УДК 347.2/3

ПРАВОВІ ЗАСАДИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

LEGAL BASIS FOR THE PROTECTION OF PERSONAL DATA

Гуйван П.Д.,
кандидат юридичних наук,
докторант
Національного юридичного університету
імені Ярослава Мудрого,
заслужений юрист України

Стаття присвячена дослідженню дієвості й ефективності юридичних механізмів захисту персональних даних в Україні. Вивчено загальні засади поняття «захист персональних даних» у науці та законодавстві. Проаналізовано його співвідношення з охороною особистої інформації. Обстоюється теза про домінування цивільно-правових способів захисту від порушень у сфері обороту персональних даних. Зазначено неконкретність та розмитість матеріальних санкцій. Внесені конкретні пропозиції щодо нормативної та правозастосовної діяльності.

Ключові слова: захист персональних даних, оброблення інформації про особу.

Статья посвящена исследованию действенности и эффективности юридических механизмов защиты персональных данных в Украине. Изучены общие принципы понятия «защита персональных данных» в науке и законодательстве. Проанализировано его соотношение с охраной личной информации. В работе отстаивается тезис о доминировании гражданско-правовых способов защиты от нарушений в сфере оборота персональных данных. Отмечена неконкретность и размытость материальных санкций. Внесены конкретные предложения по нормативной и правоприменительной деятельности.

Ключевые слова: защита персональных данных, обработка информации о лице.

This work is devoted to the study of the effectiveness and effectiveness of legal mechanisms for the protection of personal data in Ukraine. The general principles of the concept of “protection of personal data” in science and legislation are studied. Its correlation with the protection of personal information is analyzed. Thesis defends the dominance of civil law protection from violations in the sphere of personal data turnover. There is a lack of specificity and blurring of material sanctions. Concrete proposals on normative and law enforcement activities have been made.

Key words: protection of personal data, processing of information about person.

Постановка проблеми. Суспільні взаємини у сфері обороту персональних даних є одним із видів інформаційних правовідносин. Завдяки бурхливому розвитку промислових, наукових, технічних, соціальних комунікаційних процесів обмін та оброблення інформації стали більш об’ємними та легкими. Значну роль у цьому відіграє стрімкий прогрес телекомунікаційних та комп’ютерних технологій. Особливість правового регулювання обігу персональних даних пов’язана із предметом – інформацією обмеженого доступу, покликаною ідентифікувати фізичних осіб. Регламентація цієї відособленої групи суспільних відносин досягається шляхом задіянням цілого комплексу різних за юридичною силою правових норм. Встановлюється фактичний пріоритет спеціальних актів, призначених для регулювання обороту окремих видів персональної інформації, щодо загальних норм [1, с. 232]. З огляду на зазначене, значної актуальності на сучасному етапі набуває проблема захисту персональних даних від таких, зокрема, порушень прав їхнього носія, як витоки інформації, випадковий чи несанкціонований доступ до неї, незаконне знищення, зміна, копіювання, блокування та поширення.

Також негативним наслідком значного зростання обороту даних особистого характеру в різних сферах суспільного життя стало порушення немайнових прав особи, яке полягає в неправомірному збиранні, використанні і передачі третім особам персональної інформації, також із використанням електронних систем, зокрема мережі Інтернет. Як відомо, дана глобальна інформаційно-телекомунікаційна мережа є головним засобом вільного поширення інформації. Вона здатна акумулювати всі доступні інформаційні джерела. Але такі чесноти часто переходять у вади, особливо це характерно для обороту особистих даних про конкретну людину, що може порушити її право на недоторканість приватного життя. У зв’язку з необхідністю забезпечення цього права нагальною є потреба належного правового регулювання вказаних відносин, зокрема і в охоронно-правовий спосіб. Тому питання розроблення та застосування адекватного законодавчого забезпечення охорони та захисту персональних даних у національній правовій системі дуже важливе.

Чинне законодавство має не лише врегулювати питання заборони збирання, зберігання, використання та поширення особистої інформації без згоди конкретної людини і порядок діяльності органів влади та місцевого самоврядування, інших володільців персональних даних стосовно забезпечення кожному можливостей доступу до документів, які безпосередньо стосуються його прав і свобод (це певною мірою нормативно вже закріплено, інша річ – наразі ці принципи не дуже дієві), але й запровадити чіткий набір санкцій за порушення окремих обов’язків у сфері оброблення таких даних.

