

2. Закон України “Про інформацію” від 02.10.1992 р. № 2657–ХІІ.
3. Закон України “Про Національну програму інформатизації” від 04.02.1998 р. № 74/98–ВР.
4. “Україна: поступ у ХХІ століття. Стратегія економічної та соціальної політики на 2000 – 2004 рр.”. Послання Президента України до Верховної Ради України / Урядовий кур’єр, 2000. – № 16.
5. Указ Президента України від 24 вересня 2001 року № 891/2001 “Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних”.
6. Указ Президента України від 31 липня 2000 року № 928/2000 “Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні”.
7. Конвенція № 108 Ради Європи “Про захист осіб у зв’язку з автоматизованою обробкою персональних даних”. – Страсбург, 28.01.1981 р. Серія “Європейські угоди”, № 108 // www.convention.coe.int/treaty/en/Treaties/Html/108.htm.

УДК 342.721:681.302

М. ШВЕЦЬ, доктор економічних наук, професор,
заслужений діяч науки і техніки України,
лауреат Премії імені Ярослава Мудрого

В. БРИЖКО, заслужений винахідник республіки,
лауреат Премії імені Ярослава Мудрого

ДО ПИТАННЯ ОГЛЯДУ ІНФОРМАЦІЙНОГО ЗАКОНОДАВСТВА ЩОДО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В КРАЇНАХ ЄВРОПИ

У європейських країнах діяльність щодо захисту персональних даних ґрунтується на принципах Конвенції “Про захист прав і основних свобод людини” від 04.11.1950 р. [1], Конвенції № 108 Ради Європи “Про захист осіб у зв’язку з автоматизованою обробкою персональних даних” від 28.01.1981 р. [2], Директиви 95/46/ЄС Європейського Парламенту і Ради Європейського Союзу від 24.10.1995 р. “Про захист осіб у зв’язку з обробкою персональних даних і вільним обігом цих даних” [4] та Директиви 97/66/ЄС Європейського Парламенту та Ради Європейського Союзу “Про обробку персональних даних і захист прав осіб у телекомунікаційному секторі” від 15.12.1997 р. [5].

Відповідно до статті 13 Конвенції № 108 Ради Європи “Про захист осіб у зв’язку з автоматизованою обробкою персональних даних” від 28.01.1981 р. для забезпечення захисту персональних даних “кожна Сторона (держава – член Конвенції № 108 Ради Європи) призначає один чи більше органів”. Призначений орган є наглядовою інстанцією за діяльністю у сфері захисту персональних даних, забезпечує організацію законодавчої і адміністративної роботи на національному рівні і складає основу інституту Уповноваженого з питань захисту персональних даних в країні. Розглянемо стан законодавства в окремих країнах Європи.

Німеччина. Інститут Уповноваженого з питань захисту персональних даних почав формуватися в 1970 році, коли в Землі Гессен вперше у світі був прийнятий цільовий Закон “Про захист даних” [6].

Закон установив державну посаду Комісара по захисту даних на правах єдиноначальності. Цьому виборному державному службовцю закон надав і забезпечив право повної незалежності від владних структур (жоден орган виконавчої влади не може давати йому вказівки), а також надав право спостереження за діяльністю щодо персональних даних. Як наглядова, незалежна інстанція Комісар не несе прямої відповідальності за обробку персональних даних.

У 1983 році Конституційний Суд визначив, що всі громадяни мають право на інформаційне самовизначення – можливість людини визначати і контролювати використання її персональних даних. У більшості країн із законами про “privacy” існує норма про особистий контроль, як одну з цілей регулювання, але в цих державах відсутні явні конституційні гарантії, як у Німеччині.

Сьогодні захист персональних даних у країні визначається положеннями Федерального Закону “Про подальший розвиток обробки і захисту даних” від 20.12.1990 р. [7].

Згідно з параграфом 22 Закону 1990 р. за поданням Федерального уряду Бундестаг строк на п'ять років обирає Федерального уповноваженого по захисту даних, який призначається на посаду Президентом. За організаційне забезпечення Федерального уповноваженого відповідає Міністр внутрішніх справ, який здійснює посадовий нагляд за його діяльністю.

Положення про інститут Федерального уповноваженого (параграф 38 Закону 1990 р.) підтвердили його правовий статус і конкретизували права щодо порядку виборності, контрольних функцій, можливостей оскарження незаконних дій з персональними даними та ін.

