УДК 347.2/3
DOI https://doi.org/10.32782/2524-0374/2020-2/28

ОПОСЕРЕДКУВАННЯ ОБОРОТУ Й ОХОРОНИ ПЕРСОНАЛЬНИХ ДАНИХ В АКТАХ ЗАРУБІЖНОГО НАЦІОНАЛЬНОГО ЗАКОНОДАВСТВА

REGULATION OF THE TURNOVER AND PROTECTION OF PERSONAL DATA IN ACTS OF FOREIGN NATIONAL LEGISLATION

Гуйван П.Д., к.ю.н.,
заслужений юрист України, докторант
Національний юридичний університет імені Ярослава Мудрого

Стаття присвячена дослідженню питань правового регулювання збору, зберігання, використання та захисту персональних даних у різних національних легіслатурах. У роботі наголошується, що з кожним роком дедалі більш очевидною є потреба напрацювання та запровадження дієвого механізму захисту особистої інформації громадян. Вона має інтернаціональний характер, бо, по-перше, оборот персональних даних здійснюється у великому обсязі практично в усіх країнах світу, а, по-друге, обіг персональних даних в останні роки набув широкого транскордонного прояву. Тому саме зусилля національних правових систем мають спрямовуватися на вдосконалення законодавства, що регулює вказані питання, дозволяючи громадянам різних держав сприймати інформацію про себе як особисту цінність, яку необхідно берегти. Задля цього національні правові системи мусять використовувати загальні світові демократичні принципи організації захисту прав у сфері персональних даних.

Приділена увага аналізу підходів окремих країн до цього. Відзначено єдність позицій щодо застосування міжнародних усталених принципів захисту особистої інформації з урахуванням її транскордонного обороту. Водночас виділено національні та територіальні особливості нормативного опосередкування таких відносин у різних країнах. На конкретних прикладах внутрішнього законодавства окремих країн ретельно вивчена практика нормування поведінки учасників конкретних відносин. Встановлено, що усі легіслатури визначають право на захист персональних даних як елемент загального основоположного права людини на свободу, яке реалізується в контексті забезпечення недоторканості приватного життя. Загальні засади закріплені у міжнародних договорах і національних актах. Це такі принципи, як законність отримання, обробки і використання інформації; легітимна мета збору; обмеженість строку зберігання, точність; обробка персональних даних виключно за згодою відповідного суб'єкта; захист даних від несанкціонованого доступу тощо. Звісно, у внутрішніх законодавчих документах список принципів-гарантій може бути дещо розширеним, враховуючи національну, релігійну та територіальну специфіку. Але міжнародне співтовариство вказує, що головні засади, визначені в інтернаціональних актах, мають дотримуватися, а додаткові коригування принципів у внутрішньому законодавстві повинні бути достатніми та необхідними для реалізації права людини на персональні дані на засадах свободи та гуманності.

Ключові слова: персональні дані, законна обробка, право на приватність.

The article is devoted to the study of the issues of legal regulation of the collection, storage, use and protection of personal data in various national legal entities. The paper emphasizes that the need to develop and implement an effective mechanism for protecting personal information of citizens is becoming more and more evident every year. It has an international character, because, firstly, the circulation of personal data is carried out to a large extent in almost all countries of the world, and secondly, the circulation of personal data in recent years has become widespread across borders. Therefore, the efforts of national legal systems should be directed at improving the legislation that regulates these issues, allowing citizens of different states to perceive information about themselves as a personal value that must be safeguarded. For this purpose, the national legal systems should apply the general democratic principles of the organization of protection of rights in the field of personal data.

Attention is paid to analyzing individual approaches to this. The unity of positions in the application of internationally established principles of protection of personal information, taking into account its cross-border turnover, was noted. At the same time, national and territorial peculiarities of normative mediation of these relations in different countries are noted. The practice of normalizing the behavior of participants in specific relationships has been carefully studied on specific examples of domestic legislation of individual countries. It is established that all the Legislature defines the right to protection of personal data as an element of the general fundamental human right to liberty, which is implemented in the context of ensuring the privacy of individuals. General principles are enshrined in international treaties and national instruments. These are principles such as the lawfulness of receiving, processing and using information; legitimate purpose of collection; limited storage life, accuracy; the processing of personal data solely with the consent of the person concerned; data protection against unauthorized access, etc. Of course, in the internal legislative documents the list of safeguards may be somewhat broadened, taking into account national, religious and territorial specificities. However, the international community has indicated that the main principles set out in international instruments must be respected, and further adjustments to the principles of domestic law must be sufficient and necessary to exercise human rights to personal data on the basis of freedom and humanity.

