

УДК 339.1:342.721:681.302

**БРИЖКО В.М.**, кандидат юридичних наук (*Doctor of Philosophy*), с.н.с.,  
Заслужений винахідник республіки,  
співавтор Законів України “Про захист персональних даних”  
від 13 травня 2006 р. № 2618 та від 1 червня 2010 р. № 2297-VI.

## ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ: РЕАЛІЇ ТА ПРАКТИКА СУЧАСНОСТІ<sup>1</sup>

*Анотація.* Про історію, хронологію розробки та узгодження, а також про питання до застосування Закону України “Про захист персональних даних”. Пропозиції щодо створення національної цілісної системи захисту персональних даних.

*Ключові слова:* інформаційне право, персональні дані, захист персональних даних.

*Аннотация.* Об истории, хронологии разработки и согласования, а также о вопросах применения Закона Украины “О защите персональных данных”. Предложения по созданию национальной целостной системы защиты персональных данных.

*Ключевые слова:* информационное право, персональные данные, защита персональных данных.

*Summary.* About history and chronology of development and mutual approval, as well as about the questions of application of Law of Ukraine “About the personal data protection”. Suggestions on creation of the national integral system of personal data protection.

*Keywords:* information law, personal data, personal data protection.

**Вступ.** Нормативне вирішення проблеми захисту прав людини починає свою історію у 1215 році, коли англійський король Іоанн Безземельний під тиском баронів підписав Велику хартію вільностей (“Magna Carta”) [1, с. 13-19]. Значення Хартії полягає у тому, що вона була першим прецедентом обмеження деспотичної влади монарха, щоправда лише відносно феодалів і рицарства; про права простих людей мови не було.

Через 50 років Генріх III, після чергової доповіді міністрів про безладу на вулицях Лондона, промовив: “Ну-ка, давайте сюда главных крикунов. Пусть дерутся они сами, у меня на глазах, а не стравливают толпы”. У результаті монарх був вимушений присягнути першому парламенту (від фр. – “базікати”, “говорити”), хоча діяльність останнього довгий час мало сприяла забезпеченню прав людини. Про продуктивність та робочу атмосферу англійського парламенту тих часів красномовно свідчить виказана депутатом Ісаком Ньютоном лише єдина за п’ять років фраза: “Закройте окно, дует”. Потрібно було ще декілька століть, щоб від декларативних тверджень перейти до конкретних нормативних актів, що регламентують недоторканність особи.

В цьому аспекті історія ХХ сторіччя характерна активнішим просуванням по шляху досягнення індивідуальних свобод. Зараз немає такої демократичної конституції в світі, яка б не мала в своєму законодавстві природних, невід’ємних прав на особисту свободу людини.

Важливим при цьому є те, що особиста свобода невід’ємна від безпеки. І справа по обмеженню свободи є справою зміцнення безпеки людини, суспільства та держави. Захист, хочемо ми цього чи ні, це обмеження, встановлені законом. Обмеження з боку правової держави мають сенс лише тоді, коли цими обмеженнями переслідуються мета поставити перешкоди на шляху довільного поведіння з правами людини.

© Брижко В.М., 2013

<sup>1</sup> До матеріалів виступу на “круглому столі” на тему: “Особливості захисту персональних даних у сучасному кіберпросторі: правові та техніко-технологічні аспекти” (Київ, 10 жовтня 2013 р.). – Національний інститут стратегічних досліджень.

Міжнародне визнання права на захист приватної сфери особистого і сімейного життя, що передбачає захист особистих відомостей про людину, вперше увійшло до переліку фундаментальних прав і свобод у Загальній декларації прав людини, прийнятій Генеральною Асамблеєю ООН 10 грудня 1948 року. Стаття 12 Декларації проголосила: *“Ніхто не може зазнавати безпідставного втручання у його особисте життя, безпідставного посягання на недоторканність його житла, тайну його кореспонденції або на його честь і репутацію. Кожна людина має право на захист законом від такого втручання або таких посягань”* [1, с. 22-25].

