ISSN 1998-4758 • Часопис Академії адвокатури України | том 7 | №2(23) 2014

UDC | УДК : 342.723:340.5(477)

ЗАСТОСУВАННЯ ЗАРУБІЖНОГО ДОСВІДУ ПРАВОВОГО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В УКРАЇНІ

В. І. ТЕРЕМЕЦЬКИЙ*
доктор юридичних наук,
доцент кафедри цивільно-правових дисциплін,
Харківський національний університет внутрішніх справ

Д. В. ЦВІРЮК
здобувач кафедри загальноправових дисциплін,
Харківський національний університет внутрішніх справ;
суддя Дзержинського районного суду м. Харкова

✉ *зв'язок з авторами: **vladvokat@bk.ru**

Анотація: В статті автори розглядають позитивний досвід окремих зарубіжних країн, які мають багаторічну практику і розвинуте законодавство з питань захисту персональних даних. Розглядається, зокрема, діюча в США – країні, що була першою державою, яка ще у 1964–1965 рр. зайнялася проблемами захисту персональних даних – концепція захисту інформації незалежно від носія такої інформації; найважливіші принципи щодо регулювання суспільних відносин у сфері захисту персональних даних: відповідальність, ідентифікація мети, точність, особистий доступ та ін.

Проаналізовано законодавство у сфері захисту персональних даних Канади, Великобританії, Німеччини, Франції, а також країн колишнього СРСР: Російської Федерації, Республіки Азербайджан, Республіки Вірменії, Республіки Молдова та ін.

Висловлені пропозиції про можливість використання в Україні позитивного досвіду інших країн щодо захисту персональних даних.

Ключові слова: захист персональних даних; зарубіжний досвід; реєстри користувачів персональних даних; біометричні документи

APPLICATION OF FOREIGN EXPERIENCE RELATED TO LEGAL PERSONAL DATA PROTECTION IN UKRAINE

TEREMETSKY V.[1], TSVIRYUK D.[2]

1 – Dr. of Law, Assist. Professor, Kharkiv National University of Internal Affairs (Contacting author)*
2 – Researcher, Kharkiv National University of Internal Affairs; Judge, Dzerzhinsky District Court of Kharkiv

Abstract

The authors examine the positive experience of some foreign countries, which have long-term practice and developed legislation related to personal data protection. The study considers, in particular, the operating of personal data protection in the USA, the first state which in 1964 – 1965 started to deal with problems of personal data protection – the concept of information security irrespective of the data carrier as well as the most important principles of regulation of the public relations in the sphere of personal data protection: responsibility, purpose identification, accuracy, personal access, etc.

Розбудова інформаційного суспільства у будь-якій країні пов'язана, як з розвитком комп'ютерних технологій, так і з розширенням прав людини. Одним із проявів цього є розробка системи захисту персональних даних при їх автоматизованій обробці. Слід зазначити, що за останні 30 років більш ніж у 20 країнах світу були прийняті нормативно-правові акти із захисту персональних даних, у котрих закріплені реальні механізми правого регулювання обігу такої інформації [1]. Кожна держава визначає власні засади правового регулювання захисту персональних даних, завдяки чому формується значний світовий досвід із вказаної проблематики.

Аналіз наукової літератури дозволяє нам стверджувати, що проблеми захисту персональних даних у зарубіжних країнах досліджувалися у працях А. А. Баранова, В. М. Брижка, А. В. Кучеренко, А. В. Пазюка, К. М. Рудой, В. П. Радкевича, А. В. Туніка, А. М. Чернобай та інших вчених. Утім, не дивлячись на широкий спектр наукових публікацій з цього питання, багато аспектів у цій сфері ще не дістали належного осмислення, залишаючись дискусійними. До того ж, на жаль, і нині в нашій країні показники ефективності захисту персональних даних є недостатньо високими, а витрати на здійснення такого захис-

The legislation in the sphere of personal data protection in Canada, Great Britain, Germany, France, and the countries of the former USSR (Russian Federation, Republic Azerbaijan, Republic of Armenia, Republic of Moldova) has also been analyzed.

There has been offered the possibility of using the positive experience of other countries in Ukraine. It is proposed to amend the Law of Ukraine "On protection of personal data" taking into account that personal information also includes biometric documents of the natural person. There has been substantiated a proposal to establish a Register of personal data users, who are the "third party" with the access to personal data, and to create the Register of personal data owners, which will reflect data on such subjects and provide for their registration procedure. The authors support the ban to compile a personal data for Internet resources about children under age of 14 without consent of their parents.