Key words: personal data, legal processing, right to privacy.

Соціально-економічні, культурні, політичні та гуманітарні процеси, що відбуваються нині у соціумі, характеризується винятковою ємністю різного характеру відомостей, що належать до різних сфер людської діяльності. Практика взаємин між конкретними людьми, між фізичною особою й органами влади, між господарюючими суб'єктами і людиною забезпечується сучасними можливостями інформаційних і комунікаційних технологій, які об'єктивно дозволяють і формують необхідні технічні передумови для збору, зберігання, використання і поширення інформації особистого характеру. Варто відзначити, що з кожним роком перелік підстав і приводів для збору нових даних збільшується. Росте і обсяг даних про особу, які кваліфікуються як персональні та підлягають обробці уповноваженими суб'єктами. Як наслідок, збільшується загроза неправомірного використання індивідуальної інформації, через що порушуються основоположні права людини. Отже, очевидною є потреба напрацювання та запровадження дієвого механізму захисту особистої інформації громадян. Така потреба має інтернаціональний характер, бо, по-перше, оборот персональних даних здійснюється у великому обсязі практично в усіх країнах світу, а, по-друге, обіг персональних даних в останні роки набув широкого транскордонного прояву. Розвиток міждержавних відносин, глобалізація, дистанційне керування економічними і політично процесами – всі ці тенденції, властиві сучасному світові, неможливі без обміну інформацією, у т. ч. і персонального характеру.

Тож, спираючись насамперед на приписи національного законодавства, що регулює вказані питання, громадяни різних держав сприймають інформацію про себе як особисту цінність, яку необхідно берегти, і з цією метою вони, покладаючись на приписи національної правової системи, можуть отримати реальну допомогу і підтримку у відстоюванні своїх прав у сфері персональних даних. З огляду на міжнародний характер і транскордонний жвавий

обіг особистої інформації важливим є питання про уніфікований підхід до регламентації правил обороту та захисту даних у внутрішньому законодавстві усіх країни, що беруть участь у інформаційному обміні. Для цього необхідно, аби всі держави застосовували схожі принципи регулювання. І тут головними критеріями мають виступати головні міжнародно-правові акти, Конвенції, міждержавні договори, директиви Європейського Союзу та інші подібні акти, які напрацювали сталі та ефективні правила щодо принципів і методології обробки й охорони персональних даних особи. Як показує життя, у багатьох іноземних законодавствах актуальними є питання правової регламентації зберігання, захисту інформації, а також відповідальності за її незаконне розголошення.

У сучасному суспільстві персональна інформація стала одним із найважливіших об'єктів правової охорони та захисту. У багатьох європейських країнах існує поділ персональних даних на дві групи. До першої належать персональні дані загального характеру, а саме: прізвище, ім'я, по батькові, дата та місце народження, громадянство та ін.; до другої групи слід віднести вразливі персональні дані, такі як: стан здоров'я (діагноз), релігійна належність, дані про доходи, фотографії, дані про судимість, ідентифікаційні коди тощо. На відміну від вітчизняного законодавства, європейськими нормативно-правовими актами забороняється зберігання, розповсюдження й обробка саме вразливої частини персональних даних [1].

У юридичній літературі проблемам міждержавного та зарубіжного національного правового регулювання обороту та захисту персональних даних присвятили свої роботи такі науковці, як І. Городиський, І. Бачило, М. Кравчук, С. Гнатюк, А. Марущак, В. Іванський, А. Пазюк, Т. Обуховська, М. Бем, А. Тунік та ін. Але зазначені праці переважно досліджували проблематику з погляду відповідності нормативного регулювання загальносвітовим і європейським стандартам, тоді як практично не вивченим залишилося питання адекватності внутрішніх правил, що опосередковують відносини стосовно збору, зберігання, обробки, використання та захисту персональних даних, національним умовам інформаційного обороту з урахуванням місцевих національних, територіальних, релігійних і культурних особливостей. Аналітичне опрацювання цього правового матеріалу, встановлення загальних підходів і специфіки правотворення у досліджуваній царині становить мету цієї роботи.