Основними організаційно-правовими елементами системи захисту персональних даних в Німеччині є:

- * ведення реєстру файлів (параграф 26 Закону 1990 р.) і баз (параграф 32 Закону 1990 р.) персональних даних щодо державних і недержавних структур;

- * ведення переліку пристроїв і нагляд за застосуванням програм обробки персональних даних (параграф 18 Закону 1990 р.);

- * здійснення контролю (перевірки) діяльності з персональними даними у різних організаціях (параграфи 24, 38 Закону 1990 р.), оскарження порушень щодо положень Закону, заява протесту на незаконні дії (параграфи 25, 38 Закону 1990 р.).

Згідно з параграфом 36 Закону 1990 р. організації (більше п'яти чоловік), що обробляють персональні дані, повинні призначати уповноваженого організації по захисту персональних даних.

Положення параграфа 42 Закону 1990 р. встановлюють вимоги щодо призначення уповноважених по захисту даних у федеральних радіомовних організаціях, які діють від імені Федерального уповноваженого країни.

Великобританія. Інститут Уповноваженого з питань захисту персональних даних у Великобританії функціонує на основі Закону “Про захист даних” від 12.07.1984 р. [8].

Даний Закон визначив посади Міністра по захисту даних, Реєстратора по захисту даних і утворив Суд по захисту даних. Таким чином була окреслена сфера захисту персональних даних.

Міністр вправі змінити чи доповнити положення Закону з метою надання додаткових гарантій по захисту персональних даних. Проект розпорядження, правила чи наказу повинен бути схвалений постановою кожної палати Парламенту.

Реєстратор призначається грамотою Її Величності королеви й має наступні обов'язки:

- * ведення реєстру осіб, що збирають і зберігають персональні дані, а також осіб, що мають комп'ютерні бюро і надають послуги щодо персональних даних;

- * вручення повідомлень про порушення Закону 1984 р., про скасування реєстрації або про заборону передачі даних;

- * розгляд скарг про порушення Закону 1984 р.

Будь-яка особа вправі звернутися з апеляцією до Суду по захисту даних у разі відмови Реєстратора розглянути скаргу про порушення Закону 1984 р.

Основними організаційно-правовими елементами системи захисту персональних даних у Великобританії є:

- * ведення реєстру користувачів даних, баз персональних даних і осіб, що надають послуги у сфері захисту персональних даних (частина II Закону 1984 р.);

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

- * вручення повідомлення 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.).

Франція. Інститут Уповноваженого з питань захисту персональних (“номінативних”) даних у Франції функціонує на основі Закону “Про інформатику, картотеки та свободи” від 06.01.1978 р. [9]. Він поширюється на процеси автоматизованого збирання, обробки, зберігання і поширення персональних даних.

Закон передбачає створення Національної комісії з інформатики (Глава II Закону 1978 р.), під контроль якої підпадає понад 120 тисяч електронних баз даних.

Комісія є незалежним (з регламентованими повноваженнями) адміністративним органом, витрати на утримання якої включають до бюджету Міністерства юстиції Франції. Деякі витрати можуть бути основою для стягнення плати за надання послуг (ст. 7 Закону 1978 р.).

Комісія складається з 17 чоловік: двох депутатів і двох сенаторів, яких обирає Парламент; двох членів Економічної та двох членів Соціальної рад, яких обирають на їх зборах; двох членів Рахункової палати; двох членів Касаційного суду; двох фахівців з інформатики, призначених декретом за поданням голів Національних зборів і Сенату; трьох фахівців, призначених Радою міністрів. Учасник Комісії виконує покладені на нього функції протягом п'яти років (ст. 8 Закону 1978 р.).

Комісія зобов'язана:

- * інформувати громадськість про вплив інформатики на приватне життя, забезпечення прав людини та основних свобод й функціонування демократичних інститутів;

- * вносити до Уряду пропозиції щодо захисту персональних даних за умов розвитку інформатики;

- * у передбачених Законом випадках приймати регламентні акти (постанови) і видавати правила про захист персональних даних;

- * приймати заяви та скарги;

- * попереджати порушників та сповіщати органи прокуратури про порушення Закону;

- * консультувати приватних і юридичних осіб, органи державної влади та судові органи.