У 1970-х відбувся початок активного застосування інформаційно-комп’ютерних технологій, телекомунікаційних мереж та формування різних за напрямками електронних накопичувачів інформації – баз даних. Це поступово трансформувало європейське розуміння поняття “право на недоторканність особистого та сімейного життя” у бік застосування заходів “захисту права на інформаційний суверенітет особи”, зокрема, права людини визначати ким, коли, з якою метою та яким чином інформація про неї буде використовуватися іншими особами. Ця трансформація визначила зародження так званого “Інформаційного суспільства”, а у класичному праві – появу нової юридичної галузі під назвою “Інформаційне право”<sup>2</sup>. При цьому, забезпечення прав людини, зокрема у телекомунікації, отримало визначення у вигляді терміну “захист персональних даних”. Причини зазначеного полягають в тому, що з початку застосування новітніх технологій та мереж розпорошені по різних відомчих “відсіках” та у багатьох випадках анонімні інформаційні сліди життя людини стали отримувати електронну персоналізацію. Комп’ютери, програми, телекомунікації, бази даних перетворили тривалий і трудомісткий процес пошуку відомостей у високотехнологічну індустрію збирання особистої інформації з різних джерел, її обробки та поширення у визначених цілях – політичних, економічних, фінансових, кримінальних тощо. Інформація про особу, її здібності, наміри та вчинки, особисте чи сімейне життя, зміст розмов та стосунків, майновий стан, медичні відомості, особисте теле- чи відеоменю, результати вибору книг у бібліотеці, газет чи журналів, зміст файлів на комп’ютерах та на автовідповідачах, відомості щодо спілкування за допомогою засобів нового електронного середовища (е-середовища) – всі ці та багато інших даних за бажанням можна поєднати, проаналізувати та інтерпретувати (створити навіть бажаний “негативний портрет” особи) так, що людина, модель її поведінки виглядатиме “прозорою” в усіх своїх якостях та проявах.

У зв’язку з вищезазначеним у європейських країнах почали приймати закони про захист персональних даних (див. Таблицю 1). Головна їх мета бачилася у вирішенні проблеми забезпечення приватного життя людини згідно з принципами Європейської конвенції “Про захист прав людини та основоположних свобод” (Рим, 04.XI.1950 р.) [1, с. 34-44]. Відповідно до статті 8 Європейської конвенції від 1950 р.: *“Кожен має право на повагу до його приватного і сімейного життя, до житла і до таємниці кореспонденції. Органи державної влади не можуть втручатися у здійснення цього права інакше ніж згідно із законом і коли це необхідно в демократичному суспільстві в інтересах національної і громадської безпеки або економічного добробуту країни, з метою запобігання заворушенням чи злочинам, для захисту здоров’я чи моралі або з метою захисту прав і свобод інших осіб”*.

<sup>2</sup> У 1994 році група фахівців під керівництвом Мартіна Бангемана – Комісара Ради Європи із захисту персональних даних (на той час), здійснила аналіз розвитку ринкових відносин. Звіт групи є, так мовити, маніфестом побудови Інформаційного суспільства і мав назву: *“Європа і глобальне Інформаційне суспільство. Рекомендації Європейській Раді”* [2, с. 189-192].

Наприкінці 1970-х років суперечність між все більш активним впровадженням засобів автоматизованої обробки даних та їх поширенням у телекомунікаційних мережах, зловживання при використанні персональних даних, потреба у впорядкуванні експортно-імпортних операцій призвели до необхідності розробки міжнародно-правового акту, який мав забезпечити уніфіковане впорядкування інформаційних відносин у сфері захисту персональних даних. Комітетом Ради Європи з питань захисту даних були сформульовані принципи захисту від неправомірного збирання, обробки, зберігання та поширення персональних даних. Ці основоположні принципи 28 січня 1981 року отримали закріплення у першій міжнародній угоді світового рівня – Конвенції Ради Європи “Про захист осіб у зв’язку з автоматизованою обробкою персональних даних” (відома як Конвенція РЄ № 108, згідно з порядком у серії Європейських договорів)<sup>3</sup>.

З того часу захист персональних даних остаточно виокремився у самостійний вид діяльності та сферу нормативно-правового упорядкування інформаційних відносин.

Таблиця 1

Країна	Дата підписання Конвенції РЄ № 108	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. дод. 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 у зв’язку з обробкою даних	09.11.87 р. дод. 1997 р.	усі дані	так	деякі дані
Данія	28.01.81 р.	Про захист даних Про реєстри даних	08.06.82 р. 2000 р.	деякі дані	так	деякі дані
Ірландія	18.12.86 р.	Про захист даних	13.07.88 р.	деякі дані	ні	ні
Ісландія	27.09.82 р.	Про захист персональних даних	05.06.81 р. дод. 2000 р.	усі дані	так	усі дані
Іспанія	28.01.82 р.	Про регулювання автоматизованої обробки персональних даних	29.10.92 р.	усі дані	ні	деякі дані
Італія	02.02.83 р.	Про захист осіб у зв’язку з обробкою персональних даних	01.02.92 р.	деякі дані	так	деякі дані
Латвія	31.10.00 р.	Про охорону даних фізичних осіб	2000 р.			

<sup>3</sup> Матеріали Конвенції РЄ № 108 та Додаткового до неї протоколу див. у розділі журналу “Європейські правові стандарти”. Переклад з англ. укр. мовою здійснений авторами Закону України “Про захист персональних даних”, і офіційно засвідчений МЗС України від 01.07.02 р.

