

МЕХАНІЗМ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ

Автор досліджує проблемні питання захисту персональних даних на прикладі діючих норм чинного законодавства та окреслює основні напрямки його вдосконалення.

Ключові слова: персональні дані, обробка персональних даних, захист персональних даних, адаптація, систематизація, блокування.

Зростання наукового і практичного інтересу до тематики дослідження персональних даних обумовлено розвитком інформаційних систем та технологій та їх застосуванням в практичній діяльності цілого ряду державних органів, установ і підприємств. Так, в процесі розвитку постійно збільшується кількість протиправних посягань на носії інформації та інформацію про особу, а саме на персональні дані про особу. Відповідно, подібні дії становлять загрозу не лише державним і колективним інтересам, а й інтересам окремих осіб. Стрімкий розвиток новітніх технологій та їх упровадження в життя зумовлюють появу нових видів злочинності і наштовхують на думку про постійну еволюцію законодавства щодо формування захисних механізмів з метою недопущення незаконних посягань не тільки на особу, її майно, життя та здоров'я, а також на інформативну базу про особу.

Починаючи з другої половини ХХ сторіччя, правовий захист приватного життя в умовах побудови інформаційного суспільства став одним із пріоритетних напрямів дослідження зарубіжних вчених.

Персональні дані не є новим, невідомим чи недослідженим феноменом в науково-правовій доктрині. Хоча розуміння їх сутності і змісту, особливостей захисту тощо для кожного історичного періоду та країни було неоднозначним, та суттєво відмінним від сучасної інтерпретації у вітчизняних розвідках та легалізації в нормативно-правових актах.

Питання, пов'язані із персональними даними досліджувались у працях таких вітчизняних науковців, як: В. Ліпкан, Р. Калюжний, Т. Костецька, О. Кохановська, А. Марущак, А. Новицький, Н. Співак, А. Тунік, І. Усенко, К. Цьомик, М. Щербатюк,

проте наявні напрацювання свідчать лише про науковий і практичний інтерес до тематики дослідження, але вони не в повній мірі відображають основні тенденції щодо вдосконалення системи захисту персональних даних при їх обробці.

Відповідно, метою нашого дослідження буде аналіз механізму захисту персональних даних та напрямки вдосконалення законодавства в зазначеній сфері.

Відповідно до ст. 2 Закону України "Про захист персональних даних" [2], обробка персональних даних – будь-яка дія або сукупність дій, здійснених повністю або частково в інформаційній (автоматизованій) системі та/або в картотеках персональних даних, які пов'язані зі збиранням, реєстрацією, накопиченням, зберіганням, адаптуванням, зміною, поновленням, використанням і поширенням (розповсюдженням, реалізацією, передачею), знесобленням, знищенням відомостей про фізичну особу.

Характер норм-дефініцій мають також положення ч. 1 ст. 12 та ч. 1 ст. 14 Закону України "Про захист персональних даних" [2]. Отже, якщо ж у законодавстві міститься стаття, в якій даються визначення вживаних понять, то саме у цій статті усі поняття мають бути визначені, а не розкидані по тексту закону, що ускладнює його розуміння та пошук відповідних визначень, враховуючи також те, що закон розрахований на переважну більшість суб'єктів господарювання, у тому числі фізичних осіб-підприємців, які зазвичай не мають юридичної освіти, навичок користування законодавчими актами та не користуються послугами професійних юристів.

Українське визначення передбачає також дії, пов'язані із адаптацією, тоді як російське відрізняється наявністю у визначенні таких дій, як

систематизація та блокування. Як зазначає К. Цьомик, попри те, що Законом України "Про захист персональних даних" встановлено таку форму обробки як адаптування, розкриття змісту адаптування Закон України "Про захист персональних даних" не містить. Поняття адаптування важко знайти в інших нормативно-правових актах. Із загального розуміння, адаптуванням є зміна бази даних, що здійснюється виключно з метою забезпечення функціонування бази даних на конкретних технічних засобах користувача чи під управлінням конкретних програмних продуктів користувача. Наприклад, переведення картотек в електронну базу даних можна розглядати як адаптування [3].