Комісія може вимагати від голів апеляційних і адміністративних судів відрядження в її розпорядження відповідних осіб для проведення під її керівництвом нагляду чи перевірки. Особи, що викликані в Комісію для роз'яснень чи дачі свідчень, звільняються від дотримання таємниці. Міністри, посадові особи, керівники публічних і приватних організацій (підприємств) повинні всіляко сприяти роботі Комісії.

Рішенням Прем'єр-міністра при Комісії призначається урядовий Комісар по захисту персональних даних. Він бере участь у засіданнях Комісії і може в десятиденний термін призначити повторне слухання з будь-якого питання, що раніше було винесено на розгляд Комісії. Комісар очолює Французьке агентство з питань захисту персональних даних.

Основними організаційно-правовими елементами системи захисту персональних даних у Франції є:

- * ведення Національного реєстра ідентифікації фізичних осіб (Декрет від 22.01.1981 р. № 82–103). Ведення Реєстру здійснює Національний інститут статистики і економічних досліджень. До Реєстру вносять наступні відомості: прізвище, ім'я; стать; дата і місце народження; дата і місце смерті; номери свідоцтв про народження і смерть; прізвище найближчого родича по чоловічій лінії для ідентифікації однофамільців. Крім того, до Реєстру вносять номер, що присвоюється кожній особі, позначки про зміну в цивільному стані особи, що реєструють, показники, необхідні для пошуку даних;

- * 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 реклаमाцій, заяв, скарг) за дотриманням вимог по 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.).

Особи, винні у порушенні Закону “Про інформатику”, можуть бути притягнуті до адміністративної (Декрет від 23.12.1981 р. № 81–1142) та кримінальної (Розділ VI Закону 1978 р.) відповідальності.

Угорщина. Інститут Уповноваженого з питань захисту персональних даних в Угорщині функціонує на підставі Закону “Про захист інформації про особу і доступ до інформації, що становить суспільний інтерес” від 10.11.1992 р. [10].

Закон визначив виборну посаду Парламентського Комісара по захисту інформації (Омбудсмен – від шведського “ombud” – представник інших осіб), що діє згідно з положеннями Закону “Про Парламентського Комісара по правах громадян”.

Омбудсмен зобов'язаний:

- * контролювати виконання положень Закону 1992 р.;
- * розглядати скарги з питань захисту інформації про особу;
- * забезпечувати ведення реєстру по захисту інформації.

Основними організаційно-правовими елементами системи захисту персональних даних в Угорщині є:

- * нагляд за дотриманням вимог щодо захисту інформації (ст. 25 Закону 1992 р.), перевірка документів і внесення протесту (ст. 26 Закону 1992 р.);
- * звернення особи до Омбудсмена в разі порушення її прав (ст. 27 Закону 1992 р.);
- * ведення реєстру захисту інформації і осіб, які надають послуги у сфері захисту персональних даних (ст.ст. 28 та 29 Закону 1992 р.).

Реєстрація не потрібна по відношенню до обробки інформації, що:

- * включає відомості про особу, яка перебуває в ділових відносинах з розпорядником інформації;
- * регулюється правилами церков, конфесій чи релігійних громад;
- * стосується стану здоров'я особи, одержання медичної допомоги, виплат щодо соціального страхування;
- * включає відомості у зв'язку з наданням фінансової чи іншої соціальної допомоги;
- * стосується ведення справ адміністративними органами, прокуратурою і судами;
- * підпадає під чинність Закону “Про пресу”;
- * передається розпорядником до архіву;
- * використовується виключно для потреби однієї особи (ст. 30 Закону 1992 р.);
- * включає відомості у зв'язку зі статистичним обліком чи науковими дослідженнями (за умов знеособлювання персональних даних).

Інформація, яка обробляється та зберігається з метою виконання наукових досліджень, не може використовуватися з іншою метою (ст. 32 Закону 1992 р.).

Підсумовуючи зазначене, слід сказати, що за останні 20 років більшість західноєвропейських країн приєдналися до Конвенції № 108 Ради Європи, прийняли національні базові закони та сформуливали правові механізми щодо сфери захисту персональних даних [11] (див. Таблицю).