На жаль, маємо констатувати невизначеність чинного українського законодавства в площині запрова-

дження негативних наслідків для порушника прав особи на повагу до її особистої інформації. Наприклад, як у спеціальному законі про захист персональних даних, так і в нечисленних підзаконних актах відсутня відповідальність за конкретні порушення регулятивних правил оброблення даних, як-от: неповідомлення людини про збір її персональних даних, ненадання їй відомостей стосовно порядку оброблення даних та доступу до них, незаконне оброблення персональних даних або оброблення без належно оформленої і зафіксованої згоди суб'єкта, відмова в доступі до особистої інформації, надання неповних чи спотворених відомостей або надання відповіді з недотриманням встановлених строків, незаконне поширення / передача, невиконання вимоги суб'єкта змінити / видалити персональні дані, що не відповідають дійсності тощо. Для досягнення реального прогресу у сфері захисту основоположних прав людини вказані аспекти мають бути враховані, а чинне законодавство кардинально доопрацьоване.

Стан опрацювання. Проблемам, пов'язаним із належним і справедливим застосуванням чинного законодавства про захист персональних даних та напрацюванням нових підходів у даній сфері, зокрема на базі інтеграції України до світового інформаційного простору, присвячені праці таких учених, як: В. Глушков, І. Бачило, Б. Кормич, Р. Калюжний, А. Марущак, В. Іванський, А. Пазюк, Т. Обуховська, М. Бем, О. Волков та інші. У цих публікаціях розглядаються різні аспекти захисту персональних даних, зокрема в мережі Інтернет. Вважаємо, що в доктрині приділяється недостатня увага дослідженню дієвості й ефективності правових актів під час захисту прав особи на персональні дані в конкретних життєвих ситуаціях. Недостатньо проаналізовані в порівняльному плані національне та міжнародне законодавство в даній царині. Адаптування української правової системи, зокрема органів правозастосування, до світових та європейських стандартів сприятимеь належному здійсненню державної інформаційної політики, становленню інформаційного суспільства в Україні.

Метою статті є розкриття юридичної сутності та значення механізмів захисту й охорони персональних даних, їхніх особливостей та проблем правового регулювання. Для цього здійснюється детальний аналіз правового регулювання захисту персональних даних, встановлення позитивних та негативних чинників у правотворенні та правозастосуванні в цій сфері діяльності, вироблення пропозиції щодо коригування і вдосконалення.

Виклад основного матеріалу. За приписом ч. 2 ст. 8 Закону України «Про захист персональних даних», суб'єкт даних має право на захист своєї особистої інформації від незаконного оброблення, випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також на захист від надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи. Він також вправі застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних. Адже порушення в даній царині правового регулювання можуть призвести до значних негативних наслідків для особи, чиї персональні дані збираються й обробляються. Наприклад, ненадання інформації на його запит позбавляє носія права змоги з'ясувати зміст даних і законність їх оброблення, а отже, практично унеможливлює застосування охоронно-правових засобів реагування.

Будь-яка інформація може бути персональними даними, якщо вона стосується людини [2, с. 41]. Такими, що потребують найбільшої уваги, наразі є питання гарантування безпеки особистої інформації з метою належного її оброблення в інформаційних електронних системах із використанням автоматизованих засобів або без них, а також адекватних видів правового захисту особи в разі порушення її права на приватність шляхом зловживань та свавілля в цій сфері. Саме в цьому контексті мають розглядатися наявні нормативні приписи та здійснюватися законодавчі і доктринальні напрацювання, адже сучасний розвиток інформаційних технологій спричиняє появу нових загроз як безпеці самих персональних даних, так і окремим суб'єктам, суспільству та державі. Мають вдосконалюватися та щоразу модернізуватися адекватні способи реагування на такі виклики. За створення та поширення нових видів відносин із необхідністю обороту особистої інформації, ускладнення нових баз даних значна увага має приділятися вдосконаленню юридичного інструментарію захисту персональних даних.

Концепція щодо правового обґрунтування прийнятності й адекватності охоронних заходів у царині інформаційного обігу даних про особу має базуватися на детальному вивченні їхньої юридичної природи. Окремі дослідники питання виділяють такі сутнісні властивості персональних даних: 1) вони належать до непублічної інформації; 2) персональні дані недоступні для публічної сфери, тобто не є надбанням суспільства; 3) дані про конкретну особу не можуть надаватися невизначеному колу осіб; 4) персональні дані пов'язані з категорією власності та захищаються створеними в публічній сфері законами; 5) вони перебувають під загрозою через розмивання меж між приватним і публічним [3, с. 87]. Справді, можна погодитися з більшістю зазначених сутнісних характеристик персональних даних, але стосовно виключної прерогативи регулювання захисту такої інформації нормами публічного права автор помиляється. Адже коли порушується право окремої людини на приватне життя шляхом, скажімо, незаконного збирання, оброблення або поширення особистої інформації, володілець вторгається в приватноправову сферу використання особистих немайнових прав (нематеріальних благ). У такому сенсі слушним є твердження науковців, які вказують на те, що проблему захисту відомостей про особу необхідно вирішувати з погляду права власності конкретної людини на її персональні дані. Має бути