Keywords: data protection; international experience; Register of personal data users; biometric documents

ПРИМЕНЕНИЕ ЗАРУБЕЖНОГО ОПЫТА ПРАВОВОЙ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В УКРАИНЕ

ТЕРЕМЕЦКИЙ В.И.[1], ЦВИРЮК Д.В.[2]

1 – доктор юридических наук, Харьковский национальный университет внутренних дел
2 – соискатель, Харьковский национальный университет внутренних дел; судья Дзержинского районного суда г. Харькова

Аннотация: В статье авторы рассматривают позитивный опыт отдельных зарубежных стран, которые имеют многолетнюю практику и развитое законодательство по вопросам защиты персональных данных. Рассматривается, в частности, действующая в США – государстве, где еще в 1964–1965 гг. начали заниматься проблемами защиты персональных данных – концепция защиты информации независимо от носителя такой информации; важнейшие принципы регулирования общественных отношений в сфере защиты персональных данных: ответственность, идентификация цели, точность, личный доступ и др.

Проанализировано законодательство в сфере защиты персональных данных Канады, Великобритании, Герту продовжують залишатися значними. Тому метою цієї статті є дослідження зарубіжного досвіду правового захисту персональних даних і розробка пропозицій щодо запозичення певних ідей та інститутів для оптимізації методів і форм захисту персональних даних в Україні.

При розгляді зарубіжного досвіду правового регулювання персональних даних конструктивним для адаптації у національне законодавство є можливість забезпечення механізмів, які дозволяють суб'єкту персональних даних контролювати зміст і наявність його персональних даних, а також вимагати їх виправлення; обмеження обсягу і меж використання персональних даних переліком цілей, для котрих вони призначені, які не можуть бути змінені без згоди суб'єкта персональних даних; посилений режим охорони особливих категорій персональних даних (національна приналежність, погляди і переконання, здоров'я та інтимне життя) [2, 148].

Без дослідження регулятивних підходів окремих країн Європи, Сполучених Штатів Америки та інших демократичних держав, які мають розвинуте законодавство і багаторічний досвід з питань захисту прав та свобод людини, в тому числі права на захист персональних даних, ускладнюється розуміння сучасних проблем правового регулювання відносин із захисту відомостей про особу [3, 11]. Удосконалення національного законодавства можливе лише після детального вивчення й аналізу відповідної зарубіжної нормативної бази, виявлення в ній переваг та недоліків.

На сучасному етапі розвитку інформаційної сфери життя суспільства, різні держави активно взаємодіють між собою з економічних, політичних, оборонних й інших питань, що обумовлює необхідність взаємодії інформаційних систем цих країн [4, 131]. Подібні тенденції вказують на пріоритетність зазначеної сфери суспільного життя та актуальність проблем захисту інформації персонального характеру.

Без сумніву, країною з найрозвинутішою системою захисту інформаційного простору можна вважати США, оскільки її інформаційне законодавство – це найкращий приклад та орієнтир у сфері захисту персональних даних, на якому необхідно будувати вітчизняне законодавство у цій сфері. Основою нормативно-правового регулювання захисту персональних даних у США є Закон «Про свободу інформації» (The Freedom of Information Act) 1966 р. [5] та Закон «Про надання кредитної інформації про покупця» (The Fair Credit Reporting Act) [6]. Окрему увагу привертає Закон США «Про конфіденційність» (The Privacy Act) 1974 р., головною метою якого є створення умов для запобігання випадків протиправних дій з боку органів влади та державних інституцій у сфері використання інформації персонального характеру [7]. Фактично, цей Закон

мании, Франции, а также стран бывшего СССР: Российской Федерации, Республики Азербайджан, Республики Армения, Республики Молдова и др.

Высказаны предложения о возможности использования в Украине позитивного опыта других стран. Предлагается дополнить Закон Украины «О защите персональных данных» положением о том, что персональными данными также являються биометрические документы физического лица. Обосновано предложение о создании реестра пользователей персональных данных, то есть третьих лиц, которым был предоставлен доступ к сведениям персонального характера, и создать реестр владельцев персональных данных, который будет отражать сведения о таких субъектах и предусматривать для них процедуру регистрации. Обосновывается также запрет собирать для интернет-ресурсов персональных данных о детях возрастом до 14 лет без согласия на это их родителей.

Ключевые слова: защита персональных данных; зарубежный опыт; реестры пользователей персональных данных; биометрические документы

❖ ❖ ❖

став своєрідним прикладом для започаткування законотворчості у сфері захисту відомостей про особу не тільки в США, а й в інших країнах світу.

Політика США у сфері захисту персональних даних має комплексний характер, оскільки в державі прийнято значну кількість нормативно-правових актів, які регламентують питання захисту інформації персонального характеру в окремих сферах суспільного життя. Так, Закон «Про право на фінансову приватність» (The Rightto Financial Privacy Act) 1978 р., регламентує аспекти конфіденційності фінансових запитів, які систематизуються у різних банківських структурах [8]. Мова йде про встановлення заборони надання інформації персонального характеру державним установам за винятком випадків, коли відомості потрібні для проведення судового або адміністративного розслідування чи реалізації іншої законної діяльності.

