УДК 342.721

О. Г. РОГОВА

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У ЗАКОНОДАВСТВІ ЄВРОПЕЙСЬКОГО СОЮЗУ ТА УКРАЇНИ

***Р**озглянуто створене в Україні та Європейському Союзі правове забезпечення захисту персональних даних. На підставі порівняльного аналізу норм європейського та вітчизняного права обґрунтовано висновок, що в Україні зроблено важливі кроки щодо захисту персональних даних.*

Ключові слова: персональні дані, публічне адміністрування, гарантії правового захисту даних.

***I**n this article existing in Ukraine and European Union legal provision of personal data protection is reviewed. Based on comparative analysis European legislation norms and Ukrainian legislation norms, we concluded that in Ukraine essential steps had been taken to protect personal data.*

Key words: personal data, public administration, effective safeguards of legal data protection.

Орієнтація України на європейські правові цінності та стандарти останніми роками стає все більш відчутною. Тому ухвалення Закону України "Про захист персональних даних" від 1 червня 2010 р. № 2297-VI [2], який було розроблено відповідно до Конвенції Ради Європи 1981 р. № 108 "Про захист осіб у зв'язку з автоматизованою обробкою персональних даних" [11], стало знаковою подією не тільки з точки зору виконання Україною зовнішньополітичних зобов'язань перед Радою Європи, а й з точки зору збагачення вітчизняного правового поля категоріями, які раніше були відсутні. Норми Закону України "Про захист персональних даних" роз'яснюють, що суб'єкт персональних даних – це фізична особа, стосовно якої відповідно до закону здійснюється обробка її персональних даних. Важливо відзначити, що вся концепція Закону України "Про захист персональних даних" базується на правовій презумпції незгоди суб'єкта персональних даних, яку викладено у п. 6 Ст. 6: "не допускається обробка даних про фізичну особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини". Відповідно до Закону України "Про захист персональних даних", згода суб'єкта персональних даних – будь-яке документоване, зокрема письмове, добровільне волевиявлення фізичної особи щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки. Персональні дані, крім знеособлених персональних даних (тобто тих, з яких вилучено відомості, що дають змогу ідентифікувати особу), за режимом доступу є інформацією з обмеженим доступом [2].

Перспектива набуття Україною членства в ЄС визначає актуальність вивчення процесів публічного адміністрування в Європейському Союзі, які тісно пов'язані з практикою захисту даних про особу від надмірного необґрунтованого втручання

органів та інституцій ЄС та інших суб'єктів інформаційних відносин. Дослідження цієї практики дедалі більше стає важливим чинником розвитку вітчизняного правового поля у сфері захисту персональних даних та відповідної право застосовної практики.

Проблематика захисту персональних даних привертає увагу багатьох дослідників, серед яких А. Гевлич, Е. Іщенко, С. Коталейчук та ін. Можна стверджувати, що список науковців, які опрацьовують різні аспекти захисту даних про особу, і надалі буде зростати, бо ухвалення Закону України "Про захист персональних даних" відкриває нову сторінку правового регулювання в цій сфері. Поки що недостатньо визначеними залишаються організаційно-правові механізми застосування положень цього Закону, ще бракує ефективних правових гарантій захисту персональних даних. Орієнтована на найкращі європейські стандарти вітчизняна практика публічного адміністрування найближчим часом має збагатитися за рахунок створення надійних та ефективно працюючих гарантій захисту даних про особу.

Метою нашого дослідження є порівняльний аналіз правового забезпечення процесів публічного адміністрування у сфері захисту персональних даних за законодавствами ЄС та України.

