ISSN 1995-6134

УДК 004.056(075.8)
А.О. ПОПОВ, Кримський юридичний інститут Одеського державного університету внутрішніх справ

ЗАРУБІЖНИЙ ДОСВІД ПРАВОВОГО РЕГУЛЮВАННЯ ЗАХИСТУ ВІДОМЧИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Ключові слова: *національні електронні реєстри, персоніфікована інформація, інформаційне самовизначення, захист власності персональних даних*

Однією з головних загроз конституційним правам українських громадян, суспільству та державі в інформаційній сфері є протиправне розповсюдження конфіденційних баз даних, що належать державним органам. Попит на них визначається гострою конкурентною боротьбою національних суб'єктів господарювання, підвищеною зацікавленістю до особистого життя окремих категорій громадян, і як свідчать наявні матеріали, постійно зростає. Основними споживачами вказаної інформації є недержавні служби безпеки, консалтингові структури, організовані злочинні угруповання. Особливою популярністю користуються бази даних податкових органів, Державної митної служби, ДАІ МВС України. Зокрема, лише протягом поточного року органами СБУ припинено 26 спроб незаконного збуту баз даних державних установ і організацій, що містять конфіденційну інформацію, яка є власністю держави.

Дослідженню окремих проблем правового регулювання інформаційної безпеки при розробці, створенні та застосуванні відомчих інформаційних ресурсів, зокрема при формуванні електронних реєстрів за функціональним призначенням, приділялася увага в роботах таких видатних фахівців, як А.В. Пазюк, Raab Ch.D., Bennett C.J., Grant R. С.П. Rotenberg M. та інших [1-3].

Комплексні дослідження проблем і перспектив становлення ефективного механізму заходів інформаційної безпеки при застосуванні відомчих інформаційних масивів та національних електронних реєстрів до нашого часу не проводились. Поряд із зазначеним необхідність подальшого наукового дослідження проблем та перспектив застосування системи інформаційної безпеки при використанні національних електронних реєстрів, які формуються та постійно циркулюють у складі національних інформаційнихресурсів обґрунтовує також стрімкий розвиток інформаційно-телекомунікаційних систем і технологій, а також широке впровадження електронних реєстрів у діяльності міністерств, установ, закладів та організацій.

Це свідчить про те, що дослідження проблем і перспектив розробки системи заходів інформаційної безпеки при використанні національних електронних реєстрів у напрямку нормативно-правового регулювання питань захисту інформаційних ресурсів, має відповідну наукову новизну. Метою роботи є аналіз міжнародного досвіду правових питань застосування системи заходів інформаційної безпеки у складі баз даних національних електронних реєстрів, а також розробка пропозицій щодо розбудови національної системи інформаційної безпеки державних електронних реєстрів.

Національні правові традиції, а також особливості способів правового регулювання зумовили формування різних моделей захисту власності персоніфікованої інформації в національних правових системах різних країн. Найбільш поширеною у світі є модель базового регулювання, згідно з якою в країні приймається один чи декілька основних нормативних актів, що створюють відповідний правовий механізм захисту власності персональних даних. Ключовим елементом регуляторної моделі країн Західної та Центральної Європи, Австралії, Нової Зеландії, Гонконгу та Канади є наглядовий орган із захисту даних. На нього покладається низка повноважень щодо виконання наглядової, охо-

ISSN 1995-6134

ронної та регулятивної функцій у цій галузі.

Наглядова інстанція з питань захисту власності персональних даних наявна у національних правових системах більшості розвинутих країн світу. Для дослідження компетенції і повноважень наглядового органу доцільно розглянути процес його становлення та розвитку в деяких європейських країнах. Наглядовий орган з'явився разом із появою перших правил поводження з персональними даними. Його повноваження зазнавали змін, відображаючи еволюцію законодавчого регулювання цього питання.

Перші закони, серед яких закон ФРН та Швеції, були спрямовані на адміністрування баз даних у деяких публічних секторах, і здебільшого регулювали лише організаційні та технічні питання. Суб'єкту даних надається лише право доступу і виправлення даних, якщо вони були неточними. Роль наглядового органу зводилася до реєстрації баз даних і загального нагляду за дотриманням правил і процедур обробки даних органами державної влади і публічними організаціями [1].