Яскравим прикладом системної політики щодо захисту персональних даних у США є Закон «Про захист конфіденційності відеоматеріалів» (The Video Privacy Protection Act) 1980 р. [9]. Закон «Про захист користувачів кабельних мереж» (The Cable Television Consumer Protectionand Competition Act) 1992 р. [10]. Вважаємо, що в умовах інформатизації вказані нормативно-правові акти відіграють важливу роль у гарантуванні прав людини та громадянина на захист персональних даних і особисту недоторканість.

Слід зазначити, що у США діє концепція захисту інформації незалежно від носія такої інформації, а, отже, її захист здійснюється на загальних підставах (як і матеріальних цінностей). Ця концепція, як відзначають Д. П. Василенко та В. І. Маслак, реалізується через стандарт «CSA», прийнятий у 1996 р. [4, 128].

Зазначений стандарт поширюється на всі країни – члени НАТО і містить низку найважливіших принципів щодо регулювання суспільних відносин у сфері захисту персональних даних, а саме:

1) відповідальність – організація несе відповідальність за ті персональні дані, що знаходяться під її контролем, і має призначати особу або осіб, які стежать за відповідністю дій організації принципам законодавства;

2) ідентифікація мети – мета, для якої збирається інформація, має бути ідентифікована організацією до початку процесу збирання інформації;

3) згода – усвідомлення та згода особи на збирання інформації про неї є обов'язковою умовою збирання, використання чи поширення (розкриття) персональних даних, крім випадків, де це недоречно;

4) обмежене збирання – збирання персональної інформації має бути обмежене метою, яка визначена (ідентифікована) організацією. Інформація може збиратися лише для справедливої та законної мети;

5) обмежене використання, поширення, зберігання (персональна інформація має використовуватися або поширюватися лише з тією метою, для якої вона була зібрана, окрім випадків згоди особи або вимоги закону. Персональна інформація не повинна зберігатися довше, ніж це необхідно для досягнення зазначеної мети;

6) точність – персональна інформація має бути точною, повною та сучасною, щоб досягти мети, для якої інформацію було зібрано;

7) безпека – персональна інформація має бути захищена за допомогою забезпечення такого рівня безпеки, який відповідає вимогам «чутливості» інформації;

8) відкритість – організація має зробити доступною для особи специфічну інформацію про політичне та практичне відношення організації до управління персональною інформацією;

9) особистий доступ – особа має бути проінформована про існування, використання та поширення персональної інформації про неї з наданням на її вимогу доступу до інформації. Особі має бути надана можливість перевірити точність і повноту інформації та виправити таку інформацію в разі необхідності;

10) перевірка відповідності – особа повинна мати можливість направити запит щодо перевірки відповідності операцій із персональними даними принципам законодавства [4, 128].

Таким чином, розглянутий стандарт містить положення, які схожі за змістом з підставами та вимогами до обробки відомостей про фізичну особу, що містяться у ст.ст. 6, 7 та 11 Закону України «Про захист персональних даних».

Як зазначає Н. В. Кушакова, «закони, які приймає американський Конгрес, стосуються конкретних проблем (прецедентів), що виникають у процесі активного використання інформаційних технологій, зокрема мережі Інтернет, а також спрямовані на захист права на інформацію чи можливих його обмежень у зв'язку з виявленням негативного впливу на інших членів суспільства чи суспільства в цілому» [11, 131]. Такий принцип, є позитивним, оскільки узагальнення судової практики та використання її для удосконалення законодавства, гарантує отримання бажаного результату, а саме ефективних механізмів захисту персональних даних. Слід зауважити, що в Україні судова практика не отримала належного розвитку як джерела удосконалення засобів правового регулювання сфери персональних даних, адже рішення судів не мають прямого впливу на вітчизняне законодавство у сфері обігу інформації персонального характеру.

Політика США у сфері охорони й захисту персональних даних та інформації здійснюється Агентством Національної Безпеки (далі – АНБ). Найбільш важливі стратегічні питання інформаційної безпеки розглядаються на рівні Ради національної безпеки, а рішення оформляються у вигляді директив Президента. До такого типу директив відносяться: PD/NSC-24 «Політика в галузі захисту систем зв'язку» [12], в якій зазначається необхідність захисту важливої несекретної інформації; SDD-145 «Національна політика США у галузі безпеки систем зв'язку в автоматизованих інформаційних системах» [13]. Вимоги цієї директиви покладають на АНБ функції захисту інформації й контролю за безпекою на каналах зв'язку та в інформаційно-телекомунікаційній системах.