Литва	+	Про правовий захист особистих даних	11.06.96 р.			
Люксембург	28.01.81 р.	Про використання персональних даних, які обробляються у комп'ютері	31.03.79 р.	усі дані	ні	ні
Молдова	04.05.98 р.	+	2000 р.			
Нідерланди	21.01.88 р.	Про захист даних	28.12.88 р. дод. 2000 р.	деякі дані	так	ні
Німеччина	28.01.81 р.	Про подальший розвиток обробки даних	20.12.90 р. дод. 1997 р.	усі дані	так	деякі дані
Норвегія	13.03.81 р.	Про реєстраторів персональних даних	09.06.82 р.	деякі дані	так	деякі дані
Польща	21.04.99 р.	+	+			
Португалія	14.05.81 р.	Про захист персональних даних	29.04.91 р.	усі дані	ні	усі дані
Росія	+	Про персональні дані	27.06.07 р.	усі дані	так	
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 інформації, яка має суспільний інтерес	11.1992 р.	усі дані	так	деякі дані
Фінляндія	10.04.91 р.	Про файли персональних даних	04.02.87 р., дод. 1999 р.	деякі дані	так	деякі дані
Франція	28.01.81 р.	Про інформатику, картотеки та свободи	06.01.78 р.	деякі дані	так	деякі дані
Швеція	28.01.81 р.	Про захист даних	13.05.73 р. дод. 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.

Згідно з Конвенцією РЄ № 108 держави, які підписали цей документ, зобов'язуються керуватися її положеннями стосовно персональних даних, що підлягають чи не підлягають автоматизованій обробці, як у суспільному, так і приватному секторах.

Кожна держава-член Ради Європи коригує національне законодавство у частині втілення її основних принципів та поставленої мети – забезпечення на її території поваги до прав та свобод кожної людини незалежно від її громадянства або місця проживання.

Конвенція РЄ № 108 допускає обмеження у правах фізичних осіб, якщо це стосується державної чи громадської безпеки, фінансових інтересів, боротьби зі злочинністю, захисту прав та основоположних свобод інших людей.

Згідно з Конвенцією РЄ № 108 кожна держава-член зобов'язана призначити Уповноважений орган нагляду та направити відповідне повідомлення Генеральному секретарю Ради Європи. Завдання Уповноваженого передбачають створення належного організаційно-правового упорядкування відносин для захисту персональних даних у країні.

Десятиріччя, що минули з часу прийняття Конвенції РЄ № 108, показали, що інститут Уповноваженого з питань захисту персональних даних не лише зберігся, а й дістав поширення у всіх західноєвропейських країнах. Нині уповноважені органи з питань захисту персональних даних діють більше ніж у двадцяти країнах Європи. Їх діяльність свідчить, що вони є ефективним засобом, здатним забезпечити баланс інтересів людини, суспільства і держави. У Німеччині, наприклад, за участі цього інституту вдалося оформити право на захист персональних даних як основне право фізичних осіб і розглядати його як конституційну норму.

В інтересах подальшої деталізації та уніфікації національних законодавств Консультативний комітет Ради Європи у питаннях захисту персональних даних заохочує секторний (галузевий) підхід, наполегливо дотримується та намагається розвивати загальні правила щодо окремих аспектів їх обробки, продовжує удосконалювати положення Конвенції РЄ № 108 стосовно проблем європейської інтеграції. У цьому плані Кабінет Міністрів Ради Європи затвердив Поправки від 15.06.99 р. щодо приєднання до неї держав Європейського Союзу. Вони передбачають застосування положень Конвенції РЄ № 108 до даних, які стосуються груп осіб, асоціацій, фондаций, компаній, корпорацій та будь-яких інших установ, що безпосередньо чи опосередковано формуються з окремих осіб, незалежно від того, мають такі установи правосуб'єктність чи ні.

Щоб процеси торгівлі не потерпали від європейських вимог щодо захисту даних, країни Сходу (Австралія, Гонконг, Нова Зеландія), Південної Африки, Америки (Канада) стали також приймати відповідні закони з питань захисту даних. Близько 40 країн світу мають закони з питань персональних даних. Але інформаційне законодавство багатьох з них має суттєві недоліки. Навіть у найбільш демократичних країнах поширеним є несанкціоноване прослуховування та інші порушення законів, що визначають порядок доступу до даних, що розповсюджуються за допомогою електронних каналів зв'язку [3].

Як раніше зазначалося, Конвенція РЄ № 108 є першим та головним документом, який визначає основоположні, уніфіковані принципи створення національного законодавства країн світу у сфері захисту персональних даних.

Через 14 років, у 1995 р., Європейський парламент та Рада Європейського Союзу запровадили першу в ЄС законодавчу ініціативу щодо персональних даних – Директиву 95/46/ЄС “Про захист осіб у зв'язку з обробкою персональних даних і вільним обігом цих даних” від 24.10.95 р.<sup>4</sup> Згідно з директивою зміст європейської моделі захисту персональних даних можна визначити як “забезпечення єдиними механізмами виконання”.

Європейський Союз визначає, що прагне до того, щоб суб'єкти персональних даних мали визначені права і реальну можливість звернутися до посадової особи або органу, що зобов'язаний вжити дії для їх захисту. Кожній країні, що є учасником Євросоюзу, також як і в Конвенції РЄ № 108, рекомендовано створити уповноважений орган (або органи) із захисту персональних даних. Зазначене має на меті створення умов уніфікованого рівня організації та контролю за діяльністю у сфері захисту персональних даних.

