелічених критеріїв захисту полягає у їх консолідованій єдності, за якої можливе досягнення поставлених цілей (стану безпечності). Так, законодавчі норми не будуть нести бажаний результат, якщо технічні фахівці не створять належну базу для уникнення несанкціонованого використання персональних даних.

Правові заходи захисту передбачають необхідність прийняття низки необхідних нормативних і організаційно-розпорядчих актів, котрі стосуються політики обробки й захисту, порядку знищення персональних даних, положення про внутрішній аудит роботи з персональними даними.

Не можна не погодитися із думкою Тимошенко О. А., яка зазначає, що правовому забезпеченню захисту персональних даних притаманні такі специфічні риси: 1) наявність джерел правового регулювання захисту персональних даних на всіх шаблях законодавства; 2) різна галузева приналежність такого законодавства; 3) наявність розвинутого міжнародно-правового механізму захисту персональних даних; 4) наявність спеціального закону про захист персональних даних; 5) велика кількість бланкетних норм, що відсилають до законодавства у сфері національної безпеки і спеціальної технічної літератури; 6) підвищений динамізм законодавства про захист персональних даних, оскільки невинний розвиток технологій змушує постійно переглядати ефективність правових норм в цій сфері [12, с. 167].

Юридичні заходи націлені на забезпечення легальності при отриманні, обробці, знищенні персональних даних, саме тому від їх володільця може знадобитися згода на обробку персональних даних або відповідний договір чи інші документи, що можуть використовуватися в даних правовідносинах за змістом яких можна встановити волевиявлення у формі надання відповідної згоди.

Звернення до Уповноваженого Верховної Ради України з прав людини є одним із найпоширеніших способів захисту даної категорії прав. Контроль у даному випадку полягає у перевірці дотримання законодавства у сфері персональних даних. Задля здійснення функцій контролю, омбудсмен використовує механізм проведення планових/позапланових перевірок всіх суб'єктів (органи публічної влади, суб'єкти господарювання, фізичні особи), які є володільцями та/або розпорядниками персональних даних. Апелюючи до захисту своїх персональних даних через омбудсмена, суб'єкт не обмежується в праві на звернення до суду [9].

Виділяють також володільців та розпорядників персональних даних як суб'єктів котрі у відповідності до ч. ст. 24 Закону України «Про захист персональних даних» зобов'язані забезпечити захист цих даних від випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних [9].

Варто зазначити, що особа котра вважає, що відбулося кримінальне правопорушення у даній сфері не обмежена також звернутися з відповідною заявою до правоохоронних органів у встановленому законом порядку.

Крім того організаційні заходи, як правило, проте невичерпно, стосуються суб'єктів господарювання та можуть включати призначення відповідальних осіб, навчання працівників, формування культури приватності в компанії як елементу корпоративної культури. На основі норм чинного законодавства здійснюється регламентація внутрішнього порядку роботи з персональними даними та доступу до них за допомогою програмного забезпечення. У зв'язку з цим варто зазначити, що заходи технічного характеру передбачають вибір надійних постачальників програмного забезпечення і серверних потужностей, а також реалізацію заходів захисту даних під час роботи з програмним забезпеченням.

Відповідно, проблематика захисту персональних даних – питання комплексне, потребує пильної уваги та концентрації зусиль різними суб'єктами, особливо в період воєнного стану. Перший рівень передбачає застосування механізмів самозахисту шляхом:

- направлення запиту (в тому числі через довірену особу чи представника) із вимогою надання відомостей про мету обробки персональних даних, джерела збирання, їх місцезнаходження, а також місцезнаходження володільця (розпорядника) таких даних;

- отримувати відповідь на запит (на безоплатній основі) щодо змісту персональних даних, які підлягають обробці;

- висувати вимогу стосовно заперечення проти обробки персональних даних, при наявності вмотивованих підстав, а також відкликати згоду.