Ґрунтовні дослідження розвитку законодавчого регулювання обробки персоніфікованої інформації в європейських країнах відстежують тенденцію поширення технократичного підходу в першому поколінні нормативних актів, яка проявляється і в термінології, що в них використовується. Зокрема, в них відсутні такі терміни, як «власність», «інформація» чи «захист приватного життя»; натомість застосовуються технічні терміни – «дані», «банк даних», «файл даних» тощо. Подальший розвиток зазначених положень законодавства європейських країн знаменується доповненням прав суб'єкта даних правом на «інформаційне самовизначення». Під цим розуміється право людини контролювати поводження з персональними даними на всіх стадіях обробки, починаючи від збору, та закінчуючи їх знищенням.

Ця доктрина вперше була сформульована у 1983 році Федеративним Конституційним судом ФРН, який зазначив, що свобода особи планувати та здійснювати свої вчинки значною мірою обмежується, якщо вона не має достатньої впевненості у тому, яку персоніфіковану інформацію мають у своєму розпорядженні її співбесідники. А тому для захисту прав осіб необхідно їй надати повноваження визначати, яким чином персональні дані розкриваються і використовуються.

Доктрина права на інформаційне самовизначення була впроваджена у Федеративному законі ФРН про захист даних (1990 р.) та Законі Фінляндії про реєстрацію громадян (1987 р.) [4-5]. На цьому етапі повноваження наглядового органу зазнають суттєвих змін. Зокрема, на нього покладається охоронна функція, яка реалізується ним через повноваження звертатися до судових органів для захисту порушених прав людини стосовно її персональних даних. Він стає більш схожим на традиційного уповноваженого з прав людини. Не випадково, що найбільш поширеними назвами цієї інституції стають «Уповноважений з питань захисту власності» чи «Уповноважений із захисту даних».

З огляду на те, що права особи стосовно поводження з її даними не є абсолютними чи виключними та що існують інші інтереси, які мають бути враховані в інтересах суспільства, перед Уповноваженим постає складне завдання балансування між інтересами суб'єкта даних і публічними інтересами. Необхідність встановлення справедливого балансу між такими конкуруючими правами, як право на власність і право на свободу інформації, є, зокрема, однією з причин, яка зумовила покладання на Уповноваженого із захисту даних Канади і Угорщини функції нагляду за дотриманням права на вільний доступ до інформації, що становить публічний інтерес.

Принцип балансування між інтересами особи та публічними інтересами є одним із ключових у діяльності наглядового органу. Складність вирішення цього питання у комплексі та динаміці обставин була сформульована Реєстратором із захисту даних Великої Британії, який відзначив, що точка балансу є різною для різних індивідів, чиї за-

ISSN 1995-6134

конні інтереси зважуються у конкретних обставинах. Так, згідно з концепцією «ручного управління», подальший розвиток інституту наглядової інстанції має відбуватися у напрямку надання йому більших повноважень для ручного управління балансом між інтересами особи і публічними інтересами відповідно до обставин конкретної справи [2].

Серед чинників, які мають бути враховані під час встановлення такого балансу, сучасне покоління нормативних актів із захисту власності персональних даних визнає потенційну шкоду для суб'єкта даних від обробки певної категорії «вразливих» даних. Згідно з Декретом про вразливі дані 1993 року, в Нідерландах встановлено детальні вимоги стосовно правил поводження з кожним окремим видом «вразливих» даних, які стосуються релігійних чи філософських переконань (ст.2), расового походження (ст.3), політичних поглядів (ст.4), інтимних аспектів приватного життя і стану здоров'я (ст.5), кримінальних вчинків (ст.6), адміністративних порушень (ст.7) тощо.