Важливим чинником у сфері забезпечення захисту персональних даних громадян, стало прийняття Закону «Про захист приватної інформації про особу» [14]. У подальшому вказаний закон було деталізовано Федеральним Законом «Про захист онлайнових персональних даних дітей» (COPPA), що регулює використання персональної інформації в Інтернеті [15]. Цим законом встановлено заборону збирати персональні дані про дітей віком до 13 років без згоди на це їх батьків, а, отже, Закон регулює відносини щодо збирання та використання інформації про малолітніх. Він також визначає обов'язкові правила для інтернет-ресурсів, які збирають персональну інформацію про дітей. Ці ресурси мають подавати відомості, для чого вони збирають інформацію і яким чином захищатимуть її. Зазначимо, що при реєстрації на певних сайтах особа в обов'язковому порядку засвідчує свій вік. У разі невідповідності віку доступ до того чи іншого ресурсу не надається. Думка

О. П. Радкевича, що тут виникає проблема перевірки достовірності вказаних відомостей є слушною [16, 144]. Вважаємо, що спираючись на позитивний досвід США, необхідно на законодавчому рівні запровадити заборону збирання персональних даних соціальними мережами та обмеження щодо переліку відомостей, які особа надає у разі реєстрації на інших Інтернет ресурсах.

Необхідність обмеження переліку відомостей про персональні дані у мережі Інтернет пов'язано з тим, що, по-перше, спілкування в соціальних мережах не передбачає необхідність ідентифікації особи, тобто люди спілкуються заради спілкування, а отже у разі виникнення потреби особистої зустрічі, вони можуть самостійно домовитися про неї, наприклад, обмінявшись телефонами чи призначивши місце такої зустрічі. По-друге, соціальна мережа не є володільцем персональних даних, адже не має чіткої мети їх обробки, оскільки створена для задоволення інформаційних потреб суспільства та не використовує персональні дані користувачів. По-третє, інші Інтернет ресурси, наприклад, Інтернет магазини, яким персональні дані необхідні для здійснення пересилки товарів, можуть обмежитися ім'ям та телефоном замовника, оскільки усі інші дані (адреса проживання, прізвище) можна встановити у режимі телефонного зв'язку.

Подібна практика сприятиме захисту інформації персонального характеру, особливо враховуючи те, що ті самі соціальні мережі та Інтернет ресурси не мають можливості забезпечити надійний та ефективний захист персональних даних. Отже, слід погодитися із думкою Л. В. Борисової та В. В. Тулупова, що США були першою державою, яка зайнялася проблемою захисту персональних даних. Початок такої діяльності було покладено у 1964-1965 рр., роботами комісії Конгресу «ЕОМ і порушення секретності» й набуло подальшого розвитку у 1966 р., коли сенатор Дж. Маккарті запропонував Білль про ЕОМ і про права, котрий став основою для урядової пропозиції 1967 р., що відома як «Правила про секретність». Розділ VI цих Правил «Дані про особу» надав кожному громадянину право знати зміст файлу, який його стосується, і ввів просту процедуру для виправлення можливих помилок. У 1974 р. було прийнято Закон «Про охорону особистих таємниць», котрий регламентував доступ до інформаційних матеріалів, що зберігаються в державних органах США [17, 96].

Продовжуючи дослідження можливого для використання в Україні досвіду інших країн світу, значний інтерес викликає Канадський Закон «Про охорону персональної інформації», який передбачає реальні механізми захисту персональних даних та реалізації права на доступ до відомостей про себе. Згідно з цим Законом під персональною розуміється інформація про конкретну фізичну особу (за винятком особи, яка була або є співробітником державної установи, її посаду, службову адресу та телефон, рівень зарплати та службові обов'язки), що записана у будь-якій формі, в тому числі дані про національність, расу, колір шкіри, релігію, вік, освіту, стан здоров'я, фінанси, особисті погляди тощо. Вказана персональна інформація не може бути використана без згоди фізичної особи та всупереч меті, для якої вона збиралась. У деяких випадках персональна інформація може бути розкрита, наприклад, за рішенням суду, для члена парламенту, який допомагає цій особі, з метою передачі в архів або збирання статистичних даних [1]. Одразу привертає увагу теза, що персональні дані – це інформація, яка записана у будь-якій формі. Слід зауважити, що таке положення законодавства є прогресивним та універсальним, оскільки на сучасному етапі розвитку суспільства, окрім первинних документів та реєстрів персональних даних, активно запроваджуються так звані «біометричні документи», які також дозволяють ідентифікувати особу.

Перші спроби закріпити на федеральному рівні правові норми про захист приватності у публічному секторі в Канаді були у 1983 р. Закон Канади «Про персональну інформацію та електронні документи» 2000 р. поширюється на організації приватного сектора, які збирають, використовують і передають персональну інформацію під час комерційної діяльності [18]. Зокрема, кожний громадянин або особа, яка постійно проживає в Канаді, може отримати доступ до інформації про себе, що міститься в установах, і виправити її, якщо вважає її невірною. Слід погодитись із А. М. Чернобай, що канадці багато уваги приділяють питанням обробки та захисту персональних даних. Громадяни Канади, у випадках виникнення

спірних ситуацій, можуть опротестувати дії влади у Комісара із захисту персональної інформації [19, 33]. Крім цього, Закон покладає на уряд відповідальність за правомірність збирання, зберігання та використання персональних даних [1]. Такий досвід є позитивним і його доцільно використовувати в Україні.