наявне поєднання принципу недоторканності особи із принципом, який свідчить, що основою свободи є власність, і замах на неї рівнозначний обмеженню свободи. Інакше кажучи, особливої уваги потребує проблема врегулювання балансу інтересів сторін: особистості, суспільства і держави, на основі механізму взаємоврахування інтересів [4, с. 101].

Цілком очевидно, що захист прав на приватність особистої інформації в разі їх порушення здебільшого здійснюється за правилами цивільного законодавства (кн. 2 Цивільного кодексу України (далі – ЦКУ). Людина вправі обрати такий спосіб захисту, як компенсація збитків і моральної шкоди, завданих внаслідок витоку, втрати, несанкціонованої передачі даних особистого характеру чи порушення правил їх оброблення. Причому вказані приватноправові захисні регулятори поширюються на відносини з обороту особистих даних незалежно від того, за яких нормативних передумов виникли відповідні права й обов'язки. Вони застосовуються під час порушення у сфері як приватних по суті інформаційних взаємин (скажімо, укладання правочину щодо оброблення персональних даних продавцем у разі купівлі товару в кредит), так і коли взаємини стосовно обороту даних мають приватноправове підґрунтя (наприклад, володілець персональних даних, який їх обробляє згідно із законом, відмовив суб'єкту в доступі до них). Такий цивільно-правовий захист здійснюється також незалежно від того, який правовий статус – юридична особа приватного чи публічного права – має володілець чи розпорядник персональних даних. Наприклад, організації в освітній, оздоровчій, житлово-комунальній сфері, підприємства, банки, туристичні і страхові компанії, пенсійні фонди, органи державної влади та місцевого самоврядування.

До загальних матеріально-правових правил щодо відповідальності відсилають і норми спеціального законодавства – законів України «Про захист персональних даних» та «Про захист інформації в інформаційно-телекомунікаційних системах», постанови Кабінету міністрів України (далі – КМУ) від 29 березня 2006 р. № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», Типового порядку обробки персональних даних, затвердженого наказом Уповноваженого Верховної Ради із захисту прав людини від 8 січня 2014 р. № 1/02–14. Досить часто публічноправовий захист персональних даних здійснюється шляхом притягнення винних осіб до адміністративної відповідальності. Але варто погодитися з тими дослідниками, які наголошують на наявних недоліках відповідного інструментарію. Адже Кодекс України про адміністративні правопорушення передбачає відповідальність лише фізичних осіб, хоча здебільшого стягнення варто накласти саме на юридичну особу. Найчастіше такі питання порушуються, коли йдеться про недоліки процесу організації оброблення персональних даних володільцем, які базуються на внутрішніх правилах володільця, які інколи недостатньо чіткі та формальні. Тому вкрай необхідно змінити законодавство в частині запровадження можливості накладення штрафів на юридичних осіб. Така практика вже давно наявна в державах Європейського Союзу [5, с. 146].

Дуже близьким до поняття захисту персональних даних є поняття їхньої охорони. Це два окремих способи реагування на порушення в даній сфері, але між ними є деяка відмінність у механізмі вчинення дій. За приписом гл. 3 ЦКУ, захист – охоронно-правова реакція особи – носія права на порушення, яке вже відбулося. Способи поведінки надаються в ст. 16 цього акта на вибір потерпілому, хоча, звісно, вони мають бути адекватними характеру та змісту правопорушення. Серед заходів захисту власних персональних даних у разі порушення правил їх оброблення суб'єкт може обрати притягнення володільця, розпорядника чи третьої особи до відповідальності шляхом компенсації збитків, шкоди, припинення договору, стягнення пені, якщо оброблення даних здійснювалася на договірних засадах і такій вид відповідальності був обумовлений сторонами. Відповідальність як правове явище характеризується тим, що в разі її застосування в порушника виникають додаткові обтяження, з'являються нові зобов'язання матеріального або організаційного характеру, які б не виникли в разі належного здійснення регулятивних відносин. Потерпілий також вправі застосувати до порушника його права на приватність у частині неправомірного оброблення персональних даних інші санкції, які мають назву «міри захисту» і не мають характеру відповідальності. До них можна віднести примусові за рішенням суду вчинки з боку порушника: надання доступу до персональних даних (виконання обов'язку в натурі), припинення незаконного оброблення, знищення даних тощо.