Рада Європи (далі – РЄ) стала першою організацією, що надала механізмам захисту персональних даних міжнародного статусу. Процеси ратифікації документів, розроблених РЄ, дозволили багатьом державам-членам підняти свої національні законодавства на більш високий рівень захисту прав і свобод людини. Законом України від 6 липня 2010 р. № 2438-VI "Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних" було ратифіковано два важливих документи РЄ у сфері захисту персональних даних [3]. У Додатковому протоколі до Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних від 8 листопада 2001 р. зазначено, що кожна Сторона передбачає один чи більше органів нагляду, відповідальних за забезпечення дотримання заходів, які передбачено її внутрішньодержавним правом і які втілюють принципи захисту персональних даних. Для цього зазначений вище орган нагляду має, зокрема, повноваження стосовно розслідування та втручання, а також право брати участь у судовому розгляді або повідомляти компетентним судовим органам про порушення положень внутрішньодержавного права [9].

Законодавство ЄС також містить чимало актів, що створюють правове підґрунтя належної адміністративної практики у сфері захисту даних про особу. Важливо відзначити, що змістовний аналіз норм права ЄС і норм права, створених РЄ, дозволяє говорити про певну спадковість і спорідненість методологічних підходів до захисту персональних даних у праві ЄС та праві РЄ. Зокрема, в Директиві 95/46/ЄС Європейського Парламенту і Ради від 24 жовтня 1995 р. "Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних" (далі – Директива 95/46/ЄС) прямо зазначається, що викладені в Директиві 95/46/ЄС принципи захисту прав і свобод фізичних осіб, а особливо права на невтручання в приватне життя, уточнюють і посилюють принципи, викладені в

Конвенції Ради Європи від 28 січня 1981 р. про захист фізичних осіб при автоматизованій обробці персональних даних [5]. Таким чином, можна стверджувати, що існує змістовний зв'язок між правовими нормами ЄС та Ради Європи у сфері захисту персональних даних.

Аналіз Директиви 95/46/ЄС свідчить, що правовий захист персональних даних у ЄС базується на таких принципах:

– персоноцентризму (системи обробки даних створені для служіння людині);

– екстериторіальності (системи обробки даних повинні незалежно від національності чи місця проживання фізичних осіб поважати їхні основні права і свободи);

– зв'язок права на захист персональних даних з правом на невтручання в особисте життя;

– рівень захисту прав і свобод фізичних осіб при обробці цих даних повинен бути однаковим у всіх державах-членах для усунення перешкод на шляху передачі персональних даних;

– принцип субсидіарності (щоб уникнути втрати фізичною особою захисту, на який вона має право згідно з даною Директивою, будь-яка обробка персональних даних у ЄС повинна відбуватися відповідно до законодавства однієї з держав-членів; повноваження контролера, створеного в державі-члені, повинні визначатися національними законодавствами (контролер виконує завдання в інтересах суспільства, може бути державним органом або іншою фізичною чи юридичною особою, що регулюється публічним правом чи приватним правом, такою як професійне об'єднання); держави-члени за власним бажанням визначають ризики для прав і свобод суб'єктів даних у своєму законодавстві;

– зближення законодавств (держав-членів та ЄС, а також ЄС та Ради Європи) про обробку персональних даних не повинне призвести до зниження рівня наданого ними захисту, а навпаки, повинне прагнути забезпечити високий рівень захисту персональних даних;

– ці принципи не поширюються на обробку даних, створених фізичною особою у процесі діяльності виняткового особистого чи домашнього характеру;

– захист даних фізичних осіб повинен застосовуватися як до автоматизованої обробки даних, так і до ручної обробки; враховуючи, що масштаби такого захисту не повинні залежати від використовуваних методів;

– різні критерії визначення складових частин структурованої сукупності персональних даних і різні критерії управління доступом до такої сукупності можуть бути встановлені кожною державою-членом;

– будь-яка обробка персональних даних повинна бути законною і справедливою по відношенню до фізичних осіб, яких вона безпосередньо стосується; особа повинна мати можливість використати право доступу до даних, які стосуються її і перебувають в обробці, з метою їхньої перевірки;

– цілі обробки даних повинні бути чіткими і законними і повинні бути визначені на час збору даних;

– обробка персональних даних повинна розглядатися також як законна, якщо вона проводиться з метою захисту інтересу, який є надзвичайно важливим для життя суб'єкта даних;