Сьогодні у переважній більшості демократичних країн світу питання належного регулювання відносин щодо обігу, використання та захисту персональних даних врегульовані на національному рівні шляхом прийняття спеціальних законів. Одним із перших законодавчих актів щодо захисту персональних даних є німецький Закон землі Гессен «Про захист даних» 1970 р. У ньому задіяно презумпцію, що інформаційні потоки формують «нервовий центр суспільного життя» і володіння інформацією про громадян є «суспільною силою». Оскільки обробка даних без вжиття заходів щодо їх захисту може призвести до негативних наслідків і становить загрозу особистій свободі, вона суперечить інтересам громадянського суспільства. Сфера застосування Закону поширювалася на будь-які дії, пов'язані з отриманням, обробкою, зберіганням і розповсюдженням персональних даних, із використанням традиційних або автоматизованих засобів. Надалі у 1983 р. Федеральний Конституційний суд ФРН вказав на необхідність розробки нормативних документів, спрямованих на захист особистої інформації, що б гарантувало право індивіда знати інформацію про себе, а також про те, яким чином його персональні дані використовуються та розкриваються. Тож у 1990 р. вказаний акт набув статусу Федерального закону про захист даних.

Головною метою закону став захист недоторканності приватного життя при використанні персональних даних. Нормативний акт регламентує збір, обробку і використання персональної інформації, яку збирає держава і недержавні установи. Відповідно до п. 1 § 3 Федерального закону «Про захист інформації» Федеративної Республіки Німеччина під персональними даними розуміється конкретна інформація про особисті або матеріальні обставини ідентифікованої фізичної особи. До даних, які потребують захисту, відповідно до закону ФРН «Про захист персональних даних» належить дещо інший, ніж зазвичай, і більш широкий список, у т. ч. і особливі категорії даних, таких, як: персональні дані про банківські рахунки або кредитні картки; дані, отримані внаслідок професійної діяльності (лікарської, страхової і т. п.); заходи соціального захисту; про адміністративне або кримінальне переслідування і покарання; расове або етнічне походження; політичні погляди; віросповідання або філософське переконання; членство у професійній спілці; здоров'я; інтимне життя. За порушення принципів обробки даних про особу як санкції застосовуються штрафи й ув'язнення. Попри те, що цей закон був прийнятий у ФРН пізніше, ніж у деяких інших європейських державах, він вважається найбільш досконалим порівняно з подібними законодавчими актами інших країн. У 1978 р. у Франції прийнятий закон «Про обробку даних, файли даних і індивідуальні свободи». У ньому, крім визначення ключових понять, підкреслюється, що правове регулювання обробки персональних даних поширюється як на публічний, так і на приватний сектори (ст. 4). Встановлено покарання за порушення. Правопорушники штрафуються, а також можуть отримати тюремний строк до 5 років.

В англосаксонській правовій сім'ї право на захист приватного життя, недоторканність сфери приватного життя іменується «The law of privacy», або «privacy». «Прайвесі» (privacy) – це біопсихічна за своїм походженням і соціокультурна за характером свого розвитку формула захищеності особливої, інтимної сфери приватного життя людини, сфери формування та існування особистості індивіда як стійкої системи соціально-значущих рис, що характеризують індивіда як члена суспільства або спільноти. Наприкінці XIX ст., у 1890 р. науково-правове обґрунтування категорії «прайвесі» вперше було сформульоване у США і був запропонований відповідний концепт, що зводився до формули про право особи «бути залишеною у спокої» («right to be left alone»). Один із авторів цього визначення, суддя Верховного Суду США Луїз Брандез вважав прайвесі найціннішою з демократичних свобод і виступав за те, щоб її особливий статус був відображений у Конституції [2, с. 5]. За сукупністю виконуваних ним соціальних функцій «прайвесі» слід визначити як специфічний соціальний механізм, який суспільство виробляє, аби сприяти цілеспрямованій (тобто соціально релевантній, а не хаотичній або антисоціальній) психічній адаптації особистості до навколишніх соціальних умов і, у підсумку, забезпечити повноцінну інтеграцію індивіда в товариство, не завдаючи шкоди індивідуальності людини. Центральною суспільною функцією цього механізму є захист «соціальної маски» індивіда, тобто того «інформаційного образу», який індивід демонструє соціальному контролю з боку оточуючих [3, с. 134].

