10 Пацурківський Ю. П. Правовий режим майна суб'єктів підприємницької діяльності. моногр. / Ю. П. Пацурківський. – Чернівці: Рута, 2001. – 236 с.
11. Покровский И. А. Основные проблемы гражданского права. - 3-е изд., стереотип. - М.: Статут, 2001.
12. Проблемы теории гражданского права / Институт частного права. – М.: Статут, 2003. – 128 с.
13. Средства и методы правового регулирования отношений частной собственности // Общество и право: сб. трудов докторантов, адъюнктов и соискателей. / под общ. ред. В. П. Сальникова. - СПб.: Санкт-Петербургский университет МВД России, 2003. – Вып. 17. - 140 с.
14. Шамсумова Э. Ф. Правовые режимы (теоретический аспект): Дис. … канд. юрид. Наук / Є.Ф. Шамсумова. - Екатеринбург, 2001. - 127 с.

Стаття надійшла до редакції 1.12.2013 р.

Y. P. Patsurkivsky

THEORETICAL PROBLEMS OF UNDERSTANDING THE ESSENCE OF THE LEGAL REGIME OF CATEGORY

This article investigates the problem of understanding the concepts of the legal regime in the general theoretical and sectoral sense. Identified by their common and distinctive features. It is concluded that the formation of the legal regime is a special way of legal regulation. Based on the research formulated the concept of the legal regime. Legal regime should be understood as a special order of legal regulation, expressed in a combination of legal resources: permissions, prohibitions, positive prescriptions, which creates the necessary social status and well-defined degree of favorability or not favorable to the interests of legal subjects.

Keywords: *legal regulation, legal regime, sectoral legal regime means of legal regulation, the legal regime of the object.*

УДК 351.810:340

А. Л. Петрицький

АКТУАЛЬНІ ПРОБЛЕМИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В УКРАЇНІ

У статті здійснено аналіз правового забезпечення захисту персональних даних. Вказується, що саме в цій площині слід шукати витоки численних організаційних проблем механізму захисту персональних даних, оскільки на слабкій правовій базі неможливо побудувати успішну стратегію інформаційної безпеки.

Висвітлено недоліки Закону України «Про захист персональних даних». Чинна редакція Закону характеризується як така, що має велику кількість недоліків, котрі помітно знижують ефективність регулювання відповідної сфери правовідносин. Звертається увага на низку таких суперечливих та дискусійних положень Закону, як не включення до кола суб'єктів регульованих Законом правовідносин держави, віднесення всіх, без винятку, типів персональних даних до інформації з обмеженим доступом тощо. Вказується, що правове забезпечення захисту персональних даних характеризується широким спектром змістовних і структурних недоліків, котрі вимагають якнайшвидшого усунення.

Зроблено висновок про необхідність системного оновлення Закону з урахуванням об'єктивних тенденцій інформатизації суспільства, положень міжнародного законодавства, вимог юридичної техніки, в тому числі, вдосконалення законодавчої

термінології та гармонізації структури Закону, викладення його положень у чіткій логічній послідовності, з урахуванням їхнього характеру, змісту та предметного спрямування.

Ключові слова: *інформація, конфіденційність, персональні дані, захист, правове регулювання.*

Постановка проблеми. Інституціоналізація захисту персональних даних як інтегральної складової державної інформаційної політики, актуалізує питання розробки досконалої нормативної бази, котра б гарантувала стабільність правовідносин, ефективність правозастосування, баланс між правом людини на конфіденційність особистого життя та суспільними інтересами в інформаційній сфері.

Передусім, від якості правового забезпечення залежить стан інформаційної безпеки людини, суспільства, держави. Досконала правова база оптимізує та зміцнює сферу інформаційних відносин, роблячи її толерантною до внутрішніх і зовнішніх загроз. Натомість, вади правової регламентації чинять деструктивний вплив. Вони дестабілізують кореспондуючі соціальні зв'язки, провокують конфлікти між їх суб'єктами, створюють передумови для маніпуляцій, зловживань та утисків.