– відступ від заборони обробляти конфіденційні категорії даних може бути виправдано суспільним інтересом в таких сферах, як охорона суспільного здоров'я і соціальний захист, особливо з метою гарантування якості і рентабельності процедур, що використовуються під час врегулювання позовів про виплату допомоги і надання послуг у системі страхування здоров'я, а також у сфері наукових досліджень і урядової статистики;

– держави-члени можуть в інтересах суб'єкта даних чи з метою захисту прав і свобод інших осіб обмежити права на доступ і на інформування, (наприклад, доступ до медичних даних може бути отриманий тільки через медичного працівника);

– обмеження прав на доступ та інформування та обмеження деяких інших зобов'язань контролера можуть подібним чином бути встановлені державами-членами в тій мірі, в якій вони необхідні для захисту, наприклад, національної безпеки, оборони, суспільної безпеки чи важливих економічних і фінансових інтересів держави-члена чи Союзу, а також у карних розслідуваннях, переслідуваннях і діях у зв'язку з порушенням етики встановлених професій.

Свого часу для гармонізації європейського права у сфері захисту персональних даних було скликано незалежний консультативний орган – так звану "Робочу групу 29-й статті" – Робочу групу, створену Статтею 29 Директиви 95/46/ЄС. З розширенням ЄС у Робочої групи 29-ї статті, вочевидь, збільшилося поле діяльності, у зв'язку з необхідністю сприяння у застосуванні принципів Директиви 95/46/ЄС країнам, які щойно приєдналися [10]. Про діяльність Робочої групи 29-й статті йдеться і в Директиві 2009/136/ЄК Європейського Парламенту та Ради від 25 листопада 2009 р., яка доповнює Директиву 2002/22/ЄС про універсальні послуги та права користувачів стосовно електронних мереж зв'язку і послуг, Директиву 2002/58/ЄС про обробку персональних даних і захист таємниці сектора електронних комунікацій та Рішення (ЄС) № 2006/2004 про взаємодію національних органів відповідальних за забезпечення виконання законів про захист споживачів (далі – Директива 2009/136/ЄК) [8].

Один з найвідоміших документів європейського права – Хартія основних прав ЄС від 7 грудня 2000 р. містить Статтю 8 "Захист відомостей особистого характеру" (розміщена у Розділі "Свободи"), яка передбачає, що кожна людина має право на захист відомостей особистого характеру, що її стосуються. Ці відомості мають використовуватися відповідно до встановлених правил у визначених цілях та на підставі дозволу зацікавленої особи або на інших правомірних підставах, передбачених законом. Кожна людина має право на доступ до зібраних відомостей особистого характеру, що її стосуються, та домагатися внесення до них виправлень. Дотримання цих правил підлягає контролю з боку незалежного органу [12].

Важливим кроком на шляху інституціоналізації політики ЄС у сфері захисту персональних даних стало запровадження незалежного інституту Європейського Уповноваженого з захисту даних. Такий інститут було створено відповідно до ст. 41 Регламенту Європейського парламента і Ради № 45/2001 від 18 грудня 2000 р. про захист прав приватних осіб щодо обробки персональних даних органами та установами ЄС та про вільний рух таких даних. Функції цього інституту подібні до функцій омбудсмана, але більш вузько спеціалізовані в межах захисту персональних даних [9].

Право ЄС, спрямовуючи свій регулюючий вплив на велику кількість "політик", вже напрацювало чимало документів, що присвячені захисту даних про особу в різних сферах суспільних відносин. Так, наприклад, у Директиві 2009/136/ЄК йдеться про реорганізацію правових рамок ЄС для електронних комунікаційних мереж і послуг. А сама Директива "представляє вирішальний крок назустріч одночасному досягненню Єдиного європейського інформаційного простору та інклюзивної інформаційної спільноти". Ці цілі включені до правових рамок для розвитку інформаційної спільноти, як описано в Повідомленні Комісії Раді, Європейському Парламенту, Європейському Економіко-соціальному комітету та Комітету регіонів від 1 червня 2005 р. названого "i2010 – Європейська інформаційна спільнота для розвитку та зайнятості". Компетентні національні органи повинні відстоювати інтереси громадян, між іншим, сприяючи забезпеченню високого рівня захисту персональних даних та секретності. З цією метою, такі органи повинні мати необхідні засоби для виконання своїх обов'язків, включаючи повні та надійні дані про інциденти порушення безпеки по відношенню до персональних даних фізичних осіб. Вони мають контролювати прийняті міри та розповсюджувати найкращу практику серед провайдерів загальнодоступних електронних комунікаційних послуг. Провайдери повинні підтримувати список порушень персональних даних для подальшого аналізу та оцінки компетентними національними органами [8].