<sup>4</sup> Матеріали Директиви 95/46/ЄС див. у розділі журналу “Європейські правові стандарти”.

У 1997 році був затверджений наступний документ – Директива 97/66/ЄС Європарламенту і Ради Євросоюзу від 15.12.97 р. “Про обробку персональних даних і захист прав людини в телекомунікаційному секторі” [1, с. 337-344]. Проте, після подій у Нью-Йорку 11.09.01 р. у рамках антитерористичної кампанії Європейський парламент 30.05.02 р. скасував її положення.

Стосовно Інтернет-відносин, то у листопаді 2003 р. Європейський суд дав чітке пояснення: *“згадування конкретних людей у розташованих на Інтернет-сайтах матеріалах, публікація їх імен чи будь-якої іншої конкретної інформації про них, є операцією з персональними даними. Стосовно подібних дій повинна застосовуватися Директива 95/46/ЄС із захисту персональних даних”*.

У плані основних напрямів та тенденцій із забезпечення інформаційної безпеки спостерігається наступне:

- вводяться е-паспорти, за допомогою яких (завдяки чипам) стає можливим відслідковувати (із супутника) будь-кого і будь-де;
- обмежуються (у багатьох країнах) можливості самозахисту за допомогою криптографії. Вводиться обов’язковість надання “ключів” дешифрування відповідним службам;
- має місце широка практика об’єднання БД на основі ідентифікаційних номерів: податкової, медичної, соціальної інформації, відомостей про майно, родинний стан, особисті таємниці, засіб життя тощо дозволяє створити вичерпне дос’є (навіть негативне), доступне необмеженому колу осіб;
- активно використовуються системи відео спостереження в умовах відсутності зацікавленості урядів у прийнятті конкретних законів. Системи щодо порядку оповіщення громадян про спостереження, збереження записів і доступу до них не створено.
- обмежується можливість анонімності при використанні коштів комунікації (якщо не можна ідентифікувати суб’єкта відправленої транзакції);
- застосовуються технології перегляду змісту е-пошти під час відсутності законодавчих обмежень. Хоча вважається, що е-пошта і дані, що містяться у комп’ютері, така ж особиста недоторканна сфера, як житло;
- ведуться генетичні дослідження. Тестування і створення БД ДНК вже є реалією. Небезпека – можливість робити генні висновки про риси особи і складання характеристики. При цьому медичні дані дорого коштують (щодо діагнозів захворювань, відомості про аналізи, запропоновані рецепти тощо, навіть про лікарів, що обслуговують);
- практично боротьба зі “спамом”, “сокетом” (рекламні розсилання) і “троянським конем” (викачуванням інформації) має номінальний зміст. Продаж персональних даних за допомогою “спаму” – звичайна практика. Програми-шпигуни запитують анкетні дані та створюють дос’є користувачів Інтернету, а потім це несанкціоновано використовується в особистих, політичних чи економічних інтересах.

**Постановка проблеми.** Відповідно до статті 32 Конституції України 1996 р.: *“Ніхто не може зазнавати втручання в його особисте життя, крім випадків, передбачених Конституцією України. Не допускається 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”*.

У 2010 році Президент України Віктор Янукович підписав Закон “Про захист персональних даних” (№ 2297-VI), який Верховна Рада прийняла 1 червня [4].

Аналіз багатьох публікацій (див. наведену літературу, посилання на джерела та Інтернет за ключовими словами) свідчить про те, що проблематика захисту персональних даних викликає занепокоєння у значній кількості людей у зв'язку з наявністю загально визнаного європейськими правовими стандартами права на недоторканність приватного життя, з одного боку, а з іншого – поширенню у житті реалій несанкціонованого використання персональних даних не уповноваженими на це особами. Іншими словами, міжнародне право та світові стандарти – є, Конституція – є, закон про захист персональних даних – є, а захист практично існує “на папері”. Об'єктивно це може визначатися труднощами політичної та соціально-економічної реформації, яка, на превеликий жаль, йде в Україні досить повільно.

З іншого боку, побутує думка, що проблема захисту персональних даних у наш час не актуальна у зв'язку з нерозвиненістю громадянського суспільства, наявністю менталітету примата держави і низьким рівнем інформатизації. При цьому зрозуміло, що немає жодної області життєдіяльності людини, суспільства та держави, де не застосовувалися б персональні дані. Парадоксальність ситуації у тому, що потреба в захисті персональних даних громадян об'єктивно існує, але вона серйозно не сприймається.

Є три основні причини для руху в напрямі удосконалення нормативно-правового упорядкування відносин у сфері захисту персональних даних, із яких виходять європейські та інші країни:

- усунення передумов та порушень прав людини на її персональні дані;
- розвиток е-комерції (е-бізнесу, е-торгівлі);
- гармонізація національних законодавств відповідно до приписів континентального права та норм європейських правових стандартів.