Слід відзначити, що у більшості європейських країн створюються передумови розвитку вільного обміну і гармонізації національних законодавств у сфері захисту персональних даних [20]. Так, у 1984 р. у Великобританії було прийнято Закон «Про захист даних», котрий набув чинності наприкінці 1987 р., в основу якого покладено концепцію захисту персональних даних, закріплену у Конвенції Ради Європи 1981 р. «Про захист особистості відносно автоматизованої обробки персональних даних». Законом передбачені основні принципи збирання, автоматизованої обробки, зберігання і передачі даних, регламентується порядок реєстрації персональних даних, згідно з яким тільки зареєстровані у встановленому порядку дані підлягають зберіганню, використанню та видачі. Особа, чиї дані підлягають обліку та внесені до реєстру, має право доступу до інформації про себе, право коректування або знищення даних, що її стосуються у разі неадекватності або незаконності способів отримання. При відмові у видачі інформації або внесенні до неї виправлень особа вправі звернутися із скаргою до суду [3, 30].

Основними нормативно-організаційними елементами системи захисту персональних даних у Великобританії є:

– ведення реєстру користувачів даних, баз персональних даних і осіб, які надають послуги у сфері захисту персональних даних (ч. II Закону 1984 р.);

– перевірка і контроль діяльності з персональними даними (ст.ст. 9, 16 Закону 1984 р.);

– вручення повідомлень про порушення, про скасування реєстрації, про заборону передачі даних (ст. 10 Закону 1984 р.);

– адміністративне (ст. 36 Закону 1984 р.) і судове оскарження у зв'язку із захистом даних (ст. ст. 13, 14 Закону 1984 р.) [21, 33].

Позитивним убачається ведення реєстру користувачів персональних даних, які отримали відомості про фізичну особу від володільців та розпорядників. Отже, фактично мова йде про формування переліку третіх осіб, яким було надано право доступу до персональних даних суб'єкта. Вважаємо, що створення такого реєстру володільцем та розпорядником персональних даних, дозволить упорядкувати відомості про третіх осіб, що мали доступ до бази, які потім можуть бути надані суб'єкту персональних даних для ознайомлення або Уповноваженому Верховної Ради України з прав людини (далі – Уповноваженого) – для перевірки законності надання доступу до інформації персонального характеру.

На думку О. М. Чернобай, безсумнівним лідером серед країн Європи у сфері правового регулювання та захисту персональних даних є Німеччина [19, 28]. Починаючи із середини XX ст. Німеччина почала формувати законодавство у сфері захисту персональних даних. Так, у 1970 р. прийнято перший у світі нормативний акт, який регулював питання захисту персональних даних. Цей нормативний акт був запропонований федеральною землею Гесен, а згодом його було підтримано й іншими федеральними землями [22, 52]. Уряд землі Гесен розробив законопроект «Про захист даних у галузі адміністративного управління», який передбачав два основних завдання: по-перше, попередити втручання у приватну сферу громадян Німеччини за допомогою нової інформаційної техніки, а по-друге, не допустити змін визначеного конституцією країни розподілу повноважень виконавчих органів влади перед парламентськими органами у зв'язку з виникненням «інформаційних переваг». У 1977 р. аналогічній закон було прийнято й на федеральному рівні. З тих пір громадяни Німеччини мають право самостійно приймати рішення щодо розголошення своїх персональних даних, а захист їх прав з цього питання здійснює незалежний уповноважений із захисту персональних даних, якого обирають у Ландтазі.

Відповідно до Закону Німеччини «Про захист персональних даних» 1991 р., персональні дані перебувають під захистом тільки тоді, коли вони застосовуються у приватному житті й виконують певну громадську чи економічну функцію життєдіяльності. Зовнішній контроль за забезпеченням

захисту персональних даних здійснює федеральний уповноважений із захисту персональних даних, якого обирає Бундестаг Німеччини. Він нікому не підпорядковується і є незалежним від усіх державних органів. До його компетенції належить перевірка особистих скарг громадян про незаконне використання їх особистих даних федеральними державними установами й правоохоронними органами. Таким чином, незалежність уповноважених у Німеччині – це гарантія свобод громадян і надійний захист від протиправних дій з боку держави. Останнім часом в Україні також переважна більшість повноважень щодо захисту персональних даних, делегована Уповноваженому, що відповідає європейському досвіду та створює умови забезпечення ефективності захисту відомостей про фізичну особу за допомогою парламентського контролю.

Слід погодитись з думкою В. С. Сідака, що в Німеччині захист персональних даних не лише добре врегульований на законодавчому рівні, а й реально забезпечується у практичній діяльності. Так, персональні дані про громадян дозволяється збирати і використовувати тільки в рамках чітко окреслених законом цілей [23, 8]. Багато уваги приділено в Німеччині й технічному захисту інформації. Зокрема, в інтересах інформаційної безпеки урядом Німеччини у 1993 р. створено федеральне відомство із забезпечення безпеки у сфері інформаційної техніки, до компетенції якого належить, окрім технічного захисту інформації, ще й консультації громадян з питань технічного захисту інформації, а також сертифікація та стандартизація засобів безпеки.