При цьому, найбільш поширеним є порушення, що зводиться до неповідомлення суб'єкта відносно дій, котрі проводяться із персональними даними. Так, на відміну від європейської Конвенції [3], українське законодавство не містить конкретних вказівок щодо процедури інформування суб'єктів персональних даних у разі форс-мажору, такого як «витік» персональних даних.

Національний закон вказує на те, що про зміну, видалення чи знищення персональних даних або обмеження доступу до них володільця персональних даних протягом десяти робочих днів повідомляє суб'єкта персональних даних, а також суб'єктів відносин, пов'язаних із персональними даними, яким ці дані було передано [9].

Таким чином у десятиденний термін володільця також має повідомити суб'єкта персональних даних і про передачу їх третім особам (включаючи випадки ціленаправленої та помилкової передачі даних, наприклад, відправка інформації на некоректну електронну адресу). Узгодити це та низку інших проблемних питань, в тому числі у відповідності до кращих практик і стандартів країн ЄС, частково допоможе прийняття Закону України «Про захист персональних даних» зареєстрованого за номером 8153 від 25.10.2022 року [8].

Даний проект закону аргументує потребу у посиленні міри відповідальності за порушення у даному напрямку, а саме у збільшенні розміру штрафів як критерій попередження вчинення правопорушень у даній сфері.

Також систематизує підстави та порядок здійснення трансграничної передачі персональних даних, розкриває обов'язки та алгоритм дії сторін у разі витоку персональних даних, вносить істотні зміни у розподіл прав і обов'язків володільця (контролера) та розпорядника (оператора) персональних даних.

Технологічний аспект питання також містить низку рекомендацій, якими не варто нехтувати, особливо при роботі із цифровими носіями:

- варто відвідувати лише ті сайти та завантажувати застосунки, в безпечності яких переконані завчасно, в тому числі використовуючи дво- або багатофакторну аутентифікацію;

- перед початком роботи із ресурсами – в обов'язковому порядку ознайомитися із політикою кон-

фіденційності, що висуваються зі сторони володільця ресурсу;

- направляти вимогу щодо видалення або знищення персональних даних за спливом терміну і мети їх обробки;
- відмовлятися від передачі персональних даних до моменту виникнення підстав для їх збору (геологікація, персональні відомості, разові паролі, паролі доступу до акаунтів тощо).

Відповідно, обробка персональних даних має забезпечувати належний захист даних на етапі початкового проектування інформаційно-телекомунікаційної системи або при реєстрації у технічному завданні на створення або модернізацію такого об'єкта, формуються вимоги / рекомендації щодо безпечності кінцевого продукту. Під час наступного етапу – введення системи в експлуатацію – важливо визначити категорії технічних заходів, які будуть застосовуватися для забезпечення захисту персональних даних (інформація фіксується у правостановлюючому акті для відповідної системи або реєстру). Встановлення факту порушення у сфері захисту персональних даних досить часто є показником існування проблем на рівні формування внутрішніх процесів у суб'єкта господарювання.

Вказане свідчить про необхідність проведення аудиту всіх внутрішніх процесів, котрі стосуються обробки і забезпечення захисту персональних даних. Особи, наділені правом доступу до персональних даних працівників, мають підписати зобов'язання про нерозголошення конфіденційної інформації та використовувати персональні дані лише з метою, для якої вони були надані. Якщо відсутня практична можливість самостійного створення безпечного механізму, доцільно залучити спеціаліста по захисту персональних даних на умовах аутсорсингу, що забезпечить постійний контроль стану інформаційних систем.

В свою чергу, обираючи той чи інший механізм захисту персональних даних слід керуватися інформацією про наявність / відсутність фактичного порушення або ж має місце правомірне обмеження таких прав. Необхідність переосмислення стратегій контролю особистих даних виникає через складність та недостатність прозорості аналітики великих обсягів інформації. Це вимагає адаптації до конкретного соціального та технологічного серед-

овища, враховуючи недостатню освіченість користувачів у цій сфері [5, с. 388].