Законодавство Спільноти накладає обов'язки на контролерів даних стосовно обробки персональних даних, включаючи зобов'язання приймати відповідні технічні та організаційні дії захисту проти, наприклад, втрати даних. Вимоги щодо повідомлення про витік даних, які містяться в Директиві 2002/58/ЄС (Директива про секретність та електронні комунікації), забезпечують структуру для повідомлення компетентним органам і зацікавленим фізичним особам в разі, якщо до персональних даних було отримано несанкціонований доступ [Там же].

Висновок Європейської групи з етики в науці та нових технологіях для Європейської комісії "Етичні аспекти імплантатів в людське тіло засобів інформаційно-комунікаційних технологій", який було підготовлено в 2005 р. достатньо яскраво характеризує європейську політику у сфері застосування інформаційно-комунікаційних технологій (далі – ІКТ) як медичного, так і немедичного характеру. Зокрема, у Висновку йдеться про нову всеохопну концепцію особистості, повну повагу до тіла людини, яке в теперішній час розглядається не тільки, як фізичне, але й як електронне. У цьому новому світі захист даних виконує завдання забезпечення "habeas data" – настанови щодо розгляду законності доступу до персональних даних, які стають невід'ємним компонентом цивілізації. Європейська група з етики в науці та нових технологіях також звертає увагу на необхідність заборони використання ІКТ-імплантантів як основи для кібер-расизму та посилення можливостей домінування людини над іншими. Будь-які правила застосування ІКТ-імплантантів повинні базуватися на таких принципах: гідність, права людини, рівність, незалежність, мінімізація інформації, відповідність меті, пропорційність та доречність [13]. На нашу думку, вказані принципи мають стати основою регулювання захисту персональних даних як у сфері охорони здоров'я, так і в інших сферах, де є необхідним адекватний захист даних про людину.

Варто відзначити, що в Україні також державне управління у сфері правового забезпечення захисту персональних даних спрямовується на різні сфери суспільних

відносин. Так, було розроблено чимало правових актів (зокрема, у сфері охорони банківської таємниці, медичної таємниці тощо). Наріжним каменем всієї вітчизняної системи законодавства у сфері захисту персональних даних можна вважати Рішення Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України "Про інформацію" та статті 12 Закону України "Про прокуратуру" (справа К. Г. Устименка) 30 жовтня 1997 р. № 5-зп, де, зокрема, зазначається, що Конституція України "не допускає збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини" [6].

Приєднавшись до процесів європейської інтеграції, Україна активізувала роботу щодо створення ефективного правового забезпечення захисту персональних даних. На виконання положень Закону України "Про захист персональних даних" Указом Президента України № 1085/2010 "Про оптимізацію системи центральних органів виконавчої влади" створено Державну службу України з питань захисту персональних даних. Ст. 23 Закону України "Про захист персональних даних" визначає повноваження цього уповноваженого центрального органу виконавчої влади з питань захисту персональних даних, наголошуючи на його інспекторській і міжурядовій складових. Інспекторська складова дозволяє здійснювати контроль за додержанням вимог законодавства про захист персональних даних із забезпеченням відповідно до закону доступу до інформації, пов'язаної з обробкою таких даних, у базі персональних даних, та до приміщень, де здійснюється їх обробка [2].

Відповідно до Указу Президента України "Про Положення про Державну службу України з питань захисту персональних даних", Державна служба України з питань захисту персональних даних (далі – ДСЗПД України) є центральним органом виконавчої влади, діяльність якої спрямовується і координується Кабінетом Міністрів України через Міністра юстиції України [4].