Своєю чергою, охорона персональних даних передбачає комплекс позитивних дій, спрямованих на припинення чи унеможливлення правопорушення у сфері обороту інформації про особу. Досить часто такі вчинки мають превентивний характер. Вони зазвичай мають технічний чи організаційний характер і здебільшого спрямовані на забезпечення зовнішнього впливу на сам об'єкт – персональні дані (пошкодження, зміна, знищення тощо) чи несанкціонований до них доступ або поширення. Вчинення таких дій є обов'язком володільця даних. В організаційному плані володільці даних мусять встановити правила доступу до персональної інформації, реєструвати всі дії з нею та фіксувати факти несанкціонованого доступу, а також вжити заходів для відновлення втраченої інформації, яка була знищена чи пошкоджена внаслідок незаконного доступу, зламу або хакерського втручання. З метою обмеження несанкціонованого доступу, запобігання випадковій чи умисній втраті, знищенню даних тощо вони повинні вживати відповідних заходів, а також не допускати розголошення персональних даних, які стали їм відомі у зв'язку з виконанням професійних чи службових, або трудових обов'язків, це так зване зобов'язання конфіденційності (ст. ст. 10, 24 Закону).

Володілець персональних даних самостійно визначає ті заходи, яких треба вживати для забезпечення захисту персональних даних з урахуванням вимог законодавства у сфері інформаційної безпеки.

Джерелом такого законодавства, яке визначає перелік обов'язкових заходів захисту, що мають застосовуватися всіма володільцями, визначено Типовий порядок обробки персональних даних [6]. У п. 2 даного акта зазначені вимоги загального характеру, які є мінімальними у сфері захисту персональних даних, а також вказано, шо способи їх практичної імплементації обираються індивідуальним порядком кожним володільцем. У спеціальних нормативних актах, які регулюють порядок обороту персональних даних в окремих галузях, дані загальні вимоги повинні детальніше прописуватися і конкретизуватися. Наступним кроком має бути належне застосування демократичних приписів. Оскільки в Україні правозастосовна діяльність у царині захисту персональних даних фактично відсутня, а ті справи, які все ж розглядаються, мають відверто протекціоністський характер на користь володільців та розпорядників, особливо коли останні є органами державної чи комунальної влади, суб'єкти персональних даних змушені шукати захист влсних основоположних прав і свобод у міжнародних судових інституціях.

У цьому контексті варто звернутися до практики Європейського суду з прав людини, яким неодноразово розглядалося питання про відповідність реальних заходів стосовно оброблення персональних даних міжнародним стандартам. Так, у справі «Ротару проти Румунії» особа звернулася до Служби розвідки Румунії, яка була володільцем файлу, що містив персональні дані заявника, з вимогою знищити інформацію п'ятдесятилітньої давності про студентські роки заявника, навчання та участь у політичних організаціях. Заявник стверджував, що зберігання такої інформації спецслужбами було незаконним, оскільки на підставі цих матеріалів на нього було сформовано окрему «справу». Європейський суд вивчив національне законодавство Румунії та зазначив, що єдиною підставою для подальшого зберігання старих даних була норма в законі, який регламентував порядок роботи Служби розвідки, згідно з якою вона мала право збирати, зберігати та використовувати інформацію, що має значення для національної безпеки. Але Суд також зазначив, що жоден закон не визначав межі реалізації вказаних повноважень. Законодавство не передбачало, яка інформація може зберігатися, категорії осіб, щодо яких вона може збиратися, обставини, за настанням яких може здійснюватися такий збір інформації, процедури збору, строки зберігання такої інформації. Попри те, що закон встановлював право зберігати та використовувати архіви, отримані від попередніх служб розвідки, у ньому не було визначено, хто має доступ до файлів, як вони можуть використовуватися та який характер цих файлів. Суд також зазначив, що зберігання та використання такої інформації не супроводжувалося відповідними гарантіями від зловживань, зокрема не було незалежного контролю (наприклад, судового) за діяльністю Служби розвідки у цій частині. З огляду на зазначені факти Суд вказав на те, що законодавство, яке регламентувало втручання в права заявника (збереження щодо нього вказаної інформації), не було достатньо передбачуваним. Тому втручання в його права не було законним і порушувало ст. 8 Конвенції [7, п. 59–63].