Для врахування особливостей секторів, у яких запроваджується регулювання операцій з даними, наглядовий орган деяких країн наділяється регулятивною функцією. На нього покладаються повноваження щодо затвердження відповідних кодексів «чесної інформаційної практики», сертифікації запропонованих ними правил на їх відповідність до вимог національного законодавства про захист власності персональних даних. Зокрема, Комісія із захисту даних Нідерландів може декларувати, що правила, які містяться у такому кодексі, належним чином впроваджують правові положення щодо обробки персональних даних.

Уповноважений Гонконгу, наприклад, відповідно до положень Закону Гонконгу «Про захист даних» 1995 року, ухвалив два Кодекси: «Про практику стосовно номерів посвідчення особи» (1997 р.) і «Про дані стосовно кредитоспроможності споживачів» (1998 р.).

Крім того, більшість національних положень надають наглядовому органу право у той чи інший спосіб впливати на процес підготовки регулятивних актів шляхом подання пропозиції або зауважень стосовно проектів нормативних актів.

Важливість існування дієвого наглядового органу в механізмі захисту власності персоніфікованої інформації зумовила вироблення відповідних пропозицій щодо доповнення Конвенції Ради Європи про захист осіб стосовно автоматизованої обробки персональних даних 1981 року положеннями про таку інституцію. На 16-й нараді Консультативного Комітету Конвенції, що відбувалася з 6 по 8 липня 2000 року у Страсбурзі, був ухвалений проект додаткового протоколу до Конвенції. Протокол містить положення, що вимагають від держав-учасниць Конвенції впровадження наглядового органу з питань захисту власності персональних даних і надання йому необхідних повноважень для виконання наглядової й охоронної функцій. Зокрема, друга частина статті 1 проекту додаткового протоколу встановлює, що вказаний орган повинен мати, крім інших, повноваження щодо розслідування і втручання, а також повноваження вступати у юридичний процес або подавати на розгляд судовій владі порушення положень національного законодавства [6].

У деяких європейських країнах створено спеціальну інстанцію для розгляду такої категорії справ. За Законом Швейцарії 1992 року на Федерального Уповноваженого із захисту даних покладаються функції ведення реєстру баз даних, нагляду за дотриманням правил поводження з даними, захисту прав суб'єктів даних. У разі встановлення порушень він ухвалює відповідні рекомендації. Однак у разі їх невиконання Уповноважений може звернутися до Федеральної Комісії з захисту персональних даних, яка виносить рішення, що має силу судового. Крім того, Федеральна Комісія розглядає апеляції на рішення органів влади федерації і кантонів у галузі захисту власності персональних даних.

Уповноважений із захисту даних Фінлян-

ISSN 1995-6134

дії за законом 1987 року здійснює контроль за дотриманням правил поводження з персональними даними і розслідування за заявами осіб. А колегія із захисту даних Фінляндії вирішує суперечки і має право визначати, коли персональні дані можуть передаватися за кордон країни.

Наглядовий орган з питань захисту власності персональних даних для ефективного виконання своїх функцій має діяти цілком незалежно. Цей принцип закріплений у більшості європейських законів із захисту персональних даних. Він проголошується і в проекті додаткового протоколу до Конвенції Ради Європи про захист осіб стосовно автоматизованої обробки персональних даних. Так само визнаним є й принцип підконтрольності наглядового органу судовій владі. Зокрема, частина четверта вказаного протоколу передбачає, що рішення наглядового органу, які призвели до подання скарг, можуть бути оскаржені до суду.

Для сучасного стану моделі базового (статутного) регулювання принциповим є поширення як правил правового захисту власності персоніфікованої інформації, так і наглядових повноважень не тільки на публічні, але й рівною мірою на приватноправові відносини. Це є яскравим прикладом нормативного відтворення поширеної в Європі доктрини горизонтальної дії конституційних норм з прав людини у відносинах між приватними особами.