Варто також з'ясувати питання стосовно прав володільця на знищення персональних даних без згоди особи. Відповідно до п. 7 ч. 2 ст. 8 Закону України "Про захист персональних даних" суб'єкт персональних даних має право на захист своїх персональних даних від знищення. Повертаючись знову до ч. 5 ст. 6 Закону України "Про захист персональних даних" можна констатувати, що знищення без згоди особи також буде вважатися порушенням законодавства [2]. Однак законодавством не передбачена юридична відповідальність за знищення персональних даних без згоди суб'єкта персональних даних.

У зв'язку з численними зверненнями громадян щодо практичного застосування деяких положень Закону України "Про захист персональних даних" Міністерство юстиції надало роз'яснення з найбільш актуальних та поширених питань від 21.12.2011 р. "Деякі питання практичного застосування Закону України "Про захист персональних даних", в якому, зокрема, іде мова і про обробку персональних даних [4].

Метою обробки персональних даних є забезпечення володільцем бази персональних даних належного здійснення діяльності, визначеної в законах, інших нормативно-правових актах, положеннях, установчих документах, які регулюють його діяльність, та внаслідок якої виникає необхідність у вчиненні будь-якої дії або сукупності дій з обробки персональних даних у базах. Слід звернути увагу на те, що склад та зміст персональних даних мають бути відповідними та не надмірним стосовно визначеної мети їх обробки [4].

Одним з проблемних моментів в обробці персональних даних є їх використання і обробка роботодавцем у зв'язку з відсутністю чіткого ро-

зуміння їх складових і видів інформації про особу, які відносяться законодавством до персональних даних. Так, законодавством України не встановлено і не може бути встановлено чіткого переліку відомостей про фізичну особу, які є персональними даними, задля можливості застосування положень Закону України "Про захист персональних даних" [2] до різноманітних ситуацій, в тому числі при обробці персональних даних в інформаційних (автоматизованих) базах та картотеках персональних даних, що можуть виникнути у майбутньому, у зв'язку зі зміною в технологічній, соціальній, економічній та інших сферах суспільного життя.

Щодо чіткого переліку відомостей про фізичну особу, які є персональними даними, то в зв'язку з численними зверненнями громадян щодо практичного застосування деяких положень Закону України "Про захист персональних даних" Міністерство юстиції України надало роз'яснення з найбільш актуальних та поширених питань у цій сфері, зокрема зауважило, що "законодавством України не встановлено і не може бути встановлено чіткого переліку відомостей про фізичну особу, які є персональними даними, задля можливості застосування положень Закону України "Про захист персональних даних" до різноманітних ситуацій, в тому числі при обробці персональних даних в інформаційних (автоматизованих) базах та картотеках персональних даних, що можуть виникнути у майбутньому, у зв'язку зі зміною в технологічній, соціальній, економічній та інших сферах суспільного життя" [4].

Згідно з Законом України "Про захист персональних даних" підставами виникнення права на використання персональних даних є згода суб'єкта персональних даних на обробку його персональних даних, при чому суб'єкт персональних даних має право при наданні згоди внести застереження стосовно обмеження права на обробку своїх персональних даних, а також дозвіл на обробку персональних даних, наданий володільцю бази персональних даних відповідно до Закону України "Про захист персональних даних" виключно для здійснення його повноважень [2].

При цьому, якщо суб'єкт персональних даних відмовляється надати згоду на обробку його персональних даних власник бази повинен знищити усі персональні дані такого суб'єкта.

Постає питання: як має вчинити власник бази при прийманні на роботу особи, яка відмовляється-

ся надати згоду на обробку даних. Роботодавець, обробляючи персональні дані свого працівника, лише реалізує свої права та обов'язки, покладені на нього Законом як на роботодавця, а тому, в такому випадку необхідно обробляти персональні дані на підставі Закону без згоди суб'єкта.