У жовтні 1997 р. у Німеччині був прийнятий Акт захисту інформації в телекомунікаціях (Teleservices Data Protection Act) (далі – TDPA). TDPA є частиною прийнятих положень Федерального законодавства Німеччини щодо регулювання умов інформації та комунікаційних послуг [24]. Відповідно до загальних принципів TDPA, які містяться у ст. 2 Закону «Про мультимедійні засоби інформації», збирання, оброблення та використання інформації дозволяється лише у випадках, коли це дозволено законом або здійснюється за згодою користувача. Інформація може бути лише зібрана, оброблена або використана окремо для різних послуг, яких потребує один і той самий користувач. Інформація за договором може бути зібрана, доопрацьована та використана в тому обсязі, який є необхідним для виконання договору.

Увагу привертає норма статті, яка регламентує, що за договором персональні дані можуть бути зібрані володільцем. Однак ця норма є неприпустимою, адже тільки суб'єкт персональних даних має право надати ті відомості про себе, які відповідають меті обробки. Натомість, у разі такого збирання володільцем чи розпорядником, вони мають можливість отримати набагато більший обсяг інформації персонального характеру, що суперечить законодавству. Взагалі Німеччина має досить розвинуте законодавство про захист персональних даних, яке побудовано на принципах, встановлених конвенціями та директивами Європейського Союзу, що дозволяє цій країні гармонійно існувати в рамках єдиного інформаційного простору Євросоюзу.

Викликає інтерес досвід Франції, де інститут Уповноваженого із питань захисту персональних («номінативних») даних функціонує на основі Закону «Про інформатику, картотеки та свободи» від 6 листопада 1978 р. Вказаний Закон поширюється на процеси автоматизованого збирання, обробки, зберігання і поширення персональних даних, передбачає створення Національної комісії з інформатики (Глава II Закону 1978 р.), під контроль якої підпадає близько 120 тисяч електронних баз даних. Особи, які винні у порушенні Закону про інформатику можуть бути притягнуті до адміністративної (Декрет від 23 грудня 1981 р. № 81-1142) та кримінальної (Розділ VI Закону 1978 р.) відповідальності. Головними елементами в системі захисту персональних даних у Франції є:

– видача дозволу на доступ до Національного реєстру і обробку персональних даних (ст.ст. 18, 19 Закону 1978 р.), на передачу даних за кордон (ст. 24 Закону 1978 р.);

– нагляд і контроль (перевірка заяв, скарг тощо) за дотриманням вимог із захисту даних (Розділ II Закону 1978 р.), перевірка документів (ст. 21 Закону 1978 р.);

– видання розпорядження про порушення, попередження і звернення до прокуратури, оскарження неправомірних дій у суді (ст.ст. 21, 35 Закону 1978 р.);

– ведення Національного реєстру ідентифікації фізичних осіб (Декрет від 22 січня 1981 р. № 82-103), що здійснює Національний інститут статистики і економічних досліджень. До Реєстру вносять такі відомості: прізвище, ім'я, стать, дата і місце народження, дата й місце смерті, номера свідоцтв про народження та смерть, прізвище найближчого родича по чоловічій лінії для ідентифікації однофамільців. Крім того, до Реєстру вносять номер, що надається кожній особі, позначки про зміну в цивільному стані особи, показники, що необхідні для пошуку даних.

На нашу думку, регулювання сфери захисту персональних даних, повинно відбуватися не на загальному рівні (Закон Франції «Про інформатику, картотеки та свободи»), а на рівні галузевих нормативно-правових актів у сфері захисту відомостей про фізичну особу (досвід США, Німеччини, Канади). Такий підхід надає можливість зосередити увагу на особливостях правового регулювання групи суспільних відносин у сфері обробки та захисту інформації персонального характеру.

У конституціях деяких пострадянських країн (РФ, Білорусь, Молдова та ін.) проголошується право на доступ до публічної інформації та розглядається право на доступ до інформації персонального характеру, як складова загального права на доступ до інформації. Крім того, законодавство цих країн, закріплюючи право людини на доступ до персональних даних, відокремлює його від права на недоторканість приватного життя [25]. Аналізуючи законодавство у сфері захисту персональних даних вказаних країн, необхідно наголосити, що лише в окремих з них є відповідні нормативно-правові акти, а саме: Закон РФ від 27 липня 2006 р. «Про персональні дані» [26], Закон Республіки Молдова від 08 липня 2011 р. «Про захист персональних даних» [27], Закон Республіки Азербайджан від 11 травня 2010 р. «Про персональні дані» [28], Закон Республіки Вірменії від 07 листопада 2002 р. «Про персональні дані» [29], Закон Киргизької Республіки від 14 квітня 2008 р. «Про інформацію персонального характеру» [30].