Таблиця

Європейські країни, які підписали Конвенцію № 108 Ради Європи та прийняли національні закони про захист персональних даних

Країна	Дата підпису Конвенції № 108 РЄ	Назва базового закону	Дата прийняття закону	Реєстрація баз персональних даних	Реєстрація ручної обробки даних	Ліцензування діяльності щодо даних
Австрія	28.01.81 р.	Про захист даних	01.01.80 р. з додатком 2000 р.	усі дані	так	деякі дані
Бельгія	07.05.82 р.	Про захист даних	08.12.92 р.	усі дані	так	деякі дані
Болгарія	02.06.98 р.	+				
Великобританія	14.05.81 р.	Про захист даних	12.07.84 р.	усі дані	так	деякі дані
Греція	17.02.83 р.	Про захист осіб стосовно обробки даних	09.11.87 р. з додатком 1997 р.	усі дані	так	деякі дані
Данія	28.01.81 р.	Про реєстри даних	08.06.82 р.	деякі дані	так	деякі дані

		Про захист даних	2000 р.			
Ірландія	18.12.86 р.	Про захист даних	13.07.88 р.	деякі дані	ні	ні
Ісландія	27.09.82 р.	Про захист пер- сональних даних	05.06.81 р. з додатком 2000 р.	усі дані	так	усі дані
Іспанія	28.01.82 р.	Про регулювання автоматизованої обробки персо- нальних даних	29.10.92 р.	усі дані	ні	деякі дані
Італія	02.02.83 р.	Про захист осіб у зв'язку з автома- тизованою оброб- кою персональних даних	01.02.92 р.	деякі дані	так	деякі дані
Латвія	31.10.00 р.	Про захист пер- сональних даних	2001 р.			
Люксембург	28.01.81 р.	Про використан- ня персональних даних, які оброб- ляються у комп'ютері	31.03.79 р.	усі дані	ні	ні
Молдова	04.05.98 р.	+				
Нідерланди	21.01.88 р.	Про захист даних	28.12.88 р. з додатком 2000 р.	деякі дані	так	ні
Німеччина	28.01.81 р.	Про подальший розвиток обробки даних	20.12.90 р. з додатком 1997 р.	усі дані	так	деякі дані
Норвегія	13.03.81 р.	Про реєстраторів персональних да- них	09.06.82 р.	деякі дані	так	деякі дані
Польща	21.04.99 р.	+				
Португалія	14.05.81 р.	Про захист персо- нальних даних	29.04.91 р.	усі дані	ні	усі дані
Росія	07.11.00 р.	проект	внесення 24.10.00 р.	усі дані	так	усі дані
Румунія	18.03.97 р.	+				
Словаччина	14.04.00 р.	+				
Словенія	23.11.93 р.	+				
Туреччина	28.01.81 р.	+				
Угорщина	13.05.93 р.	Про захист даних та доступ до ін- формації, яка має суспільний інтерес	11.92 р.	усі дані	так	деякі дані
Фінляндія	10.04.91 р.	Про файли персо- нальних даних	04.02.87 р. з додатком 1999 р.	деякі дані	так	деякі дані
Франція	28.01.81 р.	Про інформатику, картотеки та сво- боди	06.01.78 р.	деякі дані	так	деякі дані

Швеція	28.01.81 р.	Про захист даних	13.05.73 р. з додатком 1988 та 1999 рр.	деякі дані	ні	деякі дані
Швейцарія	02.10.97 р.	Про захист даних	19.06.92 р.	деякі дані	так	ні
Естонія	24.01.00 р.	Про особисті документи	2002 р.			

Примітка: + – базовий закон про захист персональних даних, що відповідає положенням європейських стандартів, прийнятий. Інших відомостей не визначено.

Росія. Правова основа роботи з персональними даними визначена Конституцією Російської Федерації (ст.ст. 22, 23 і ст. 29 п.4) та Законом РФ “Про інформацію, інформатизацію і захист інформації” від 20.02.1995 р. [12]. На органи державної влади покладено обов'язок забезпечити кожній особі можливість ознайомлення з документами, що їй безпосередньо стосуються, якщо інше не передбачене законом.

Питання обробки персональних даних знайшли відображення в Основах законодавства РФ “Про Архівний фонд Російської Федерації і архіви” (ст. 20), у Федеральному Законі “Про оперативно-розшукову діяльність” (ст.ст. 3, 5, 9, 10, 12, 21), Законах РФ “Про державну таємницю” (ст. 5), “Про засоби масової інформації” (ст.ст. 41, 43, 46, 51, 57), “Про федеральні органи податкової поліції” (ст. 10), “Про податкові органи Російської Федерації” (ст.ст. 7, 11), “Про міліцію”, у законодавстві про вибори.