У Законі України "Про захист персональних даних" відсутня чітка процедура знищення персональних даних, що є дуже важливим, враховуючи особливості комп'ютерних технологій обробки даних [2].

Занадто широкі повноваження надані контролюючому органу: "спеціальний уповноважений орган з контролю за дотриманням законодавства про захист персональних даних, до повноважень якого належить інспектувати дотримання вимог Закону України "Про захист персональних даних", вносити приписи на усунення порушень та реєструвати всі бази персональних даних в Україні" [2].

Іншим проблемним моментом є відсутність належного нормативно-правового регулювання порядку проведення та механізмів проведення перевірок. Відповідно до Закону України "Про захист персональних даних" представники уповноваженого органу мають право безперешкодно потрапляти до будь-якого приміщення, де обробляються персональні дані (тобто практично до кожного офісу та в кожну квартиру), що є рівнозначним праву на проведення обшуку, яке до сьогодні мали лише правоохоронні органи [2].

Актуальною правовою проблемою можна вважати згоду суб'єкта на збереження його персональних даних у базі. На думку О. Дмитренка, реєстрація баз даних є беззмістовною, тому що реєструється не зміст бази даних, а лише її факт. У цьому випадку особа не зможе дізнатися, яка саме база і які відомості про неї містить. Дослідник наголошує, що у Європейському Союзі реєстрація персональних даних – це лише нотифікація, повідомлення, зроблене за добровільним заявочним принципом. Натомість в українському законодавстві такий елемент не доопрацьовано [5, с. 41].

Існує думка, яка підтримується багатьма дослідниками охорони персональних даних, про те, що персональні дані мають бути поділені на персональні дані загального характеру та вразливі персональні дані. Так,

А. Тунік відзначає: "разом із тим відповідно до європейських стандартів персональні дані

поділяються на дані загального характеру (прізвище, ім'я, по батькові, дата та місце народження, громадянство, місце проживання) та вразливі персональні дані (про стан здоров'я – історія хвороби, діагнози тощо; етнічна належність; ставлення до релігії; ідентифікаційні коди чи номери; персональні символи; підпис; відбитки пальців, записи голосу, фотографії; про розмір зарплати й інші законні доходи, про вклади та рахунки в банках, нерухомість, податковий статус; кредитна історія; дані про судимість та інші форми притягнення особи до кримінальної, адміністративної чи дисциплінарної відповідальності; результати іспитів, професійного й іншого тестування тощо). Європейськими нормативними актами забороняється збирання, зберігання, використання та поширення без згоди суб'єкта саме вразливих персональних даних, а не взагалі всіх персональних даних, як це зроблено у вітчизняному законі" [6, с. 97].

Як відзначає Н. Співак, "Обробку персональних даних без згоди суб'єкта персональних даних дозволено здійснювати у випадках, передбачених законодавством (трудовим, податковим, пенсійним, виборчим тощо). Міністерство юстиції України роз'яснило, що паспортні дані, відомості про освіту, стан здоров'я і т.д., які необхідні для оформлення на роботу згідно з трудовим законодавством, становлять бази персональних даних співробітників. Хибною є поширена думка про те, що якщо робітник не дає згоди на обробку своїх даних у базі персональних даних, то й обробляти їх не можна.

Тут можливі два варіанти: 1) дані є – згоди немає: у такому випадку можна обробляти ті персональні дані, які необхідні відповідно до Кодексу законів про працю; 2) немає всіх необхідних документів та згоди – немає й роботи. За цим же принципом мовчазного дозволу законодавства на обробку персональних даних існує і Список виборців, зареєстрований Центральною виборчою комісією України. Громадяни згоди не підписували – а в базу внесені. Хоча прикладів таких небагато" [7]. Таким чином, можна зробити висновок, що при обробці персональних даних працівника отримання згоди на обробку таких персональних даних не є обов'язковим.