Для України актуальність і об'єктивна необхідність захисту прав громадян в інформаційній сфері визначається:

- розвитком інформаційних технологій і розповсюдження автоматизованих засобів і засобів збору, обробки, зберігання і поширення персональних даних;
- значною активністю у формуванні баз даних (соціального, фінансового, маркетингового, медичного, екологічного, адміністративного, правоохоронного та ін. змісту) та несанкціонованим поширенням персональних даних;
- використанням інформаційних технологій кримінальними структурами, що підривають зусилля з розвитку і зміцнення демократичної, правової держави.
- потребою у приведенні норм вітчизняного законодавства до приписів європейських правових стандартів в аспекті участі України в міжнародному процесі обміну інформацією, в міжнародних проектах, що засновані на використанні інформаційних технологій у різних секторах соціальної, економічної, наукової та науково-технічної діяльності.

Таким чином, проблема, що розглядається, не може не викликати стурбованості та нарікань щодо існуючого стану та потреби у створенні в державі цілісного та ефективного механізму захисту людиною своїх прав стосовно її персональних даних.

**Метою статті** є підсумок стану та формулювання пропозицій щодо створення цілісної системи у сфері захисту персональних даних в Україні.

**Виклад основних положень.** Сьогодні Україна перебуває на порозі доленосного рішення. Мова йде про підписання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом і його державами-членами, з іншої сторони [5] (далі – Угода про асоціацію), проект якої було схвалено Урядом України 18 вересня 2013 року [6].

У проєкті Угоди про асоціацію, у статті 15 “Захист персональних даних” (Розділ III “Юстиція, Свобода та Безпека”), визначено: “Сторони погоджуються співпрацювати з метою забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів, зокрема відповідних документів Ради Європи. Співробітництво у сфері захисту персональних даних може включати, *inter alia* (“в тому числі” – Авт.), обмін інформацією та експертами”. Надалі Угода про асоціацію згадує поняття “захист персональних даних” ще чотири рази (ст.ст. 80, 123, 129 та 141) і лише у декларативному значенні повтору його необхідності. Про інструменти чи механізми реалізації правового захисту персональних даних мови у документі не йде, на противагу детальному розкриттю упорядкування відносин щодо економічних аспектів.

Звернемо увагу на те, що *Європейський Союз* має економіко-правову спрямованість діяльності, яка передбачає об’єднання європейських держав, націлене на їх інтеграцію з метою *формування спільного ринку*, що передбачає вільний рух товарів, капіталу і послуг, включаючи скасування паспортного контролю в межах Шенгенської зони, а також виробляє спільну політику в області торгівлі, сільського господарства, рибальства і регіонального розвитку. У складі інститутів ЄС є посада *Інспектора із захисту даних*.

Одночасно, *Рада Європи* має соціально-правову спрямованість діяльності, яка передбачає сприяння співпраці між всіма країнами світу з метою *впровадження стандартів права, демократичного розвитку, законності і культурної взаємодії*. Ця міжнародна організація є повністю самостійною, яка не входить в систему інститутів ЄС.

Україна у 2006 році ратифікувала Конвенцію Ради Європи № 108 “Про захист осіб у зв’язку з автоматизованою обробкою персональних даних” від 28.01.81 р. та “Додатковий протокол до Конвенції про захист осіб у зв’язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних” від 08.11.01 р. Раніше зазначалося, Конвенція РЄ № 108 є першим та головним документом у сфері правового захисту персональних даних, який був прийнятий на розвиток положень Конвенції Ради Європи “Про захист прав та основоположних свобод” 1950 р.

Головними у Раді Європи вважаються два окремих інститути, які очолюють:

- Омбудсмен (від швед. – “захисник народу”) – загальні питання прав і свобод;
- *Комісар із захисту персональних даних* – усі питання щодо персональних даних.

Кожний з інститутів підпорядкований особисто Генеральному секретарю Ради Європи.

Якщо неупереджено порівняти функціональне призначення зазначених міжнародних організацій та деякі їх акти (див. Таблицю 2), кожен з яких спрямований на уніфікацію національних законодавств, може виникнути дилема у виборі рішень стосовно пріоритетів захисту прав людини у сфері персональних даних.

Економіка як сукупність виробничих відносин не може існувати без наявності певних відомостей, зокрема персональних даних. Держава також потребує персональних даних у контексті необхідності зворотного зв’язку в управлінні і забезпечення інформаційної безпеки, яка є складовою національної безпеки. Звідси й потреба в отриманні різноманітних даних та відповідному нормативному упорядкуванні відносин.

З іншого боку – присутній соціально-правовий аспект та міжнародне визнане право людини на повагу до її приватного і сімейного життя, до недоторканості житла і таємниці кореспонденції. В Україні статтею 32 Конституції встановлено – “...Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом”. Це визначає необхідність обмеження в поширенні персональних даних.