Модернізація законодавства у сфері захисту персональних даних із урахуванням досягнень технічної сторони питання – це не виклик, а обґрунтована потреба, з огляду на реалії та сьогодення українців. У Верховній Раді України від 07.06.2021 перебував на розгляді законопроект № 5828 [7], який мав на меті оптимізувати підхід до захисту персональних даних. В цілому, 16.08.2022 проект було знято із розгляду та все ж декілька ініціатив, закладених у його зміст, на нашу думку заслуговують на увагу. Із аналізу тексту вбачається, що розробники апелюють до наступного: діючі норми не відповідають міжнародним стандартам, зокрема Загальному регламенту про захист даних [10] і Конвенції [3].

Тому наявність законопроектів щодо персональних даних свідчить про необхідність удосконалення регулювання даної сфери котра впливає також на інформаційні відносини та різноманітні сфери щодо роботи, нерухомого майна, та відображення його в реєстрах, тощо.

Висновки. Вивчаючи проблематику ефективного захисту прав громадян як суб'єктів персональних даних, слід розглядати юридичний, технологічний та організаційні аспекти даного питання. Правова сторона зводиться до ідентифікації регламентованого обсягу прав суб'єктів персональних даних, а також визначення оптимальних механізмів їх захисту. Технологічний аспект полягає в необхідності виконання певних рекомендацій, спрямованих на безпечну обробку особистих даних за допомогою інформаційно-телекомунікаційних технологій і систем. Мова йде про конфіденційність та цілісність персональних даних (шифрування, захист від несанкціонованого доступу). Крім того, суб'єкти персональних даних також повинні вживати відповідних заходів безпеки та виконувати вимоги щодо обробки особистих даних або відмовлятися від їх використання у випадках, коли це необхідно; за умови виявлених порушень – звертатися із відповідною заявою до омбудсмена чи суду (організаційний рівень). Перспективи подальших наукових пошуків вбачаємо у аналізі норм іноземного законодавства в частині обробки біометричних та інших (чутливих) категорій персональних даних.

ЛІТЕРАТУРА

1. Виноградова Г. В. Правове регулювання інформаційних відносин в Україні: навч. Посібник. Київ: Юстиніан, 2006. 117 с.
2. Гуржій Т. О. Правовий захист персональних даних: монографія. Київ: Київ. нац. торг.-екон. ун-т, 2019. 216 с.
3. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981. *Офіційний вісник України*. 2011. 14 січ. (№ 58). Ст. 701
4. Малімон В. І. Способи захисту персональних даних громадян як пріоритет національної безпеки України. *Digital Transformations of Modernity: Proceedings of the Multidisciplinary International Scientific-Practical Conference (January 24, 2022. Coimbra, Portugal)*. Chernigiv: REICST, 2022. С. 142–145.
5. Посібник з європейського права у сфері захисту персональних даних. К.: К.І.С., 2020. 432 с.
6. Про введення воєнного стану: указ Президента України від 24.02.2022 № 64/2022. URL: <https://zakon.rada.gov.ua/laws/show/64/2022#Text> (дата звернення 28.02.2024).
7. Проект Закону про захист персональних даних від 07.06.2021 № 5628. Офіційний веб-портал Верховної Ради України. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=72160
8. Проект Закону про захист персональних даних від 25.10.2022 № 8153. Офіційний веб-портал Верховної Ради України. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=75101
9. Про захист персональних даних : Закон України від 13.04.2012 № 4651-VI. *Верховна Рада України. Законодавство України*. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата звернення 28.02.2024).
10. 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). URL <https://www.kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf>
11. Сокол М. В., Тимошук А. В. Поняття персональних даних працівника та їх відмежування від іншої інформації. *Право та державне управління* № 2. 2020. С. 48–54.
12. Тимошенко О. А. Захист персональних даних в цивільних правовідносинах: вітчизняне правове забезпечення крізь призму практики Європейського суду з прав людини. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. Вип. 4. 2023. С. 165–172.