Так, у ст. 26 Закону Молдови «Про захист персональних даних» від 08 липня 2011 р. регламентовано створення та функціонування Реєстру обліку контролерів персональних даних з метою обліку обробки персональних даних та ознайомлення спільноти з переліком зареєстрованих контролерів персональних даних. Відповідно до ст. 3 Закону контролер – це фізична чи юридична особа публічного або приватного права, включаючи орган публічної влади, іншу установу чи організацію, яка самостійно або спільно з іншим суб'єктом, визначають мету та засоби обробки персональних даних [27]. Таким чином, під контролером слід розуміти володільця персональних даних, який здійснює обробку та захист відомостей про фізичну особу. Слід зазначити, що створення такого реєстру є позитивним досвідом, адже суб'єкт персональних даних має знати чи здійснює володілець обробку на законних підставах, що у подальшому впливає на гарантування цим суб'єктом захисту персональних даних фізичної особи.

Процес становлення вітчизняної системи законодавства у сфері захисту персональних даних, безперечно потребує використання зарубіжного досвіду, але, на нашу думку, таке запозичення повинно мати системний характер. Проведений аналіз дозволяє стверджувати, що використання такого досвіду вже простежується, про що свідчить делегування повноважень у сфері захисту персональних даних Уповноваженому, прийняття Закону України «Про захист персональних даних» та ратифікація Конвенції Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних». Слід погодитися з твердженням О. Г. Рогової, що процеси реформування вітчизняного законодавства та запровадження найкращих європейських принципів і цінностей в Україні активізуються. Наразі можна стверджувати, що захист персональних даних став одним із основоположних методологічних підходів створення в Україні демократичного публічного адміністрування [31, 6].

Виходячи з викладеного можна зробити такі висновки:

1. Захист персональних даних у світовій правовій традиції розуміється як одна з неодмінних підстав забезпечення фундаментального права людини на недоторканість її особистого життя, яке в свою чергу, є основоположним для сучасної демократії з дотриманням поваги до прав та гідності людини.

2. Незважаючи на те, що за останній час Україні в цілому вдалося сформувати сучасну та адекватну нормативно-правову основу для подальшого формування вітчизняної системи захисту персональних даних, наразі в Україні закладені лише основи вітчизняного законодавства у сфері захисту персональних даних, яке у цілому відповідає міжнародним стандартам. Однак потрібна подальша робота з його систематизації, розробки підзаконних актів, відповідних національних стандартів, чіткого визначення термінів, понять та категорій.

3. Досвід зарубіжних країн може бути прийнятним і корисним для України в частині заборони збирати персональні дані про дітей віком до 14 років без згоди на це їх батьків (визначити обов'язкові правила для інтернет-ресурсів, які збирають персональну інформацію про дітей та зобов'язати ці ресурси подавати відомості, для чого вони збирають інформацію і яким чином захищатимуть її); доповнення Закону України «Про захист персональних даних» положенням, що персональними даними також є біометричні документи фізичної особи.

4. Доцільним є створення користувачів персональних даних, тобто третіх осіб, яким було надано доступ до відомостей персонального характеру, та створення реєстру володільців персональних даних, котрий відображатиме відомості про таких суб'єктів і передбачатиме для них процедуру реєстрації.

Вважаємо, що у подальшому перспективним напрямом наукових досліджень є наукова розробка питань, що стосуються аналізу зарубіжного досвіду у контексті удосконалення адміністративного законодавства та адміністративної відповідальності у сфері захисту інформації персонального характеру в Україні.

СПИСОК ЛИТЕРАТУРИ

1. Михеева Н. Р. Проблема правовой защиты персональних данных [Електронний ресурс]. – Режим доступу : http://sb.biz.ua/problema-pravovoj-zashhity-personalnyx-dannyx-mixeeva/=2462.
2. Тунік А. В. Захист персональних даних: аналіз національного законодавства / А. В. Тунік // Підприємництво, господарство і право. – 2011. – № 8. – С. 97–102.
3. Різак М. В. Правове регулювання відносин обігу персональних даних : дис. … канд. юрид. наук : спец. 12.00.07 «адміністративне право і процес; фінансове право; інформаційне право» / Михайло Володимирович Різак. – Київ : Державний науково-дослідний інститут МВС України, 2012. – 214 с.
4. Василенко Д. П. Законодавство провідних країн світу в сфері захисту інформації / Д. П. Василенко, В. І. Маслак // Вісник КДУ імені Михайла Остроградського. – 2010. – № 2 (61). Ч. 1. – С. 128–132.
5. The Freedom of Information Act // [Електронний ресурс]. – 2013. – Режим доступу : http://www.justice.gov/oip/foia_updates/Vol_XVII_4/page2.htm
6. The Fair Credit Reporting Act // [Електронний ресурс]. – 2013. – Режим доступу : http://www.ftc.gov/os/statutes/031224fcra.pdf
7. The Privacy Act of 1974 // [Електронний ресурс]. – 2013. – Режим доступу : www.justice.gov/opcl/privstat.htm
8. The Right Financial Privacy Act // [Електронний ресурс]. – 2013. – Режим доступу : www.accessreports.com/statutes/RFPA.htm.
9. The Video Privacy Protection Act of 1988 // [Електронний ресурс]. – Режим доступу : http://law.cornell.edu/uscode/html/uscode18.
10. The Cable Television Consumer Protection and Competition Act of 1992 // [Електронний ресурс]. – Режим доступу : http://transition.fcc.gov/Bureaus/OSEC/ library/legislative_histories/ 1439.pdf
11. Кушакова Н. В. Конституційне право на інформацію в Україні (порівняльний аналіз) : дис. … канд. юрид. наук 12.00.02 / Наталія Вадимівна Кушакова. – К. : Київ. нац. ун-т ім. Тараса Шевченка, 2003. – 243 с.
12. Jimmy Carter Library and Museum Telecommunications Protection Policy [Електронний ресурс]. – Режим доступу : http://www.jimmycarterlibrary.gov/documents/pddirectives/pd24.pdf
13. Presidential Directives and Executive Orders. National Policyon Telecommunications and Automated Information Systems Security [Електронний ресурс]. – Режим доступу : http://www.fas.org/irp/offdocs/nsdd145.htm
14. Federal Trade Commission. Children's Online Privacy Protection Act [Електронний ресурс]. – Режим доступу : http://www.ftc.gov/ogc/coppa1.htm