Саме в площині правового регулювання слід шукати витоки численних організаційних проблем та системних «збоїв» механізму захисту персональних даних. З року в рік зростає кількість випадків несанкціонованого доступу та використання конфіденційної інформації, збільшується число нелегальних інформаційних баз, зростає кількість правопорушень. Вочевидь, ці тенденції матимуть місце доти, доки не буде усунуто системні вади законодавства про захист персональних даних. Адже на слабкій правовій базі неможливо побудувати (і, тим більше, реалізувати) успішну стратегію інформаційної безпеки.

Викладене зумовлює необхідність удосконалення правового захисту персональних даних. З цією метою доцільно провести ґрунтовний аналіз галузевого законодавства, висвітлити пов'язану з ним проблематику, окреслити перспективні напрями його розвитку.

*Аналіз наукових досліджень і публікацій***.** З огляду на широкий резонанс та неабияку суспільну значущість проблематики захисту персональних даних, її ґрунтовним вивченням займалися такі авторитетні правники, як: І. В. Арістова, К. І. Бєляков, В. М. Брижко, М. В. Гуцалюк, В. С. Цимбалюк, М. Я. Швець та інші [1; 2; 3; 4]. Однак наразі широкий комплекс проблем правового забезпечення захисту персональних даних лишається нерозв'язаним, що зумовлює актуальність цієї статті.

*Виклад основного матеріалу***.** Зважаючи на велике розмаїття суспільних відносин у сфері захисту персональних даних, їх регламентація забезпечується широким колом правових актів: Конституцією України, законами України, підзаконними актами Президента України, Кабінету Міністрів України, центральних і місцевих органів виконавчої влади, інших державних органів, а також міжнародними договорами України, згода на обов'язковість яких дана Верховною Радою України.

Однак, безумовно, стрижневим актом інформаційного законодавства є Закон України «Про захист персональних даних», яким урегульовано суспільні відносини, пов'язані із захистом та обробкою персональних даних, захистом основоположних прав і свобод людини та громадянина: права на невтручання в особисте життя, права вимагати вилучення будь-якої інформації про себе та членів своєї сім'ї, права на ознайомлення в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не становлять державної або іншої захищеної законом таємниці.

За висновками міжнародних експертів прийняття цього Закону в 2010 році істотно сприяло соціальному, економічному та науково-технічному прогресу, забезпеченню

балансу прав людини, суспільства й держави в сфері інформації, покращенню нормативно-правового забезпечення захисту персональних даних відповідно до норм міжнародного права та законодавства ЄС, зокрема Страсбурзької Конвенції про захист осіб стосовно автоматизованої обробки даних особистого характеру від 28 січня 1981 року та Директиви 95/46/ЕС Європейського парламенту і Ради від 24 жовтня 1995 р. про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних [5].

Закон має загальносистемний характер і визначає фундаментальні засади обробки та захисту персональних даних в Україні. Його дія поширюється на діяльність щодо обробки персональних даних із застосуванням автоматизованих засобів, а також на обробку персональних даних, які містяться в картотеках чи призначені для внесення до картотек із застосуванням неавтоматизованих засобів.

Охопивши найважливіші аспекти захисту персональних даних, він акумулював загальні та особливі вимоги щодо їх збору, обробки, накопичення, зберігання, використання, поширення, видалення та знищення.

Чимала увага в Законі приділяється питанням доступу до персональних даних. Зокрема, ст. 16 регламентує відповідну процедуру, визначає форму запиту на доступ до персональних даних, закріплює строки його подання та розгляду. У свою чергу, ст. 17 визначає підстави для відстрочення або відмови у доступі до персональних даних, ст. 18 – гарантує право на оскарження рішень про відстрочення/відмову в доступі, а ст. 19 – поряд із правом безкоштовного доступу до інформації про себе, врегульовує питання плати за доступ до персональних даних інших осіб.