Інший підхід до законодавчого регулювання питань поводження з даними був обраний Сполученими Штатами Америки, які уникали ухвалення загального закону із захисту даних, поширюючи відповідні правила лише на певні сектори. Так званий, ліберальний підхід, оснований на концепції невтручання держави у відносини між приватними особами, обумовлює особливості національного режиму захисту власності персональних даних у приватному секторі США та інших країн. Як відмічає американський правозахисник, професор Марк Ротенберг, Закони США з захисту даних, як правило виникали як реакція на питання, що залишалися неврегульованими судовими прецедентами чи як спроба кодифікувати правові стандарти для їх застосування під час комерційних операцій з використанням нових технологій [3].

До першої категорії можна віднести такі закони: «Про право на фінансову власність» (1978 р.), «Про захист власності» (захист від неправомірного збору інформації під час обшуку і виїмки) 1980 р. та «Про власність електронних комунікацій» (1986 р.). Ці закони були прийнятті внаслідок того, що Верховний Суд Сполучених Штатів у своїй практиці не визнав відповідні права на власність.

До другої категорії відносяться такі закони: «Про власність» (право на доступ до персональних даних у публічних реєстрах) 1974 р., «Про захист власності під час відео-зйомки» (захист від стеження) 1988 р., «Про захист споживачів телефонних послуг» 1991 р. Перелічені закони з'явилися з упровадженням нових технологій, які викликали відповідну зацікавленість громадськості у захисті власності.

Забезпечення додержання правил поводження з даними за цією моделлю покладається на низку органів, серед яких суди, прокуратура, Федеральна торгова комісія, Департамент транспорту та інші органи, які здійснюють загальний нагляд за виконанням умов ліцензій на певні види діяльності тощо.

За цим підходом виникає проблема у разі появи нової технології, яка вимагає окремого законодавчого регулювання питань захисту власності. Наприклад, у США відсутній закон про захист власності генетичних даних. Унаслідок такої правової прогалини на цю категорію персональних медичних даних не поширюється режим власності.

Крім того, галузева юрисдикція наглядових органів у США дозволяє порушникам права на власність в певних випадках уникати відповідальності. Так, юрисдикція Федеральної торгової комісії в цьому питанні поширюється на нечесну чи обманну діяльність або практику лише тоді, коли вони здійснюються на комерційній основі або впливають на комерцію. З іншого боку, якщо особи чи

ISSN 1995-6134

організації неправомірно збирають інформацію без комерційної мети, це виходить за межі юрисдикції Федеральної торгової комісії.

До того ж, нечесною визнається практика, яка може заподіяти чи заподіяла значну шкоду споживачам, якщо її не можна уникнути і вона не переважується користю від цього для споживачів або конкуренції (§ 45, Секція 5 Закону США «Про Федеральну торгову комісію»). Однак поширеною, зокрема, серед постачальників інформаційного продукту, є практика надання споживачам безоплатного товару в обмін на повідомлення персональних даних. В таких випадках, за законодавством США, відповідальність настає лише у разі обману покупців, які надали інформацію про себе, а взамін нічого не отримали.

За європейською моделлю, галузевий підхід не замінює, а доповнює базове законодавство з захисту даних. Крім того, з метою сприяння правильному застосуванню загальних положень, враховуючи галузеві особливості, європейські стандарти передбачають можливість створення професійними організаціями чи іншими представницькими органами кодексів поведінки стосовно поводження з персональними даними.

Теоретично механізм саморегуляції може забезпечити прийнятний рівень захисту власності персональних даних. За цією моделлю, споживачеві певної послуги дається право вибирати серед постачальників, зважаючи на запропонований ними рівень захисту власності. За ідеальних умов рівності всіх учасників ринку певної послуги конкурентні переваги буде мати той постачальник, який пропонує найбільш оптимальний для споживачів рівень захисту. А отже, це повинно спонукати постачальників приєднуватися до галузевих кодексів «чесної інформаційної практики».

Передача персоніфікованої інформації від споживача до постачальника послуг, який знаходиться в іншій країні, несе ризик втрати контролю за операціями з персональними даними, оскільки фактично дуже складно проконтролювати додержання постачальником правил, встановлених у контракті або у внутрішніх правилах захисту власності, які демонструє постачальник споживачам через свою веб-сторінку. В електронному середовищі доволі поширеними стали схеми сертифікації дотримання компаніями проголошеної корпоративної політики щодо поводження з персональними даними у формі маркування чи поставлення сертифікаційних печаток, ярликів на веб-сторінках постачальників, які мають посвідчувати факт дотримання ними зобов'язань про захист власності.