Відзначене, на наш погляд, й обумовлює складнощі у нормативно-правовому та організаційному вирішенні проблем, які існують у сфері захисту персональних даних.

Таблиця 2

Рада Європи	Європейський Союз
<b>Основні акти</b>	
<p>Конвенція РЄ № 108 “Про захист осіб у зв’язку з автоматизованою обробкою персональних даних” від 28.01.81 р.                      Протокол до Конвенції РЄ № 108 щодо органів нагляду та транскордонних потоків даних від 08.11.01 р.</p>	<p>Директива 95/46/ЄС “Про захист осіб у зв’язку з обробкою персональних даних і вільним обігом цих даних” від 24.10.95 р.                      Регламент ЄС № 45/2001 “Про захист фізичних осіб щодо обробки персональних даних установами і органами ЄС та вільного переміщення таких даних”</p>
<b>Деякі інші документи на розвиток основних актів</b>	
<p>Рекомендації РЄ № R (81)1 “Про захист персональних даних у автоматизованих базах медичних даних”                      Рекомендації РЄ № R (81)19 “Про доступ до інформації, що знаходиться у розпорядженні державних органів”                      Рекомендації РЄ № R (91)10 “Про передачу третім особам персональних даних, які знаходяться в розпорядженні державних органів”                      Рекомендації РЄ № R (87)15 “Про регулювання використання персональних даних у секторі поліції”                      Рекомендації РЄ № R (99)5 “Про захист осіб у зв’язку з обробкою даних у інформаційних магістралях”                      Рекомендації РЄ № R (2000)13 “Про європейську політику доступу до архівів”                      Рекомендації РЄ № R (95)13 “Про кримінально-процесуальні принципи, пов’язані з інформаційними технологіями”                      Рекомендації РЄ № R (99)15 “Про висвітлення у засобах масової інформації виборчих компаній”                      Рекомендації РЄ № R (2000)7 “Про права журналістів не розголошувати їх джерела інформації”                      Рекомендації РЄ № R (89)9 “Про злочини, пов’язані з комп’ютерами”</p>	<p>Директива 96/9/ЄС “Про правовий захист баз даних”                      Директива 97/13/ЄС “Про спільну базу для загальних дозволів та індивідуальних ліцензій в сфері телекомунікаційних послуг”                      Директива 96/19/ЄС ЄС “Про внесення поправок до Директиви 90/388/ЄЕС “Про забезпечення повної конкуренції на ринках телекомунікацій”                      Резолюція Ради ЄС від 20.06.01 р. “Про оперативні запити правоохоронних органів щодо громадських телекомунікаційних мереж та послуг”                      Директива 97/66/ЄС “Про обробку персональних даних і захист прав осіб у телекомунікаційному секторі” (скасована)                      Директива 97/7/ЄС “Про захист прав споживачів у дистанційних контрактах”                      Резолюція Ради ЄС від 17.01.95 р. “Про законне перехоплення телекомунікаційних повідомлень”                      Директива 99/93/ЄС “Про систему електронних підписів, що застосовується в межах Співтовариства”                      Директива 2000/31/ЄС “Про правові аспекти інформаційних послуг щодо електронної комерції на внутрішньому ринку”                      Директива 2002/58/ЄС “Про обробку персональних даних та захист таємниці у секторі телекомунікацій”</p>

Сьогодні, виходячи з європейських і світових уявлень про права і свободи журналісти борються за свободу слова. Віруючі – відстоюють свободу віросповідання і виступають проти заміни імені людини на ідентифікаційний номер. Мусульмани – заперечують будь-яке втручання в тіло людини (біометрія, чипи). Іудеї – проти того, щоб рахували євреїв. Правозахисники – стурбовані проблемами у реалізації права на

приватність персональних даних, поширеним несанкціонованим прослуховуванням телефонних розмов тощо. Підприємці – не бажають щоб інформація про їх і їхню діяльність (угоди, доходи, нерухомість, автомобілі, їхня родина тощо) потрапляла до рук злочинців (хоча саме в цьому середовищі спостерігається найактивніша діяльність із збору в БД персональних даних; як запевняють – в комерційних інтересах<sup>5</sup>). Пенсіонери – намагаються захистити свої права від бандитів, які завдяки “наведенню” з існуючих баз персональних даних шахрайськими способами заволодівають їх квартирами, майном тощо.

При цьому, процес отримання персональних даних перетворюється на окремий бізнес, метою якого є тільки збір, обробка та поширення персональних даних на комерційних засадах. Раніше персональні дані накопичувалися в картотеках і державних реєстрах. Тепер вони активно обробляються в комп’ютерах у приватних інтересах. Роблячи покупки в Інтернет-магазинах та отримуючи дисконтні картки, споживач змушений повідомляти свої персональні дані. Власники зазначених магазинів, з одного боку, зацікавлені у відомостях про стан попиту на ринку, який може бути оцінений завдяки відомостям про покупців та потенційних споживачів їх продукції, а з іншого – не завжди забезпечують захист персональних даних людини, навіть можуть збирати та пропонувати зазначені дані для продажу й отримання іншого виду прибутку, без диверсифікації номенклатури продукції. Останнє в умовах ринку – значний важіль у конкурентній боротьбі, гарант від розорення при змінах кон’юнктури.