Серед позитивних рис Закону варто згадати внутрішню узгодженість, логічну структуру, врахування вимог міжнародного інформаційного законодавства. Навіть вже сам факт його прийняття став вагомим здобутком в контексті виконання Україною своїх міжнародних зобов’язань.

Тим не менш, аналіз ключових положень Закону України «Про захист персональних даних» та практики його застосування не дає особливих підстав для оптимізму. За одностайним визнанням вітчизняних і зарубіжних експертів, чинна редакція Закону характеризується великою кількістю недоліків, котрі помітно знижують ефективність регулювання відповідної сфери правовідносин.

Як зауважує І. Б. Усенко, навіть сама назва Закону не зовсім добре узгоджена з його сьогоднішнім змістом, який здебільшого стосується не всіх питань захисту персональних даних, а лише тих, які пов’язані з їх «обробкою» в електронних базах і картотеках [6]. І хоча наприкінці 2012 року до Закону було внесено зміни, спрямовані на розширення меж його дії (зокрема, остання редакція ст. 5 визнала об’єктом правового захисту будь-які персональні дані, безвідносно до форми систематизації), це питання досі відкрите. Адже, попри оновлення деяких положень, загальна структура Закону лишилась незмінною: сьогодні, як і раніше, він «акцентований» на регламентацію відносин з приводу функціонування відповідних інформаційних баз.

«Вразливим» місцем Закону України «Про захист персональних даних» є термінологічний апарат (див.: ст. 2 Закону), який характеризується багатьма невизначеностями та недостатньою «проробкою».

Зокрема, важко збагнути, чому під базою даних слід розуміти саме іменовану сукупність упорядкованих персональних даних. Невже структуровані інформаційні масиви без власної назви не вважаються картотеками та не підпадають під дію Закону? Гадаємо, це питання риторичне.

До «володільців персональних даних» Закон відносить фізичних або юридичних осіб, яким законом або за згодою суб'єкта персональних даних надано право на обробку цих даних. Знову ж таки, виникає питання, чи не означає це, що з-під дії Закону

«випадуть» особи, які не мають дозволу, але здійснюють обробку персональних даних попри його відсутність. У даному зв'язку слід погодитись з думкою експертів Ради Європи Марі Жоржа та Грема Саттона, які наголошують: «посилання на правову основу права володільця на обробку даних (закон чи згода суб'єкта даних) … слід або видалити з визначення, або викласти в іншій редакції з використанням більш загального формулювання» [7, с. 9].

Крім того, наведене визначення містить очевидне внутрішнє протиріччя. Володільцями персональних даних у ньому визнаються не особи, які мають в своєму розпорядженні/володінні персональні дані, а ті, хто мають право на їх обробку. Отож, з формальної точки зору, володільцем персональних даних може виступати особа, котра ними фактично не володіє (наприклад, суб'єкт, який ще не розпочинав збору інформації). Такий підхід суперечить загальноприйнятому уявленню про «володіння», як «фактичне обладання чимось» [8].

Небездоганними є й інші визначення, наведені у ст. 2 Закону України «Про захист персональних даних». Наприклад, поняття «обробка персональних даних» містить вичерпний і, водночас, недостатньо повний перелік технічних операцій, здійснюваних у рамках обробки. Зокрема, ним не охоплені такі операції з даними, як: пошук, аналіз, упорядкування, комбінування, блокування, стирання тощо. Уявляється, що перелік технічних дій у визначенні має бути «відкритим». Він повинен містити лише типові приклади операцій з обробки, оскільки неможливо навести всі види технічних операцій, які можуть здійснюватися з даними, особливо в світлі невпинного розвитку інформаційних технологій.