Слід відзначити такі системи посвідчення власності, які покликані запропонувати нові можливості для посилення захисту власності в електронному середовищі: «Електронна печатка кращої ділової практики щодо власності», «Електронна Довіра» і «Японська Система маркування захисту власності». Відповідні позначення сертифікації даються за результатами проведення аудиту додержання запропонованих стандартів захисту власності в електронному середовищі. Така сертифікація є одним із способів саморегуляції приватного сектора шляхом встановлення галузевих стандартів і забезпечення їх додержання за допомогою як фінансових санкцій, так і позбавлення статусу сертифікованого постачальника зняттям позначки про сертифікацію з його веб-сторінки.

Модель саморегуляції, однак, не може розглядатися як альтернативна до законодавчого регулювання. Низький рівень захисту і неможливість забезпечення проголошених професійних стандартів є слабкими місцями цієї регулятивної моделі.

У документі, який був підготовлений Робочою Групою статті 29 Директиви ЄС 95/46 ЕС за назвою «Судячи індустріальну саморегуляцію», експерти ЄС дійшли висновку, що інструмент саморегуляції може розглядатися як дієва складова «адекватного захисту» за умов, що він буде:

- обов'язковим до виконання для всіх членів, яким дані передаються, і забезпечувати адекватні гарантії у разі передачі даних не

ISSN 1995-6134

членам;

- прозорим і містити основний зміст принципів захисту даних;

- мати механізм для забезпечення достатнього рівня його додержання в цілому через систему превентивних санкцій і покарання, а також обов'язків безсторонній аудит;

- надавати підтримку і допомогу суб'єктам даних, які зіткнулися з проблемами;

- мати легкодоступний, неупереджений і незалежний орган для розгляду заяв суб'єктів даних і прийняття рішень у разі порушень кодексу;

- гарантувати у випадках його порушення відповідну компенсацію для суб'єкта даних [7].

Зрозуміло, що забезпечити виконання цих вимог лише інструментами саморегуляції проблематично. Разом із тим, у поєднані з механізмом державного регулювання така модель має право на існування.

Слід відзначити, що європейські стандарти захисту власності, які базуються на соціально-захисному підході, одержують все більше визнання у світі, що можна спостерігати на прикладі таких традиційно ліберально-ринкових країн як Канада і Австралія.

Аналізуючи чинне федеральне законодавство Канади про захист власності у публічному секторі, яке діє з 1983 року, слід виділити Закон Канади «Про персональну інформацію і електронні документи» (2000 р.), вимоги якого поширюються на організації приватного сектора, які збирають, використовують і поширюють персональну інформацію під час комерційної діяльності. Закон було введено в дію у три етапи:

1) з 01.01.2001 року – до будь-якої організації, яка здійснює діяльність за федеральним законодавством у секторах авіаперевезень, банківської справи, телебачення, радіомовлення, між-провінційних перевезень і телекомунікації, а також до будь-яких організацій, які передають дані за межі провінції чи Канади;

2) з 01.01.2002 року – до медичної персоніфікованої інформації, яка обробляється задіяними на першому етапі організаціями;

3) з 01.01.2004 року – до всіх організацій, які збирають, використовують і поширюють персональну інформацію під час комерційної діяльності на території провінції, незалежно від того, поширюється на таку організацію федеральний статус чи ні.

Однак, на думку експертів Робочої Групи Європейського Союзу, законодавство Канади все ж таки ще не надає адекватного рівня захисту, оскільки має прогалини. Зокрема, воно не поширюється на неприбуткові організації, не передбачає спеціальних гарантій щодо обробки вразливих даних і передачі даних до третіх країн.