Природно, там, де “пахне” грошима, відразу виникає й активно розвивається відповідна злочинність. Збір та продаж персональних даних – звичайно не виняток. Відомості про паспортні та медичні дані, звички, коло знайомих, матеріальний стан, особисте життя, маршрути подорожей та багато ін. збираються у БД та реалізуються на дисках або розміщуються в Інтернеті. Коштує така БД від 10 (дрібний продаж) – до 1500 (через Інтернет) дол. Інформація мобільного зв’язку потрапляє на чорний ринок (номер коштує 50 дол., прослуховування – 150 дол. на рік). Як зазначалося у [8]: “...світовий ринок персональних даних досягає 3 млрд. доларів у рік”, у Росії – 20 - 24 млн. дол., а деякі експерти вважають, що він становить 100 млн. дол. на рік [9, 10]. У [11] повідомлялося, що збиток, завданий британській економіці розкраданнями ідентифікаційних даних у 2006 р., становив 1,8 млрд. ф. ст., а на кінець десятиріччя ця цифра могла досягти 3,8 млрд. ф. ст. завдяки росту злочинності у е-середовищі.

Окремі приклади комерційного поширення персональних даних див. на Рис. 1, 2.

Ті, хто займається маркетингом, продовжують вишукувати нові шляхи для збору будь-яких відомостей про своїх конкурентів та потенційних покупців: їх діяльність, оточення, стосунки, погляди, інтереси, характер, поведінка та багато ін. Для бізнесу персональні дані – зручне, а тепер і необхідне доповнення із усього того, що надає Інтернет або інші мережі. Уже цілком чітко усвідомлено, що за допомогою засобів е-середовища набагато легше збирати величезні обсяги різної інформації, а аналіз і взаємне ув’язування відомостей забезпечує істотні прибутки і лідерство в бізнесі. Критерії, відповідно до яких відомості про людину включаються до списку, призначеного для маркетингових заходів, очевидні. Так дані про людину, що має машину, вносять до

---

<sup>5</sup> Перша картотека персональних даних та комерційне поширення відомостей із неї з’явилися у 1886 році, коли шовкоторговець Л’юїс Тепен із Нью-Йорка створив агентство збору та аналізу інформації про кредитоспроможність підприємців, які зверталися до нього за позикою. Накопичивши декілька томів кредитних звітів, він став продавати інформацію. Клієнти платили від 100 до 200 дол. на рік [7].

списку її відповідної моделі; дані про власників моторних човнів – до списку відповідних моделей володарів човнів, і так далі.

**Предлагаем Вашему вниманию новейшие базы данных**  
 телефон для связи **8-066-295-91-36**

1. ГТК Украина 2003/2004/2005/2006 Базы данных по внешнеэкономической деятельности (таможня) \* 250 грн.  
 Отправитель, адрес отправителя, получатель, адрес получателя, код банка, МФО, адрес банка, счет, ответственный за фирму, его адрес, наименование товара, вес, стоимость, направление (импорт-экспорт).
2. Украина - Минстат - 2006.01.01 \* 250 грн.  
 Организации, адреса, телефоны, учредители, работники, нарушения, ликвидации
3. Физические лица \* 250 грн.  
 Фамилия, имя, отчество, дата получения кода, дата рождения, адрес рождения, адрес проживания, телефон, пол.
4. Доходы физических лиц Украины 2004/2005 \* 400 грн.  
 Доходы та налоги, место работы, данные о работодателе.
5. ГНА 2005 \* 250 грн.  
 Налоговая Украины 2005\* + "Госкомстат Украины"  
 БД по зарегистрированным в Украине предприятиям. Все учетные данные по каждому предприятию, включая: наименование, юридический и фактический адреса, рег. номер, дату регистрации, регистрирующий орган, размер уставного фонда, данные об учредителях и т.д. 981000 предприятий. Объем 1,5 Gb по 20 декабря.
6. Государственный регистр предприятий \* 250 грн.  
 Регистрационные данные о предприятиях, учредители, счета предприятий, адреса, филии, иностранные представительства.

А также есть все базы по России.

Рис. 1. Комерційна пропозиція персональних даних в Україні [12].