Визначення поняття «суб'єкт персональних даних» (фізична особа, стосовно якої відповідно до закону здійснюється обробка її персональних даних) суперечить цілому ряду законодавчих положень, заснованих на тому, що обробка персональних даних може здійснюватись як на підставі чинного законодавства, так і за згодою фізичної особи (див., напр.: абз. 3 ст. 2, ч. 1 ст. 10 та ст. 11 Закону).

Натомість, поняття «одержувач» (фізична чи юридична особа, якій надаються персональні дані, у тому числі третя особа) недостатньо добре узгоджується з Директивою Європейського Парламенту і Ради ЄС від 24.10.1995 №95/46/ЄС, котра містить куди більш детальну дефініцію: «Одержувач – фізична чи юридична особа, орган державної влади, департамент чи будь-який інший орган, якому розкриваються дані, який може бути чи не бути третьою особою».

Перелік дискусійних моментів Закону України «Про захист персональних даних» не вичерпується вадами термінології. Достатньо підстав для критичних зауважень дають й інші його положення.

Наразі Закон не включає до кола суб'єктів регульованих ним правовідносин державу, змушуючи трактувати її як третю особу *(див.: ст. 4)*. Відкритим лишається питання про належність до цього кола суб'єктів міжнародного права, котрі приймають участь у відносинах, пов'язаних з персональними даними.

Впадає у вічі невідповідність абз. 3 ст. 2 та ч. 2 ст. 4 Закону. Якщо перша норма визнає володільцем персональних даних всіх фізичних осіб, яким законом чи договором дано право їх обробки (до речі, аналогічний підхід застосовано в Директиві Європейського Парламенту і Ради ЄС від 24.10.1995 №95/46/ЄС), то згідно з другою – володільцем персональних даних можуть бути лише фізичні особи-підприємці.

Вище вже згадувалось про недоцільність віднесення всіх, без винятку, типів персональних даних до інформації з обмеженим доступом. На жаль, кореспондуючі настанови Ради ЄС при творенні та подальших змінах Закону враховані не були. Як наслідок, будь-які типи персональних даних, навіть найбільш загальні та широковідомі, можуть вважатися конфіденційними. Слід підкреслити, що це системний недолік

вітчизняного інформаційного законодавства, який знайшов відображення і в новій редакції Закону України «Про інформацію». Тож його виправлення можливе тільки в рамках комплексного підходу.

В контексті аналізу відповідних положень Закону (зокрема, ч. 2 ст. 5) виникає питання про коректність терміну «знеособлені персональні дані». Адже, за своєю природою персональні дані передбачають пряму чи опосередковану ідентифікацію особи. Внаслідок знеособлення дана властивість ними втрачається, дані – деперсоніфікуються і, таким чином, перестають бути персональними. Фактично, цей термін містить нерозв'язне протиріччя, що суперечить елементарним правилам формальної логіки.

Недостатньо чіткою та обґрунтованою видається вимога ч. 1 ст. 6 Закону, згідно з якою: «У разі зміни визначеної мети обробки персональних даних суб'єктом персональних даних має бути надана згода на обробку його даних відповідно до зміненої мети, якщо нова мета обробки несумісна з попередньою». Варто зазначити, що критерій сумісності/несумісності є суто відносним, що створює передумови для його вільного тлумачення, як володільцями персональних даних, так і суб'єктами юрисдикційних повноважень. Дана обставина зумовлює ризик маніпуляцій, в ході яких первинна (узгоджена із суб'єктом персональних даних) мета обробки інформації без його згоди може бути змінена на іншу, зовні подібну, але відмінну по суті.

З нашої точки зору, будь-які зміни в цільовому призначенні обробки персональних даних повинні узгоджуватися з їх суб'єктом. Лише такий підхід здатен гарантувати право особи на захист персональних даних та приватність особистого життя.