Керуючись цим принципом, британський акт про захист персональних даних від 1984 р. в його новій редакції Закону 1998 р. («Закон про захист персональних даних») [4] запроваджує нові правові категорії для формулювання змісту персональних даних. Так, відповідно до припису ст. 1 постулюється термін «Персональні дані» як сукупність інформації про особу, яка поряд із традиційними елементами включає також будь-який вираз думки про особу, але без якоїсь вказівки про наміри користувача даних щодо цієї особи. Інакше кажучи, цей закон надає категоріям «думка» і «намір» правового статусу. Таким чином, будь-який вираз думки про індивіда (суб'єкта

даних) включається до складу персональних даних, тоді як конкретна вказівка на наміри користувача даних щодо суб'єкта даних однозначно виключається зі складу персональних даних (слід підкреслити, що наміри третьої сторони, оскільки вони в явній формі не виключені законом, включаються до складу персональних даних) [5, с. 162].

Значна увага у британському законі приділяється легітимності мети та законності збору даних. Скажімо, у п. 1 ч. 2 цього акта вказується, що визначаючи, чи правильно обробляються персональні дані, слід враховувати спосіб, яким вони отримані, зокрема, чи будь-яка особа, від якої вони отримані, була введена в оману щодо мети чи цілі, для яких вони повинні бути оброблені. При визначенні того, чи будь-яке розголошення персональних даних сумісне з ціллю або цілями, для яких отримані дані, слід враховувати мету, для якої особисті дані призначаються для обробки особою, якою вони розкриті (п. 6 ч. 2). Оброблюваним персональним даним має бути забезпечено адекватний рівень захисту, який є достатнім у всіх обставинах справи, зважаючи, зокрема, на: a) характер персональних даних, b) країну чи територію походження інформації, що міститься в даних, c) країну або територію кінцевого призначення цієї інформації, d) цілі та терміни, протягом яких дані призначаються для обробки, e) закон, що діє у певній країні чи території, f) міжнародні зобов'язання цієї країни або території, g) будь-які відповідні кодекси поведінки або інші правила, які можуть бути застосовані в цій країні або на території (як за правилом, так і за домовленістю у конкретних випадках); h) заходи безпеки, вжиті щодо даних у цій країні чи території (п. 13 ч. 2).

Діяльність щодо регулювання та захисту індивідуальної інформації про особу у США регламентується дещо жорсткіше, ніж у Європі, особливо стосовно даних в інтернет-просторі. Приміром, у Сполучених Штатах визначена кримінальна відповідальність за неналежне зберігання й обробку персональної інформації та її знищення не за законом, тоді як у Європейському Союзі кримінальні справи можуть заводитися тільки у разі завдання шкоди державній безпеці й основним правам громадян. Для європейських держав неналежне поводження з персональними даними переважно віднесено до адміністративних правопорушень. Такий самий підхід спостерігається і в Україні [6, с. 125]. У Канаді в 1985 р. був прийнятий федеральний закон «Акт про захист громадян щодо недоторканості приватного життя (прайвесі) [7]. У главі 7 цього документа, присвяченій захисту особистої інформації, вказується, що особиста інформація, підконтрольна урядовій установі, без згоди особи, якої вона стосується, не може використовуватися установою, крім a) для цілей, для яких інформація була отримана або складена установою або для використання відповідно до цієї мети; або b) для цілей, за якими ця інформація може бути розкрита установі. Особисті дані, що знаходяться під контролем державної установи, без згоди особи, якої вона стосуються, не повинні розголошуватися інститутом, крім випадків, передбачених цим розділом. В іншому законі Канади «Акті про доступ до персональних даних» [8] регулюються механізми отримання даних про особу, які зберігаються у відповідних електронних чи картотечних базах. Враховуючи національну специфіку країни, встановлено правило, за яким, якщо доступ до запису або його частини має бути наданий відповідно до цього Закону, а особа, яка звертається, має отримати доступ певною офіційною мовою, копія запису або її частини повинна бути надається людині цією мовою a) негайно, якщо запис або його частина вже існує під контролем державної установи цією мовою; або b) протягом розумного періоду часу, якщо керівник державної установи, яка контролює цей запис, вважає, що це відповідає суспільним інтересам, щоб він міг підготувати переклад (ст. 12).