Як зазначають дослідники В. Ліпкан та Ю. Максименко, "якщо проаналізувати дефініції "національні інтереси", "національна безпека", а також перелік пріоритетів національних інте-

ресів, загроз національним інтересам і національній безпеці України, основних напрямів державної політики з питань національної безпеки України, то можна дійти висновку, що винятки з правила, закріпленого ст. 32 Конституції України, переважають саме правило, тобто випадки, коли не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, є значно меншими, ніж випадки, коли збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди допускається, оскільки майже будь-що охоплюється поняттям національної безпеки" [8, с. 64].

Враховуючи зазначене, норми Закону України "Про захист персональних даних" щодо підстав обробки персональних даних варто застосовувати з розумінням того, що обробка персональних даних дозволяється лише у випадках, прямо передбачених у законі і у відповідності до визначеної законом мети, або, якщо відповідного випадку обробки персональних даних не передбачено законом, за згодою суб'єкта персональних даних. Така зміна акцентів змушує у першу чергу шукати підстави обробки у законі, і у разі їх наявності, дозволяє не вимагати згоди на обробку від суб'єкта даних, яка буде не потрібною. Загальний перелік таких підстав повинен, на нашу думку, бути розміщений у самому Законі України "Про захист персональних даних".

Іншим проблемним моментом, що потребує надійної системи захисту персональних даних в процесі їх обробки є розміщення їх в мережі Інтернет. Оскільки персональні дані кожного з нас чи то медичного, фінансового характеру, не кажучи вже про ті, що ми використовуємо у своїх візитках є або можуть бути об'єктом використання в автоматизованій системі обробки, ми, користуючись Інтернетом там залишаємо велику кількість своїх персональних даних. І що головне використання наших даних нічим не обмежене і не врегульоване тобто фактично, такі дані залишаються не захищеними. І вони безперешкодно можуть використовуватися з метою впливу на наш вибір чи то економічний, чи то політичний – будь-який, можуть впливати на наші переконання і думки або використовуватися якимось іншим чином. Такі бази даних постійно вдосконалюються, уніфікуються і з кожним разом зачіпають приватне життя кожної людини все сильніше і сильніше [9]. Відповідно,

існує потреба правового регулювання зазначених відносин.

Загалом, захист персональних даних – це вміння балансувати між інформаційною відкритістю та закритістю, між двома прагненнями: максимально розширити доступ громадян до нествореної публічної інформації (державної, наукової, освітньої, персональної тощо) і водночас максимально захистити інформацію приватного змісту. Вирішення стратегічних завдань, пов'язаних із удосконаленням інформації про особу полягає у розвитку нових програм, створенні вітчизняних систем захисту, розв'язання протиріч, що виникають у сучасному законодавстві. Також важливого значення нині набуває законодавчий контроль за розвитком електронного середовища, комп'ютерних систем. Цей аспект є дуже важливим, оскільки майбутній розвиток суспільства в усіх галузях буде пов'язаний із розвитком комп'ютерних систем і мереж та відповідно існує потреба захисту персональних даних при їх обробці та використанні. Переведення бази даних з однієї електронної форми існування в іншу також є адаптуванням (приклад Microsoft Office Access, MySQL, PostgreSQL та ін.) [3]. Ми погоджуємось з думкою вчених, що натомість дії щодо систематизації та блокування являються досить поширеними формами обробки даних, у тому числі персональних, тому варто передбачити їх у Законі України "Про захист персональних даних" та дати відповідно їм визначення у ст. 2 вказаного Закону України "Про захист персональних даних".