Взаємовиключаючий характер мають окремі положення ст. 7 Закону, котрою визначаються особливі вимоги до обробки персональних даних. Зокрема, ч. 1 цієї статті містить заборону обробки персональних даних про засудження до кримінального покарання. Натомість, ч. 2, котра встановлює виняток із загального правила, наголошує, що положення частини першої цієї статті не застосовується, якщо обробка персональних даних стосується вироків суду.

У цьому зв'язку слід наголосити, що ст. 8 Директиви Європейського Парламенту і Ради ЄС від 24.10.1995 №95/46/ЄС (здебільшого саме вона лягла в основу відповідних положень Закону), не містить рекомендацій щодо заборони на обробку даних, пов'язаних з правопорушеннями, юридичною відповідальністю та судовою практикою.

Разом з тим, вона передбачає спеціальний режим обробки такої інформації: «Обробка даних, що стосуються правопорушень, обвинувачення у кримінальних справах чи засобів безпеки, може проводитися тільки під контролем офіційного органу або якщо національне законодавство передбачає відповідні спеціальні гарантії, відповідно до національних положень, що передбачають такі гарантії. Однак, повний реєстр обвинувачень у кримінальних справах може вестися лише під контролем офіційного органу. Держави-члени можуть передбачити, що дані про адміністративні санкції чи про судові рішення в цивільних справах теж повинні оброблятися під контролем офіційного органу».

На наш погляд, саме цю нормативну модель потрібно взяти «на озброєння» вітчизняному законодавцю. Адже обробка персональних даних деліктологічного характеру є важливим аспектом функціонування правоохоронної системи, запорукою ефективності планування профілактичних, оперативно-розшукових та інших заходів, спрямованих на боротьбу з деліктністю, охорону громадського порядку, забезпечення особистої безпеки громадян, захист їх прав, свобод і законних інтересів. Зважаючи на це, обробка таких даних повинна являти собою правило, а не виняток (звичайно ж, за умови суворого дотримання гарантій конфіденційності та пов'язаних з ними

обмежень).

Що ж до інших винятків з правила про заборону обробки деяких видів персональних даних, то частина з них потребують уточнення й конкретизації. Зокрема, доцільно розкрити поняття «медичний працівник», яке використовується в п. 6 ч. 2 ст. 7 Закону. Водночас, у п. 7 ч. 2 цієї статті поруч з контррозвідувальною і оперативно-розшуковою діяльністю варто було б зазначити ще й розвідувальну діяльність. Аналогічні зауваження стосуються також ч. 4 ст. 15 та п. 1 ч. 2 ст. 21 Закону України «Про захист персональних даних».

Перелік закріплених у Законі (ст. 8) прав суб'єкта персональних даних в цілому відповідає «букві» і «духу» рекомендацій Ради ЄС, але при цьому містить низку принципових відмінностей. Головна з них полягає в тому, що Закон України «Про захист персональних даних» гарантував право особи знати про місцезнаходження бази персональних даних, яка містить його персональні дані, місцезнаходження та/або місце проживання (перебування) володільця чи розпорядника персональних даних або дати відповідне доручення щодо отримання цієї інформації уповноваженим ним особам, крім випадків, встановлених законом.

У даному зв'язку варто дослухатись до зарубіжних експертів, які застерігають: «право знати місце, де зберігаються дані, може поставити під загрозу безпеку бази даних». І це застереження не марне. Адже ніщо не зобов'язує суб'єкта персональних даних зберігати конфіденційність отриманої інформації. Як наслідок, вона може потрапити, образно кажучи, «не в ті руки» та бути використана для несанкціонованого доступу до бази персональних даних.

Крім того, відповідне положення Закону створює конфлікт суб'єктивних прав: права суб'єкта персональних даних на отримання пов'язаної з ним (його даними) інформації та права фізичної особи-володільця персональних даних на конфіденційність інформації про себе.