У Цивільному кодексі РФ стаття 152 захищає честь, гідність і ділову репутацію громадянина. У Кримінальному кодексі РФ у статті 137 встановлено кримінальну відповідальність “за незаконне збирання чи поширення відомостей про приватне життя особи, що складають його особисту чи сімейну таємницю”. Але стосовно всіх випадків порушення конфіденційності персональних даних (у тому числі засобами масової інформації) цього явно недостатньо. В країні об'єктивно склалася потреба приведення правової основи сфери захисту персональних даних до положень європейських стандартів.

Спочатку в Росії був розроблений законопроект “Про захист персональних даних”. Проте у Думу був внесений і прийнятий до розгляду протоколом від 24.10.2000 р. № 49 засідання Комітету з питань інформаційної політики законопроект “Про інформацію персонального характеру” [13]. Відмінності між ними полягають у тім, що перший проект розроблений на базі принципів і підходів Конвенції № 108 Ради Європи (пріоритет прав людини), а другий – Директиви 95/46/ЄС Європейського Парламенту і Ради Європейського Союзу [4] (пріоритет економічних питань).

Координацію робіт у сфері захисту персональних даних законопроект доручає вести Уповноваженому органу з питань захисту персональних даних. Виконання відповідних завдань і функцій передбачено покласти Урядом РФ на один з діючих органів державної влади.

Уповноважений орган зобов'язаний вести реєстр баз персональних даних щодо органів державної влади і органів місцевого самоврядування. Він повинен виключити невиправдане дублювання при комплектуванні цих даних, а також здійснювати ліцензування роботи (діяльності) з персональними даними, сертифікацію інформаційних технологій і систем, що використовують для обробки персональних даних.

Порядок реєстрації баз персональних даних визначається Урядом РФ (ст. 19 проекту Закону 2000 р.).

Основними організаційно-правовими елементами системи захисту даних в Росії є:

- * облік, реєстрація і ведення реєстру масивів персональних даних: архіви, картотеки, електронні бази даних тощо (ст.ст. 19, 20, 21, 28 проекту Закону 2000 р.);
- * ведення реєстру населення Росії (ст. 20 проекту Закону 2000 р.);
- * ведення реєстру первинного обліку фізичних осіб і розпорядників персональних даних (ст.ст. 21, 31 проекту Закону 2000 р.);
- * ліцензування робіт з персональними даними (ст. 28 проекту Закону 2000 р.);

* сертифікація інформаційних технологій і інформаційних систем, призначених для обробки персональних даних (ст. 28 проекту Закону 2000 р.);

* контроль за використанням персональних даних, що отримані органами державної влади і органами місцевого самоврядування від інших державних розпорядників персональних даних (ст. 21 проекту Закону 2000 р.);

* розгляд скарг, заяв, пропозицій щодо захисту персональних даних (ст.ст. 13, 14 проекту Закону 2000 р.).

Розгляд конфліктних ситуацій передбачається проводити Уповноваженим органом з питань захисту персональних даних, а також в адміністративному чи судовому порядку (ст. 20 проекту Закону 2000 р.).

Модельний закон про захист персональних даних для країн СНД. На чотирнадцятому пленарному засіданні Міжпарламентської Асамблеї держав – членів Співдружності Незалежних Держав був прийнятий Модельний закон про персональні дані (постанова від 16.10.1999 р. N 14–19) [14].

До основних форм державної регуляції віднесено: ліцензування діяльності з персональними даними, реєстрацію баз персональних даних, реєстрацію розпорядників персональних даних і сертифікацію інформаційних систем, призначених для обробки персональних даних (ст. 5 проекту Закону 1999 р.).

Ліцензування діяльності (робіт) з персональними даними (ст. 6 проекту Закону 1999 р.) забезпечує державний контроль за діяльністю в цій сфері. Ліцензія на діяльність з персональними даними видається органами виконавчої влади, на які покладені функції захисту прав у сфері захисту персональних даних.