Серед європейських країн маємо згадати Закон Чеської республіки № 101 від 4 квітня 2000 р. «Про захист персональних даних». У ньому чітко визначений обсяг зобов'язань операторів та обробників даних про особу. Так, оператор зобов'язаний: точно визначити мету, заради якої персональні дані повинні бути оброблені; точно визначити засоби і способи обробки персональних даних; обробляти тільки точні персональні дані, отримані відповідно до цього закону. У разі необхідності оператор зобов'язаний оновити дані. Якщо оператор вважає, що оброблювані дані неточні щодо встановленої мети, то він у розумні терміни вживає відповідних заходів, зокрема блокує обробку і виправляє або доповнює персональні дані, в іншому разі він повинен знищити персональні дані. Збирання персональних даних мусить відбуватися відповідно до точно встановленої мети і в межах, необхідних для виконання точно встановленої мети тільки протягом необхідного для мети їх обробки періоду часу. Після закінчення цього періоду персональні дані можуть бути збережені тільки для цілей державної статистичної служби, а також для наукових і архівних цілей. Обробляти персональні дані слід лише відповідно до мети, заради якої вони були зібрані.

Забороняється збирання даних під приводом якихось інших цілей або діяльності; необхідно також гарантувати, що зібрані для різних цілей персональні дані не будуть зводитися в загальну базу. Оператор може обробляти персональні дані лише за згодою суб'єкта даних (ч. 1, 2 ст. 5). За правилом ст. 13 цього закону оператор і обробник зобов'язані вжити заходів, що попереджають як неправомочний або випадковий доступ до персональних даних, їх зміну, руйнування або втрату, неправомочну передачу, іншу незаконну обробку, так і інше неправильне використання персональних даних. Цей обов'язок залишається в силі після припинення обробки персональних даних. Оператор або обробник зобов'язаний створювати і документувати технічно-організаційні заходи, що вживаються і здійснюються для забезпечення захисту персональних даних відповідно до закону та інших нормативних актів.

Заслуговує на увагу Іспанський «Органічний закон про захист персональних даних» [9]. Він спирається на основні принципи регулювання обороту даних, яких дотримується Європейська спільнота. Так, у ст. 4 вказується, що особисті дані можуть бути зібрані для обробки та пройти таку обробку, лише якщо вони є адекватними, відповідними та не надмірними щодо обсягу і зазначеної, явної та законної цілі, для якої вони були отримані. Особисті дані, що піддаються обробці, не можуть використовуватися для цілей, несумісних із тими, для яких вони були зібрані. Особисті дані повинні бути точні й оновлені таким чином, щоб надати справжню картину про поточне становище суб'єкта даних. Якщо записані особисті дані виявляються неточними повністю або частково, або неповними, вони повинні бути стерті й офіційно замінені чи відповідно виправлені без шкоди для прав, наданих суб'єктам даних. Особисті дані видаляються, коли вони перестають бути необхідними або актуальними для мети, для якої вони були отримані або записані. Вони не повинні зберігатися у формі, яка дозволяє ідентифікувати суб'єкта даних довше, ніж це необхідно для цілей, для яких вони були отримані або записані. Особисті дані зберігаються таким чином, щоб це дозволило здійснити право доступу до них. Збір даних шляхом шахрайських, несправедливих або незаконних засобів заборонений.

За правилом ст. 5 цього закону суб'єкти, від яких вимагаються персональні дані, повинні бути попередньо поінформовані явно, точно й однозначно про: a) наявність операції з обробки файлів або персональних даних, мету збирання даних і одержувачів інформації; б) обов'язковий або добровільний характер відповіді на поставлені запитання; в) наслідки отримання даних або відмову в наданні ними даних; г) можливість здійснення прав на доступ, виправлення, стирання та заперечення; e) осіб та адресу контролера або його представника, якщо такі є; там, де контролер не створений на території Європейського

Союзу, і він є використовувачем засобів обробки, що знаходяться на території Іспанії, він повинен, якщо це не означає використання для транзитних цілей, призначити представника в Іспанії, без шкоди до будь-яких дій, які можуть бути вжиті проти самого контролера.