Основними завданнями ДСЗПД України є такі: 1) внесення пропозицій щодо формування державної політики у сфері захисту персональних даних; 2) реалізація державної політики у сфері захисту персональних даних; 3) контроль за додержанням вимог законодавства про захист персональних даних; 4) здійснення міжнародно-правового співробітництва у сфері захисту персональних даних.

Законом України "Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних", набрання чинності якого має відбутися 1 січня 2012 р., Кодекс України про адміністративні правопорушення доповнено статями, що передбачають відповідальність за порушення законодавства у сфері захисту персональних даних [1].

Процеси реформування вітчизняного законодавства та запровадження найкращих європейських правових принципів і цінностей в Україні активізуються. Але вже сьогодні можна стверджувати, що захист персональних даних став одним із основоположних методологічних підходів створення в Україні демократичного публічного адміністрування. Перспективи подальших досліджень, на нашу думку, пов'язані з необхідністю вивчення в ЄС нормативних та інституційних гарантій захисту персональних даних, застосуванням відповідних гарантій у вітчизняній управлінській практиці.

Література:

1. Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних : Закон України від 2 червня 2011 р. № 3454-VI (Набрання чинності відбудеться 01.01.2012). – Режим доступу : http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=3454-17.

2. Про захист персональних даних : Закон України від 1 червня 2010 р. № 2297-VI. – Режим доступу : http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2297-17

3. Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних : Закон України від 6 липня 2010 р. № 2438-VI // ВВР України. – 2010. – № 46. – Ст. 542.

4. Про Положення про Державну службу України з питань захисту персональних даних : Указ Президента України від 6 квітня 2011 р. № 390/2011. – Режим доступу : http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=390%2F2011

5. Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних : Директива 95/46/ЄС Європейського Парламенту і Ради від 24 жовтня 1995 року. – Режим доступу : http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=994_242

6. Рішення Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України "Про інформацію" та статті 12 Закону України "Про прокуратуру" (справа К. Г. Устименка) 30 жовтня 1997 р. № 5-зп (Справа № 18/203-97). – Режим доступу : http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=v005p710-97

7. Стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі: Директива 97/66/ЄС Європейського Парламенту і Ради від 15 грудня 1997 року. – Режим доступу : http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=994_243

8. Директива 2009/136/ЄК Європейського Парламенту та Ради від 25 листопада 2009 р., яка доповнює Директиву 2002/22/ЄС про універсальні послуги та права користувачів стосовно електронних мереж зв'язку і послуг, Директиву 2002/58/ЄС про обробку персональних даних та захист таємниці сектора електронних комунікацій та Рішення (ЄС) № 2006/2004 про взаємодію національних органів відповідальних за забезпечення виконання законів про захист споживачів. – Режим доступу : www.nkrz.gov.ua/img/zstored/File/Directive_2009_136.doc

9. Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних : Протокол Ради Європи від 8 листопада 2001 р. – Режим доступу : http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=994_363

10. *Ищенко Е. А.* Защита персональных данных в праве Европейского Союза / Е. А. Ищенко // Российское право в Интернете. – 2009. – № 1. – Режим доступу : http://www.rpi.msal.ru/prints/200901ishenko.html

11. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних : Конвенція Ради Європи від 28 січня 1981 р. – Режим доступу : http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=994_326

12. Хартия основных прав Европейского Союза от 07.12.2000 // Сайт законодавства України. – Режим доступу : http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=994_524

13. Этические аспекты имплантантов в человеческое тело средств информационно-коммуникационнных технологий : Заключение Европейской группы по этике в науке и новых технологиях для Европейской комиссии 16/03/2005 (Оригинал составлен на английском языке, источник: http://europa.eu.int/comm/european_group_ethics/clocs/avis2Den.pdf). – Режим доступа : posoh.ru/tend/intern_org/doc/zakl.doc

Надійшла до редколегії 01.07.2011 р.