У ліцензії вказують:

* мету і способи одержання та використання персональних даних, режими і терміни їхнього зберігання;

* категорії чи групи суб'єктів персональних даних;

* перелік персональних даних;

* джерела персональних даних;

* порядок повідомлення суб'єктів про одержання їх персональних даних;

* заходи щодо забезпечення недоторканності персональних даних і конфіденційності поводження з ними;

* перелік осіб, відповідальних за роботу з персональними даними;

* наявність сертифікатів на інформаційні системи, що призначені для обробки персональних даних та засобів їхнього захисту.

Інформаційні продукти, що містять персональні дані, повинні мати посилання на видану ліцензію.

Ліцензування не передбачене:

* для органів виконавчої влади, що здійснюють роботу з персональними даними відповідно до їхньої компетенції;

* у разі роботи з персональними даними з метою, що не передбачає передачу персональних даних іншим юридичним і фізичним особам;

* у разі використання цих даних в особистих цілях, що не передбачає їх поширення.

Реєстрація баз персональних даних (ст. 7 проекту Закону 1999 р.) забезпечує їх облік і дозволяє інформувати громадян про можливості доступу до своїх персональних даних.

Бази персональних даних підлягають обов'язковій реєстрації в органах виконавчої влади, на які покладені функції захисту персональних даних.

При реєстрації баз персональних даних фіксуються:

* найменування баз персональних даних;

* мета одержання і використання персональних даних;

* перелік персональних даних, що збираються;

* категорії чи групи суб'єктів персональних даних;

* терміни зберігання персональних даних.

Реєстрація розпорядників персональних даних (ст. 8 проекту Закону 1999 р.) забезпечує ведення загальнодоступного Реєстру розпорядників персональних даних, до якого вносяться наступні відомості:

- * мета, способи одержання і використання персональних даних, режим і терміни їхнього зберігання;
- * категорії чи групи суб'єктів персональних даних;
- * джерела персональних даних;
- * порядок повідомлення суб'єктів про внесення їх персональних даних до баз персональних даних;
- * заходи щодо забезпечення зберігання персональних даних і конфіденційності дій з ними;
- * особи, які безпосередньо відповідальні за роботу з персональними даними;
- * наявність сертифікатів на інформаційні системи, що призначені для обробки та засобів захисту персональних даних.

Сертифікація автоматизованих інформаційних систем (ст. 9 проекту Закону 1999 р.), призначених для обробки персональних даних, здійснюється з метою забезпечення необхідного рівня захисту персональних даних.

Сертифікацію здійснюють органи з питань сертифікації згідно з національним законодавством.

Уповноважений орган може мати наступні права (ст. 16 проекту Закону 1999 р.):

- * безперешкодний доступ до масивів (баз) персональних даних;
- * право на запит і одержання від розпорядника персональних даних будь-яких необхідних документів і матеріалів у зв'язку із захистом персональних даних;
- * проведення самостійно чи разом з уповноваженими органами і посадовими особами перевірок діяльності розпорядників персональних даних, щодо яких є відомості про порушення захисту персональних даних;
- * внесення вимоги про відкликання ліцензії щодо діяльності з персональними даними.

Висновки

1). У сфері захисту персональних даних у різних країнах спостерігаються наступні загальні тенденції:

- * створюється інфраструктура для вирішення проблем правового та організаційного захисту персональних даних;
- * формується спеціальна сфера правового регулювання;
- * організуються спеціальні державні інститути уповноважених для забезпечення нагляду і контролю за дотриманням прав у сфері захисту персональних даних.

У європейських країнах закони про захист персональних даних охоплюють як суспільний, так і приватний сектор, створені інститути незалежних контролерів (комісар, омбудсмен, уповноважений) по захисту персональних даних та уповноважених органів. В американській моделі захист персональних даних охоплює суспільний сектор, носить мозаїчний зміст норм права в різних законах (банківська, кредитна діяльність, охорона здоров'я) і у судових рішеннях. У зв'язку із формуванням юридичної архітектури е-середовища розглядаються питання створення базового, федерального законопроекту щодо захисту персональних даних.

2). Спеціалізовані закони про захист персональних даних з'явилися у світі відносно недавно. Одним з перших можна вважати Закон німецької Землі Гессен (1970 р.). Пізніше за прикладом Німеччини пішли Швеція (1973 р.), Франція, Австрія (1978 р.) й інші західноєвропейські країни. У подальшому вони спиралися на положення міжнародних стандартів, основні з яких сформовані у Конвенції № 108 Ради Європи від 28.01.1981 р. і Директиві 95/46/ЄС від 24.10.1995 р.