Австралія ухвалила федеральний закон про захист власності у 1998 році. Закон встановлює детальні «Принципи Інформаційної Власності», які ґрунтуються на Керівних принципах ОЕСР 1980 року. Крім того, Закон впроваджує так звані «Національні Принципи Власності», які базуються на принципах, розроблених Федеральним Комісаром з власності у 1998 році і узгоджених з позицією представників приватного сектора економіки Австралії. Подібно до канадського, законодавство Австралії не містить заборону на обробку вразливих даних, не передбачає правил щодо обробки даних у цілях «прямого продажу» товарів і послуг, що відзначається у висновку Робочої Групи ЄС.

Отже, можна стверджувати, що переважає тенденція поширення європейського, соціально-захисного підходу регулювання обробки персоніфікованої інформації до країн, які є традиційно ліберальними у їх ставленні до відносин між публічним і приватним секторами. Це ще раз доводить необхідність вибору саме європейської моделі захисту права на власність для упровадження в України.

ЛІТЕРАТУРА

1. Пазюк А. В. Міжнародно-правовий захист права людини на приватність персоніфікованої інформації: дис. … кандидата юрид. наук : 12.00.11 / Пазюк Андрій Валерійович ; Нац. ун-т імені Тараса Шевченка. –

ISSN 1995-6134

Київ, 2004. – 205 с.

2. Raab Ch. D. From Balancing to Steering: New Directions for Data Protection / Raab Ch. D., Bennett C. J., Grant R. // Visions of Privacy: Policy Choices for the Digital Age. – University of Toronto Press, 1999. – P. 73.

3. Rotenberg M. Preface to first edition / Rotenberg M. // The Privacy Law Sourcebook 2001. — Washington: EPIC, 2001. – P. 66.

4. German Federal Data Protection Act. - 1990.

5. Henkilorekisterialaki (Finish Persons Register Act). – 1987. – 471. – НЕ. – 49/86.

6. Конвенція Ради Європи № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; Amendment to Convention ETS No.108 allowing the European Communities to accede). – Страсбург, 28.01.1981 р. Серія «Європейські угоди», № 108 [Електронний ресурс]. – Режим доступу: http://www.convention.coe.int/treaty/en/Treaties/Html/108.htm. [Офіційний переклад засвідчено МЗС України від 01.07.2002 р.].

7. Підсумкові документи Всесвітнього саміту з питань інформаційного суспільства / Міністерство транспорту та зв'язку України, Державний Департамент з питань зв'язку та інформатизації. – К., 2006. – 77 с.

Попов А. О. Зарубіжний досвід правового регулювання захисту відомчих інформаційних ресурсів / А. О. Попов // Форум права. – 2009. – № 3. – С. 513–519 [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/e-journals/FP/2009-3/09paovir.pdf

Проведено аналіз правового регулювання інформаційної безпеки при застосування електронних баз персональних даних в провідних країнах Європи, Азії, Америки та Австралії. Визначені потенційні загрози інформаційній безпеці через можливість широкого несанкціонованого доступу до електронних баз даних, що містяться у складі електронних національних реєстрів держав. Запропоновано необхідність вибору європейської моделі правового захисту інформаційних ресурсів у складі державних електронних реєстрів України.

***

Попов А.О. Зарубежный опыт правового регулирования защиты ведомственных информационных ресурсов

Проведен анализ правовой регуляции информационной безопасности при применении электронных баз персональных данных в ведущих странах Европы, Азии, Америки и Австралии. Определены потенциальные угрозы информационной безопасности через возможность широкого несанкционированного доступа к электронным базам данных, которые содержатся в составе электронных национальных реестров государств. Предложена необходимость выбора европейской модели правовой защиты информационных ресурсов в составе государственных электронных реестров Украины.

***

Popov A.O. Foreign Experience of the Legal Adjusting of Defense of Department Informative Resources

The analysis of the legal adjusting of informative safety is conducted at application of electronic bases of the personal information in the leading countries of Europe, Asia, America and Australia. Potential threats informative safety is certain through possibility of wide unauthorized division to the electronic databases, which are contained in composition the electronic national registers of the states. The necessity of choice of the European model of legal defense of informative resources is offered in composition the state electronic registers of Ukraine.