У справі «Цибутару проти Молдови» порушенням права особи на приватність персональних даних за ч. 1 ст. 8 Конвенції було визнано відмову державних органів змінити у відповідному реєстрі інформацію про національність особи [8, п. 59]. Суд зауважив, що поняття особистої автономії є важливим принципом, що лежить в основі тлумачення гарантій, передбачених ст. 8. За цим принципом, захист надається кожній особистій сфері, серед яких право встановлювати подробиці своєї ідентичності. Етнічна ідентичність також є деталлю, що стосується особистості (п. 49). У певній групі справ, які він розглядає, Європейський суд, окрім вирішення їх по суті, вказує на недосконаліть та недемократичність внутрішнього законодавства країни-учасниці і наголошує на необхідності вчинення дій загального характеру з метою узгодження національного законодавства з демократичними та гуманними канонами. Наприклад, у справі «Гарнага проти України» [9, п. 41] Суд зафіксував факт порушення ст. 8 Конвенції, а також наголосив на невідповідності європейським принципам регулювання коментованих відносин припису українського законодавства щодо неможливості змінити по батькові особи.

Висновки. Необхідно розпочати серйозну нормотворчу роботу з метою конкретизації загальних положень Закону України «Про захист персональних даних» та деталізації механізмів відповідного правозастосування. Наприклад, потребує визначеності порядок надання персональних даних зацікавленим особам та компетентним органам без згоди суб'єкта даних. У нормативному акті недоцільною та навіть шкідливою і такою, що спричиняє зловживання, є розмитість формулювань на кшталт «для виконання повноважень», «для забезпечення авторитету правосуддя» тощо. Правила такої передачі даних мають бути викладені чітко й однозначно. Також необхідно змінити законодавчий підхід до визначення змісту поняття «згода суб'єкта персональних даних». Загальне правило про необхідність інформування людини має бути змінене та доповнене вказівками на зміст такої інформації (про початок збирання й оброблення, передачу, зміну даних тощо), а також стосовно того, що згода має надаватися в письмовій формі (або в іншій, яка може бути зафіксована) та викладатися однозначно.

Важливим кроком для встановлення належної ефективності матеріального законодавства має стати запровадження конкретної відповідальності володільців та розпорядників персональних даних за кожне окреме порушення правил їх обороту. Це може бути, наприклад, штраф на користь суб'єкта персональної інформації. Відповідальність у вигляді законної неустойки та компенсації шкоди повинна бути введена і для посадових осіб органів влади та правосуддя за недотримання вимог про знеособлення персональних даних під час їх публічного поширення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Бугель Н., Никулин А. Защита персональный данных как объект организационно-правового регулирования. Вестник Санкт-Петербургского университета МВД России. 2012. № 2 (54). С. 232 (230–233).

2. Handbook on European data protection law. European Union Agency for Fundamental Rights, 2014. URL: http://fra. europa. eu/ en/publication/2014/handbook-european-data-protection-law.

3. Сухих Н. Персональные данные и философия приватного в нормативных актах. Ценности и смыслы. Государство и право. Юридические науки. 2016. С. 84–93.

4. Обуховська Т. Захист персональних даних в умовах розвитку інформаційного суспільства: передумови, принципи та міжнародне законодавство. Вісник НАДУ. 2014. № 1. С. 95–103.

5. Бем М., Городиський І., Саттон Г., Родіоненко О. Захист персональних даних: правове регулювання та практичні аспекти: науково-практичний посібник. К.: К.І.С., 2015. 220 с.

6. Типовий порядок обробки персональних даних, затверджений наказом Уповноваженого Верховної Ради із захисту прав людини від 8 січня 2014 р. № 1/02–14. URL: http://zakon0.rada.gov.ua/laws/show/v1_02715-14/page.

7. Рішення ЄСПЛ від 4 травня 2000 р. у справі «Ротару проти Румунії» (Rotaru v. Romania), заява № 28341/95. URL: https://swarb.co.uk/rotaru-v-romania-echr-4-may-2000/.

8. Рішення ЄСПЛ від 27 квітня 2010 р. у справі «Цибутару проти Молдови» (Ciubotaru v. Moldova), заява № 27138/04. URL: https://en.wikipedia.org/wiki/Ciubotaru_v._Moldova.

9. Рішення ЄСПЛ від 16 травня 2013 р. у справі «Гарнага проти України», заява № 20390/07. URL: http://zakon2.rada.gov.ua/laws/show/974_960.