3). В усіх державах – членах Конвенції № 108 Ради Європи на національному рівні організаційно-правове забезпечення захисту персональних даних здійснює Уповноважений з питань захисту персональних даних та спеціальний орган нагляду. Уповноважений з питань захисту персональних даних у виконанні обов'язків є незалежним, підпорядкований закону, підзвітний парламенту, в організаційних питаннях може бути підконтрольний уряду. У Німеччині, напри-

клад, Уповноважений має подвійне підпорядкування – Бундестагу і Міністру внутрішніх справ, якому він дає клятву щодо сумлінного виконання обов'язків. Згідно з параграфом 36 Федерального Закону “Про подальший розвиток обробки даних та захисту даних” від 20.12.1990 р. в організаціях і підприємствах усіх форм власності забезпечення захисту персональних даних здійснює відповідний уповноважений організації (фірми).

Основними вимогами до Уповноваженого органу з питань захисту персональних даних є: компетентність, що передбачає виконання їм арбітражної функції, важливої у зв'язку з тривалістю судових процедур і швидкою зміною інформаційно-комп'ютерних технологій; незалежність від інших гілок державної влади.

У ряді країн створюються колегіальні органи нагляду за діяльністю Уповноваженого органу, що мають назву – комісія, колегія чи рада по захисту персональних даних.

4). За останні 20 років більшість західноєвропейських країн прийняли національні базові закони, сформувавши правові механізми захисту персональних даних та приєдналися до Конвенції № 108 Ради Європи.

Незважаючи на розходження правових систем, в основу законів західноєвропейських країн про захист персональних даних покладені однакові принципи, і ці основоположні принципи залишаються незмінними дотепер, навіть якщо саме законодавство в деяких країнах (у Німеччині, наприклад) оновилося. Зазначене навряд чи можна пояснити запозиченням досвіду – хоча б тому, що деякі закони були прийняті майже одночасно. Всі вони мають однакову структуру, однакову мету і відрізняються лише в деталях. Захист персональних даних передбачає обов'язкову реєстрацію баз даних і ліцензування діяльності щодо персональних даних відповідними уповноваженими органами. Відмовлення від реєстрації чи ліцензування розглядається як порушення національного законодавства.

Зазначене пояснюється тим, що проблеми захисту персональних даних в індустріальних країнах мають однакове походження і потребують однакового вирішення. Таке рішення в демократичному суспільстві покликано підтримувати оптимальний баланс прав людини, суспільства і держави як агента суспільства. Засобом установа балансу прав і інтересів є правовий режим захисту персональних даних, заснований на визначених принципах, єдиних для всіх демократичних держав незалежно від особливостей їх правових систем. У 1981 році вказані принципи були сформульовані на міжнародному рівні в Конвенції № 108 Ради Європи, головному на сьогодні міжнародно-правовому акті щодо захисту персональних даних. У подальшому положення Конвенції отримали розвиток у Директиві 95/46/ЄС від 24.10.1995 р. та у Директиві 97/66/ЄС від 15.12.1997 р. Це дає підставу говорити про наявність у сучасному світі загальновищаних стандартів щодо захисту персональних даних.

5). Законодавство про захист персональних даних практично в жодній країні не досягло своєї зрілості, навіть на термінологічному рівні. Повна адекватність національних законодавств про захист персональних даних ще не досягнута. На це є об'єктивні й суб'єктивні причини.

Основною дилемою організаційно-правового регулювання у сфері захисту персональних даних є протиріччя між прагненням максимального використання персональних даних у державних та корпоративних інтересах й, одночасно, бажання максимально захистити права на недоторканність приватного життя людини. Ідея захисту персональних даних виходить з необхідності захисту індивідуума і гарантій верховенства його інтересів над “суспільними інтересами”. Зазначені інтереси можуть виконувати волю одного керівника із силою і невідворотністю на товпу. Проте будь-яке насильство повинне застосовуватися процедурно.

Щодо бажань максимальної деталізації у забезпеченні захисту персональних даних, то є сенс мати на увазі, що, по-перше, ідеальну модель захисту створити можна, але реалізувати її практично неможливо; абсолютного захисту не існує, життя не в змозі перемогти смерть. Подруге, зайва деталізація правового регулювання у цій сфері може знижувати попит на розробку нових інформаційно-комп'ютерних технологій. Це обумовлена мотивація для “бізнес-софт-індустрії”, яка буде пропонувати менше технологій, здатних забезпечити сильний захист.