Викладене ставить під сумнів необхідність законодавчого закріплення (та й загалом – існування) права суб'єкта персональних даних отримувати відомості про місце знаходження відповідної бази даних, а також про місце знаходження (проживання, перебування) володільця чи розпорядника персональних даних.

Неможливо обійти увагою і той факт, що в тексті Закону деякі права суб'єктів персональних даних сформульовані в спосіб, який суттєво утруднює їх реалізацію та захист на практиці.

Наприклад, гарантуючи право доступу до інформації про себе (в т.ч., право особи знати про місцезнаходження бази персональних даних, яка містить її персональні дані; право отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються її персональні дані; право отримувати не пізніш як за тридцять календарних днів з дня надходження запиту відповідь про те, чи зберігаються його персональні дані у відповідній базі персональних даних, а також отримувати зміст її персональних даних, які зберігаються), Закон не визначає, хто ж саме повинен надавати суб'єкту персональних даних відповідну інформацію: володілець, розпорядник, уповноважений орган з питань захисту персональних даних абощо?

Іншим прикладом є право суб'єкта персональних даних «знати механізм автоматичної обробки персональних даних», закріплене у ч. 12 ст. 8 Закону. Стосовно цієї норми постають одразу два питання: 1) Чи насправді суб'єкту персональних даних потрібна інформація саме про механізм (читай – сукупність засобів) автоматичної обробки інформації? 2) Чому суб'єкт персональних даних наділяється правом знати механізм автоматичної обробки всіх персональних даних, а не лише тих, які стосуються його особисто?

У пошуку відповідей звернімося до Директиви Європарламенту та Ради ЄС від 24.10.1995 №95/46/ЄС, згідно з якою: «Держави-члени гарантують кожному суб'єкту даних право отримати від контролера: … інформацію про логіку, використовувану під час автоматизованої обробки даних, що його стосуються» *(підкреслено мною – А.П.)*. Зі змісту цього положення стає очевидним, що обидва дискусійні моменти ч. 12 ст. 8 Закону України «Про захист персональних даних» зумовлені не стільки практичною доцільністю, скільки невдалим калькуванням рекомендацій ЄС.

Вельми неоднозначний характер має ч. 1 ст. 10 «Використання персональних даних», у якій зазначається: «Використання персональних даних передбачає будь-які дії володільця щодо обробки цих даних, дії щодо їх захисту, а також дії щодо надання часткового або повного права обробки персональних даних іншим суб'єктам відносин, пов'язаних із персональними даними…». Як неважко помітити, ця норма пов’язує процес використання персональних даних виключно з діями володільця, що суперечить ряду інших законодавчих положень (зокрема, у ст. 2, ст.4 та ст. 8 Закону передбачено використання персональних даних не лише володільцем, а й розпорядником).

Крім того, згадана норма вступає у протиріччя з логікою понятійно-категоріального апарату Закону. По-перше, в поняття «використання персональних даних» нею вкладено невиправдано широкий зміст (зокрема, ним охоплюються і захист персональних даних, і їх обробка, і надання права такої обробки іншим суб’єктам). Хоча, наприклад, у тій же ст. 2 Закону використання персональних даних розглядається лише як окремий різновид обробки. По-друге, за Законом право на обробку персональних даних може передаватись не всім суб’єктам відносин, пов'язаних із персональними даними, а виключно розпорядникам. Гадаємо, ця обставина мала б обов’язково знайти відображення в змісті ч. 1 ст. 10 Закону України «Про захист персональних даних».

Суттєвого уточнення потребує й законодавча вимога щодо обов’язкового повідомлення в момент збору персональних даних (або у випадках, передбачених п.п. 2-5 ч. 1 ст. 11 Закону – протягом десяти робочих днів з дня збору персональних даних) суб’єкта персональних даних про володільця персональних даних, склад та зміст зібраних персональних даних, його законні права, мету збору персональних даних та осіб, яким передаються його персональні дані (див.: ст. 12 Закону).