У Фінляндії прийнято спеціальний закон, що регулює обробку і використання персональних даних громадян, пов'язаних із діяльністю поліції [10]. За цим документом встановлюється перелік даних, які можуть бути записані в систему даних про ідентичність осіб, котрі підозрюються у вчиненні злочину або підлягають досудовому розслідуванню чи примусовому заходу. Вони складаються з таких, як прізвище, дата народження особи, код особи, стать, мова, національність, сімейний стан, країна народження, муніципалітет (резиденція) при народженні, професія, адреса та номер телефону або інші контактні дані, інформація про смерть особи, інформація про туристичний документ (для іноземця) та будь-які особисті дані, що стосуються власної безпеки особистості (ч. 2 розділу 2 Глави 2).

У Росії також прийнято Федеральний Закон «Про персональні дані» [11]. У ньому приділено увагу заходам щодо забезпечення безпеки персональних даних при їх обробці. Законом визначається перелік таких заходів, а також передбачається, що рівні захищеності персональних даних при їх обробці в інформаційних системах персональних даних, вимоги до їх захисту, а також до матеріальних носіїв біометричних персональних даних і технологій їх зберігання поза інформаційних систем встановлюються не тільки державою в особі уряду Російської Федерації, а й асоціаціями, спілками та іншими об'єднаннями операторів з урахуванням своєї діяльності. У чинній нині редакції закону наведено вичерпний перелік випадків обробки персональних даних. Також вказано широкий перелік випадків, у яких не потрібне отримання згоди на обробку персональних даних від суб'єктів персональних даних. Наприклад, у випадках, коли обробка персональних даних необхідна для виконання договору, стороною якого або вигодонабувачем або поручителем за яким є суб'єкт персональних даних, а також для укладення договору з ініціативи суб'єкта персональних даних або договору, за яким суб'єкт персональних даних буде вигодонабувачем або поручителем. Визначено низку основних засад, якими має керуватися володілець (розпорядник) особистої інформації. Так, обробка повинна здійснюватися на законній основі; вона мусить обмежуватися досягненням конкретних, заздалегідь визначених і законних цілей; не допускається об'єднання баз даних, що містять персональні дані, обробка яких здійснюється, несумісних між собою; обробці підлягають дані про особу, що відповідають цілям їх обробки; зміст і обсяг оброблюваних даних повинні відповідати заявленим цілям обробки; оброблювані інформаційні відомості особистого характеру не повинні бути надмірними щодо заявлених цілей їх обробки; при обробці повинні бути забезпечені точність даних, їх достатність; зберігання персональних даних має здійснюватися не довше, ніж цього вимагають цілі обробки.

Крім країн Європи й Америки, інші держави також розробляють і використовують норми національного законодавства, аби забезпечити гарантованість права громадянина на приватність, зокрема в частині захисту його персональних даних. Так, «Закон про захист персональних даних» ПАР, який набрав чинності в 2013 р., під персональними даними розуміє інформацію, що стосується ідентифікованої, живої, фізичної особи, а також, якщо це може бути застосовано, до ідентифікованої існуючої юридичної особи [12]. Там само дається перелік інформації, яка вважається персональною. Особиста інформація охоплює: вік, стать, фізичне або психічне здоров'я, добробут, інвалідність; медичну / фінансову історію; ідентифікаційний номер, електронну пошту, фізичну адресу, номери телефонів; біометричну інформацію, наприклад, ДНК, відбиток пальців, тип крові; особисті думки, погляди, уподобання людини; відповідність особистого або конфіденційного характеру; погляди або думки іншої особи про людину; ім'я особи. У ст. 5 цього закону утверджено правило, згідно з яким суб'єкт даних має право обробляти особисту інформацію відповідно до умов законної обробки особистої інформації, включаючи право отримувати повідомлення про те, що особиста інформація про нього збирається, або його особиста інформація була доступна або придбана від несанкціонованої особи; встановити, чи відповідальна сторона має таку інформацію, та мати доступ до особистої інформації; вимагати, у разі необхідності, виправлення, знищення чи видалення особистої інформації; заперечувати з розумних підстав, що стосуються його конкретної ситуації щодо обробки; вимагати не обробляти його особисту інформацію, для цілей прямого маркетингу за допомогою небажаних електронних комунікацій; подати скаргу до Регулятора стосовно передбачуваного втручання щодо захисту особистої інформації будь-якого суб'єкта даних або подання скарги регулятору щодо визначення судді; порушити цивільний позов щодо передбачуваного втручання в захист його особистої інформації. Серед країн Азії слід згадати Гонконг, який 24 жовтня 1995 р. прийняв закон про захист персональних даних і на його основі закони «Про практику стосовно номерів посвідчення особи» та «Про дані стосовно кредитоспроможності споживачів».