Крім того, як позитивне явище, Кабінет Міністрів пропонує додатково наділити Уповноваженого Верховної Ради України з прав людини повноваженнями здійснювати контроль за дотриманням законодавства у сфері захисту персональних даних. Зокрема Уповноваженого з прав людини передбачається наділити повноваженнями з проведення планових та позапланових перевірок власників та розпорядників баз персональних даних; направлення подання для вжиття ними заходів щодо усунення виявлених порушень законодавства; надання рекомендацій у сфері захисту персональних даних. Також щороку Уповноважений ВР з прав людини готуватиме та оприлюднюватиме щорічну доповідь про стан дотримання законодавства про захист персональних даних у державі [10].

Отже, прийняття Закону України "Про захист персональних даних" було однією із вимог

співробітництва ЄС та України, з метою наближення правової системи нашої країни до європейських стандартів. Цей Закон був створений на базі міжнародних та європейських стандартів у цій сфері. Водночас аналіз норм цього нормативно-правового акту та компаративний аналіз засвідчує про значне розходження у розумінні сутності і змісту персональних даних. Крім того, вітчизняне законодавство у сфері захисту персональних даних є недостатньо сформованим через наявність значної кількості прогалин та колізій, що сприяє правопорушенням у цій сфері.

Література

1. Конституція України від 28.06.1996 р. № 254к/96-ВР // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.
2. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI // Відомості Верховної Ради України (ВВР). – 2010. – № 34. – Ст. 481.
3. Цьомик К. В. Обробка персональних даних: юридичний аспект [Електронний ресурс]. – Режим доступу: http://soter.kiev.ua/publications/legal_database_processing.
4. Деякі питання практичного застосування Закону України "Про захист персональних даних": роз'яснення Міністерства юстиції України від 21.12.2011 р. [Електронний ресурс]. – Режим доступу: <http://zakon2.rada.gov.ua/laws/show/n0076323-11/conv>.
5. Дмитренко О. До проблеми поширення режиму відкритої інформації на персональні дані у світлі практики Європейського Суду з прав людини: Дослідження пропозиції поширення режиму загальнодоступної інформації на окремі персональні дані на предмет відповідності європейським стандартам захисту персональних даних, відображених у практиці Європейського Суду з прав людини / О. Дмитренко // Підприємство, господарство і право. – 2008. – № 4. – С. 41-43.
6. Тунік А. Захист персональних даних: аналіз вітчизняного законодавства / А. Тунік // Право України. – 2011. – №8. – С. 97-100.
7. Співак Н. Типові помилки у сфері захисту персональних даних. Газета "Аптека" [Електронний ресурс]. – Режим доступу: <http://www.apteka.ua/article/116863>.
8. Ліпкан В. Інформаційні права і свободи людини і громадянина / В. Ліпкан, Ю. Максименко // Підприємство, господарство і право. – 2011. – № 9 (189). – С. 64-68.
9. Щербатюк М. Особливості захисту персональних даних в Інтернеті [Електронний ресурс]. – Режим доступу: <http://www.inau.org.ua/15.225.0.0.1.0.phtml>.
10. Кабмін хоче уповноважити омбудсмена контролювати захист персональних даних [Електронний ресурс]. – Режим доступу: <http://economics.unian.net/ukr/news/156960-kabmin-hoche-upovnovajiti-ombudsmena-kontrolyuvati-zahist-personalnih-danih.html>
11. Кохановська О.В. Теоретичні проблеми інформаційних відносин у цивільному праві: Монографія. – К.: Видавничо-поліграфічний центр "Київський університет", 2006. – 463 с.

Сопилко И.Н.

Механизм защиты персональных данных: проблемы и перспективы

Автор исследует проблемные вопросы защиты персональных данных на примере действующих норм действующего законодательства и определяет основные направления его совершенствования.

Ключевые слова: персональные данные, обработка персональных данных, защита персональных данных, адаптация, систематизация, блокировка.

Sopilko I.M.

Mechanism of personal data protection: the issues and the perspectives

The author explores the issues of personal data protection in the case of the current active legislation and outlines the main areas of it's improvement.

Keywords: personal data, personal data processing, data protection, adaptation, classification, blocking.