Використана література

1. Конвенція Ради Європи “Про захист прав і основних свобод людини ” (Рим, 04.11.1950 р.) та Протокол № 11 // Голос України. – 2001. – № 3 (2503). – С. 6–8.
2. Конвенція № 108 Ради Європи “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 // www.convention.coe.int/treaty/en/Treaties/Html/108.htm. Офіційний переклад здійснено у ДКЗІ України, засвідчено МЗС України від 01.07.2002 р.
3. Додатковий протокол до Конвенції № 108 Ради Європи “Про захист осіб у зв’язку з автоматизованою обробкою персональних даних” щодо уповноважених органів нагляду та міждержавних інформаційних потоків. Страсбург, від 08.11.2001 р. // www.conventions.coe.int/treaty/en/Treaties/Html/181.htm. Офіційний переклад здійснено у ДКЗІ України, засвідчено МЗС України від 01.07.2002 р.
4. Директива 95/46/ЄС Європейського Парламенту та Ради Європейського Союзу “Про захист осіб у зв’язку з обробкою персональних даних і вільним обігом цих даних” від 24.10.1995 р. // www.evropa.eu.int/ISPO/legal/en/dataprot/directiv/directiv.html.
5. Директива 97/66/ЄС Європейського Парламенту та Ради Європейського Союзу “Про обробку персональних даних і захист прав осіб у телекомунікаційному секторі” від 15.12.1997 р. // www.evropa.eu.int/ISPO/legal/en/dataprot/protection.html.
6. Закон Землі Гессен (ФРГ) “О защите данных”, 1970.
7. Федеральный Закон ФРГ “О дальнейшем развитии обработки данных и защиты данных” от 20.12.1990 г.
8. Закон Великобритани “О защите данных” от 12.07.1984 г.
9. Закон Франции № 78–17 от 06.01.1978 г. “Об информатике, картотеках и свободах” (Journal officiel de la Republique Fracaise, 7 janvier 1978, 25 janvier 1978).
10. Закон № LXIII Венгрии “О защите персональных данных и доступе к информации, представляющей общественный интерес”, 1992.
11. Европейские страны, подписавшие Конвенцию № 108 Совета Европы. По состоянию на 06.02.2002 г. // www.conventions.coe.int/Treaty/EN/searchsig.asp?NT=108&CM=1&DF=../0.
12. Федеральный Закон РФ “Об информации, информатизации и защите информации” от 20.02.1995 г. № 24–ФЗ. Собрание законодательства Российской Федерации, 1995. – № 8.
13. Проект Федерального Закона РФ “Об информации персонального характера”. Внесен в Государственную Думу от 05.10.2000 г. // www.duma.gov.ru/kmpage/50200023/input3/24.htm.
14. Модельный закон “О персональных данных”. Принят на четырнадцатом пленарном заседании Межпарламентской Ассамблеи государств–участников СНГ (постановление от 16.10.1999 г. N 14–19) // www.contel.ru/rus/organizers/law3.html).



УДК 342.9(075.8)

В. ЦИМБАЛЮК, кандидат юридичних наук,
лауреат Премії імені Ярослава Мудрого

АДМІНІСТРАТИВНО-ПРАВОВІ ДЖЕРЕЛА МЕТОДОЛОГІЇ ІНФОРМАЦІЙНОГО ПРАВА (синергетичний та кібернетичний аспекти)

Рубіж ХХ – ХХІ століть для України знаменувався входженням до інформаційного суспільства – суспільства, в якому діяльність людей ґрунтується на використанні послуг, що надаються за допомогою інформаційних технологій та технологій зв’язку [9, – С. 81]. З огляду на це, виникла необхідність наукового забезпечення правового регулювання суспільних відносин щодо інформації, яка нині у всьому світі усвідомлена як важливий ресурс суспільних відносин разом з такими різновидами майна, як речі та енергія.

У контексті постановки проблеми в загальному вигляді та її зв’язку із важливими науковими та практичними завданнями, зокрема публічного правотворення у сфері державного управління суспільними відносинами щодо інформації, існує необхідність формування методології такого нового соціального феномена, як інформаційне право.

Легально у нашій країні інформаційне право як напрям наукового дослідження було