Із проведеного дослідження можемо зробити певні висновки. Вивчаючи міжнародно-правове та зарубіжне національне регулювання персональних даних, слід виділити основні тенденції, яких дотримується вказане нормативне забезпечення. Всі без винятку легіслатури визначають право на захист персональних даних як елемент загального основоположного права людини на свободу, яке реалізується в контексті забезпечення недоторканості приватного життя. Законодавства різних країн і навіть різних континентальних організацій одностайні у визначенні основоположних принципів щодо регулювання механізмів збору, зберігання, обробки та захисту персональних даних. Ці принципи обов'язково закріплені у міжнародних загальних і галузевих договорах та національних актах. Це такі засади, як законність отримання, обробки і використання інформації; легітимна мета збору; обмеженість строку зберігання, точність; обробка персональних даних виключно за згодою відповідного суб'єкта; захист даних від випадкового доступу, несанкціонованого знищення чи випадкової втрати інформації; відкритість і гласність процесу обробки даних, поінформованість суб'єкта особистої інформації про кожну дію, яка вчиняється; забезпечення права доступу особи до персональної інформації стосовно неї; права перевірки і внесення змін у свої дані тощо. Звісно, у внутрішніх законодавчих документах список принципів-гарантій може бути дещо розширеним, враховуючи національну, релігійну та територіальну специфіку. Але міжнародне співтовариство вказує, що головні засади, визначені в інтернаціональних актах, мають дотримуватися, а додаткові коригування принципів у внутрішньому законодавстві повинні бути достатніми та необхідними для реалізації права людини на персональні дані на засадах свободи та гуманності.

ЛІТЕРАТУРА

1. Цісар Г.І. Захист персональних даних в умовах сучасного інформаційного суспільства. URL: http://www.legalactivity.com.ua/index.php?option=com_content&view=article&id=1394%3A061216-01&catid= 167%3A2-1216&Itemid=208&lang=ru

2. Свобода інформації та право на приватність в Україні. Т. 2. Право на приватність: conditio sine qua non. Харківська правозахисна група; Харків : Фоліо, 2004. С. 5.
3. Иванский В.П. Правовая защита информации о частной жизни граждан (опыт современного правового регулирования). Москва : Изд-во РУДН, 1999. 276 с.
4. Data Protection Act 1998. URL: http://www.legislation.gov.uk/ukpga/ 1998/29/contents.
5. Иванский В.П. Правовое регулирование персональных данных в законодательстве зарубежных государств. *Вестник РУДН. Серия Юридические науки*. 2012. № 1. С. 156–168.
6. Кравчук М. Міжнародний досвід правового регулювання захисту персональних даних у мережі Інтернет. *Наукові записки Інституту законодавства Верховної Ради України*. № 3. С. 123–126.
7. Privacy Act (R.S.C., 1985, c. P-21). URL: Privacy Act (R.S.C., 1985, c. P-21)laws-lois.justice.gc.ca/eng/acts/p-21/page-2.html#h-6.
8. Access to Information Act (R.S.C., 1985, c. A-1). URL: http://laws-lois.justice.gc.ca/eng/acts/A-1/FullText.html.
9. Organic law on the Protection of Personal Data (Madrid, 13 December 1999). URL: www.legislationline.org/documents/id/9044.
10. Act on the Processing of Personal Data by the Police (761/2003). URL: http://www.legislationline.org/topics/country/32/topic/3.
11. Федеральный закон РФ от 27 июля 2006 г. № 152 «О персональных данных». URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102108261.
12. Act No. 4 of 2013 Protection of Personal Information Act, 2013 Cape Town, Kaapstad, 26 November 2013 № 37067. URL: http://www.cao.ac.za/ download/POPI_2013-004.pdf.