15. U.S. Department of Health & Human Services. Health In surance Portability and Accountability Act of 1996 [Електронний ресурс]. – Режим доступу : https://www.cms.gov/HIPAAGenInfo/Downloads/HIPAALaw.pdf.

16. Радкевич В. П. Забезпечення охорони і захисту персональної інформації у Сполучених Штатах Америки та Великій Британії / В. П. Радкевич // Вісник Вищої ради юстиції. – 2012. – № 1(9). – С. 141–153.

17. Борисова Л. В. Захист прав суб'єктів персональних даних / Л. В. Борисова, В. В. Тулупов // Форум права. – № 1. – 2013. – С. 96–100.

18. Canadian Personal Information and Electronic Documents Act [Електронний ресурс]. – Режим доступу : http://laws.justice.gc.ca/eng/acts/P-8.6.

19. Чернобай А. М. Правові засоби захисту персональних даних працівника : дис. … канд. юрид. наук : спец. 12.00.05 / Антонина Миколаївна Чернобай. – Одеса : Нац. юридична академія, 2006. – 200 с.

20. О европейских странах, подписавших Конвенцию № 108 Совета Европы в святи с автоматизированной обработкой персональных данных [Електронний ресурс]. – Режим доступу : http://www.conventions.coe.int/Treaty/EN/searchsig.asp?NT=108&CM=1& DF=.../0.

21. Брижко В. М. Порівняльно-правове дослідження відповідності законодавства України законодавству ЄС у сфері персональних даних / В. М. Брижко, А. І. Радянська, М. Я. Швець. – К. : Тріумф, 2006. – 256 с.

22. Голубев В. О. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій : моногр. / В. О. Голубев, В. Д. Гавловський, В. С. Цимбалюк ; за заг. ред. Р. А. Калюжного. – Запоріжжя : Просвіта, 2001. – 252 с.

23. Сідак В. С. Організація системи захисту інформації в Німеччині: еволюція та сучасний стан / В. С. Сідак // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2006. – № 2(13). – С. 7–11.

24. Teleservices Data Protection Act [Електронний ресурс]. – Режим доступу : http://ourworld.compuserve.com/homepages/ckune r/multimd3.htm.

25. Конституції нових держав Європи та Азії / упор. С. Головатий. – К. : Право, 1996. – 544 с.

26. О защите данных : Закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ [Електронний ресурс]. – Режим доступу : http://www.consultant.ru/document/cons_doc_LAW_149747

27. О защите персональных даннях : Закон Республики Молдова от 08 июля 2011 г. № 133 [Електронний ресурс]. – Режим доступу : http://lex.justice.md/viewdoc.php?action=view&view=doc&id=340495&lang=2

28. О персональних даннях : Закон Азербайджанської Республики от 11 мая 2010 г. № 998-IIIQ [Електронний ресурс]. – Режим доступу : http://www.rabita.az/uploads/qanunverilcik/qanunlar_ru/opersonalnidannix.pdf.

29. О персональных даннях : Закон Республики Армения от 07 июля 2002 г. № ЗР-422 [Електронний ресурс]. – Режим доступу : http://www.parliament.am/legislation.php?sel=show&ID=1331&lang=rus

30. Об информации персонального характера : Закон Кыргызской Республики от 14 апреля 2008 г. № 58 [Електронний ресурс]. – Режим доступу : http://base.spinform.ru/show_doc.fwx?rgn=22274

31. Рогова О. Г. Захист персональних даних у законодавстві Європейського Союзу та України / О. Г. Рогова // Теорія та практика державного управління. – № 3 (34). – 2011. – С. 1–7.