Слушність існування даної вимоги безсумнівна. Однак, цього не можна сказати про абсолютний характер її дії. Як відомо, збір персональних даних здійснюється не лише для задоволення приватних, корпоративних, наукових чи творчих потреб, а й у цілях національної безпеки, оборони, попередження, виявлення та розслідування злочинів тощо. Відповідно, у ряді випадків постає необхідність «закритого» збору персональних даних, що зумовлено специфікою розвідувальної, контр-розвідувальної та оперативно-розшукової діяльності. У таких випадках повідомлення суб’єкта про збір пов’язаної з ним інформації, може призвести до провалу важливих оперативних заходів, поставити під удар інтереси держави, створити загрозу для життя і здоров’я громадян.

З огляду на викладене, вважаємо доцільним закріпити в ст. 12 Закону України «Про захист персональних даних» застереження про те, що передбачені цією статтею вимоги можуть бути обмежені на підставі закону, якщо таке обмеження необхідне в інтересах національної безпеки, оборони, боротьби зі злочинністю, захисту важливих економічних та фінансових інтересів держави, забезпечення особистої безпеки громадян.

Дещо «усіченим» є перелік підстав для видалення або знищення персональних даних. На сьогодні ст. 15 Закону передбачає лише три такі підстави: 1) закінчення строку зберігання даних, визначеного згодою суб'єкта на їх обробку або законом; 2)

припинення правовідносин між суб'єктом персональних даних та володільцем чи розпорядником; 3) набрання законної сили рішенням суду щодо вилучення даних про фізичну особу з бази персональних даних.

Між тим, нею не враховано право суб'єкта відкликати згоду на обробку персональних даних та/або пред'являти вмотивовану вимогу володільцю персональних даних із запереченням проти обробки інформації, котра його стосується. В обох випадках вмотивована вимога суб'єкта персональних даних виключає можливість їх подальшої обробки, а отже – й зберігання володільцем і розпорядником. З огляду на це, єдино можливим правовим наслідком такої вимоги є знищення інформації, що, за логікою, мало б знайти відображення в ст. 15 Закону.

До вразливих місць Закону України «Про захист персональних даних» слід віднести також і недостатньо продуману структуру. Наразі цілий ряд законодавчих положень містяться в статтях, які не відповідають їх змісту, характеру та предметній спрямованості.

Наприклад, за усталеною традицією нормотворення, норма про пріоритет міжнародних договорів України над актами «внутрішнього» законодавства повинна міститись у ст. 3 «Законодавство про захист персональних даних» (а не в ч. 2 ст. 29 Закону, як це має місце зараз). До цієї ж статті варто включити норму, згідно з якою: «Положення щодо захисту персональних даних, викладені в цьому Законі, можуть доповнюватися чи уточнюватися іншими законами, за умови, що вони встановлюють вимоги щодо захисту персональних даних, що не суперечать вимогам цього Закону» (нині це ч. 1 ст. 27).

Водночас, положення, яке обмежує дію Закону та його окремих статей (див.: ст. 25) за логікою свого змісту мало б міститися або у ст. 1 «Сфера дії Закону» (в якості окремої частини), або одразу після неї (в якості самостійної статті).

Висновок. Отже, як свідчить аналіз, правове забезпечення захисту персональних даних характеризується широким спектром змістовних і структурних недоліків, котрі вимагають якнайшвидшого усунення. Першочерговим кроком у даному напрямі має стати внесення до Закону України «Про захист персональних даних» комплексу змін, спрямованих на:

- вдосконалення законодавчої термінології, зокрема, уточнення понять «база персональних даних», «обробка персональних даних», «використання персональних даних», «одержувач» та ін.;
- включення держави та суб'єктів міжнародного права до кола суб'єктів правовідносин, пов'язаних з персональними даними;
- узгодження положень Закону (абз. 3 ст. 2 та ч. 2 ст. 4), якими визначається суб'єктний склад володільців персональних даних;
- вилучення зі змісту Закону та практичного обігу терміну «знеособлені персональні дані», як такого, що містить внутрішнє протиріччя та суперечить правилам формальної логіки;
- запровадження вимоги, згідно з якою будь-які зміни в цільовому призначенні обробки персональних даних (а не лише ті, що є несумісними з раніше узгодженою метою) вимагають обов'язкової згоди їх суб'єкта;
- узгодження права суб'єкта персональних даних на отримання пов'язаної з ним (його даними) інформації з правом фізичної особи-володільця персональних даних на конфіденційність інформації про себе;
- розширення переліку підстав для видалення або знищення персональних даних (до таких мають бути віднесені випадки відкликання суб'єктом персональних даних раніше даної згоди на їх обробку, а також пред'явлення ним вмотивованої вимоги володільцю персональних даних із запереченням проти обробки інформації,

котра його стосується);

- гармонізацію структури Закону, викладення його положень у чіткій логічній послідовності, з урахуванням їхнього характеру, змісту та предметного спрямування.

Список використаної літератури

1. Арістова І. В. Державна інформаційна політика: організаційно-правові аспекти : моногр. / І. В. Арістова. – Х. : Вид-во Університету внутрішніх справ, 2000. – 368 с.
2. Брижко В. М. Організаційно-правові питання захисту персональних даних : автореф. дис... канд. юрид. наук: 12.00.07 - адміністративне право і процес, інформаційне право / В. М. Брижко. – Ірпінь, 2004. – 20 с.
3. Бєляков К. І. Інформатизація в Україні: проблеми організаційного, правового та наукового забезпечення: моногр. / К. І. Бєляков. – К. : КВІЦ, 2008. – 576 с.
4. Інформаційне право та правова інформатика у сфері захисту персональних даних : моногр. / В. Брижко, М. Гуцалюк, В. Цимбалюк, М. Швець; за ред. М. Швеця. – К. : НДЦПІ АПрН України, 2006. – 450 с.
5. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. – Strasburg : European Council, 1981. – 10 p.
6. Усенко І. Коментар до Закону України «Про захист персональних даних» [Електронний ресурс] // Права людини в Україні: інформаційний портал Харківської правозахисної групи. – Режим доступу: http://khpg.org/index.php?id=1330343937
7. Аналіз і коментарі до змін до Закону України про захист персональних даних / М. Жорж, Г. Саттон. – Страсбург, 2012. – 71 с.
8. Большой энциклопедический словарь / сост. И. Лапина, Е. Маталина, Р. Секачев, Е. Троицкая, Л. Хайбуллина, Н. Ярина и д.р. – М. : Астрель, 2002. – 1248 с.

Стаття надійшла до редакції 19.11.2013 р.

A. L. Petrytskyi

ACTUAL PROBLEMS OF LEGAL SECURITY OF PERSONAL DATA PROTECTION

The article presents the analysis of the legal security of personal data protection. It is claimed that in this area should seek the origins of many organizational problems of the mechanism of protection of personal data, since a successful strategy for information security can not be built on a weak legal framework.

The shortcomings of the Law of Ukraine «On the protection of personal data» are highlighted. The current wording of the Law is characterized as having a large number of defects that significantly reduce the effectiveness of legal regulation in that area. Attention is drawn to a number of conflicting and controversial provisions of the Law, as not including in the range of legal entities, governed by the Law, the state; attributing all, without exception, the types of personal data to undisclosed information and more. Specifies that the legal protection of personal data is characterized by a wide range of content and structural deficiencies that require prompt removal.

The conclusion about the need to update the Law is based on objective trends of the information society, the provisions of international legislation and requirements of legal technique. This also includes the improvement of the legal terminology and harmonization of Law structure, an overview of its provisions in strict logical sequence, given their nature, content and subject areas.

Keywords: *information, privacy, personal data protection, legislative regulation.*