Назва баз персональних даних	Ціна (руб)
“Приватні особи м. Москви та Московської області”	\$ 150
“Приватні особи Росії та СНД” (включає е-адресу)	\$ 200
“Фізичні особи Московської області”	1000
“Жителі Московського регіону” (повні відомості щодо паспорта)	400
“Прописка у м. Москві”	500
“Прописка у Московській області”	400
“Квартири та їх власники м. Москви”	1000
“Приватизовані квартири м. Москви”	400
“Експортно-імпортні операції” (товар, вартість, постачальник, споживач тощо)	1400
“Московська ліцензійна палата” (про ліцензії)	400
“Московська реєстраційна палата” (про юридичних осіб і приватних підприємців)	500
“Московський земельний комітет”	200
“ДАІ м. Москви” (повні відомості про автомобілі та їх власників)	500
“Посвідчення водія у м. Москва та Московській області”	500
“Мобільні телефони Московського регіону”	500
“Єдина міська телефонна мережа м. Москви”	500
“МТС 2003” ( усі телефонні номери, реквізити та адреса абонентів)	500
“Банки Росії” (усі реквізити)	300

Рис. 2. Комерційна пропозиція персональних даних в Росії [13].

В основу прямого маркетингу покладене створення списків людей, поєднаних загальними демографічними даними. І для цих цілей зовсім не потрібна конфіденційна інформація. Головне, щоб її було якомога більше.

Реальність така, що за відсутності в державі ефективного механізму та цілісної системи захисту персональних даних структури та окремі особи, що збирають, обробляють та поширюють персональні дані, заробляють як їм заманеться, з порушенням прав тих, чії дані обробляються. Від такої “комерції” бюджет держави взагалі нічого не одержує<sup>6</sup>.

І все це на тлі ілюзорності і ефемерності абсолютного захисту та нарікань щодо недоліків законодавства України у сфері персональних даних.

### **Про деякі проблемні аспекти, пов’язані з законом.**

Історично при укладанні національних правових систем захисту персональних даних дотримуються двох принципів, які передбачають:

- створення всеохоплюючого закону про захист приватного життя, який спрямований на упорядкування інформаційних відносин, пов’язаних з визначеними даними. Цей підхід веде до необхідності коригування положень закону при появі нових загроз;

- створення спеціальних законів для кожного типу зазіхань на приватне життя або для кожної сфери, яка є потенційним джерелом загрози та порушень (наприклад, для мас-медіа, банків, телекомунікацій та ін.). Але при виникненні нових загроз такий підхід призводить до безсистемності, дублювання та суперечливості окремих норм.

У практичному застосуванні обидва підходи виявили свою низьку ефективність.

Набутий досвід враховується законодавцями – при створенні національного закону застосовують змішаний підхід. Він полягає у створенні рамкового (базового, системоутворювального) закону про захист персональних даних, а вже на його основі розробляються окремі галузеві нормативно-правові акти. При виникненні нових загроз та видів порушень прав особи на її персональні дані система захисту залишається незмінною, а до галузевих актів вносяться необхідні доповнення та зміни.

Саме в цьому і полягала основна ідея при розробці Закону України, яка так й не була сприйнята повною мірою. Створити “закон-панацею” для персональних даних на всі випадки життя не є можливим. Звідси і нарікання до окремих правових конструкцій, які є до нашого часу. Але в кожного свій погляд і свій інтерес, які, нерідко, не узгоджуються з прагненнями інших, що взагалі не сприяє створенню єдиній системи.

Розробку проекту Закону України “Про захист персональних даних” було ініційовано в 1996 році у Національному агентстві з питань інформатизації при Президенті України, після публікації статті за назвою “*Персональные данные: есть проблемы?*” [14].

Перша версія законопроекту була підготовлена до середини 1998 року. Вона неодноразово розглядалася в таких міністерствах і комітетах як: Мінекономіки, Мінфінансів, Мін’юстиції, МВС, СБУ, Комітет з питань державних секретів, Державна податкова адміністрація, Рада національної безпеки і оборони, Уповноважений ВР України з прав людини.

---

<sup>6</sup> Якось після демонстрації дослідів з електрикою, Майкла Фарадея запитали: “*Яка користь від електрики?*”

Він відповів: “*Коли-небудь ви будете мати можливість обкласти її податком*”.

Наведемо тільки деякі відомості щодо кількості експертиз (розглядів) та зауважень в органах влади.

*Мін'юстиції*: перший розгляд – 25 зауважень; другий – 10 зауважень; третій – 11 зауважень; четвертий – 6 зауважень; п'ятий – 3 зауваження.

*Мінекономіка*: при першому і другому розгляді було одне і те ж зауваження щодо ліцензування діяльності на персональні дані, на третій – вже 5 інших зауважень, у четвертий – законопроект був узгоджений, у п'ятий розгляд виникло нове зауваження: “...необхідним є обґрунтований прогноз про очікувані соціально-економічні наслідки закону”.

*Мінфінансів*: після першого розгляду законопроект був узгоджений без зауважень. При другому розгляді було вже 3 зауваження. При третьому і четвертому розглядах зауважень не було – узгоджений. При п'ятому розгляді – 2 зауваження.

*Державна податкова адміністрація*: при першому розгляді було 6 зауважень, при другому, третьому і четвертому розгляді зауважень не було – узгоджений, при п'ятому розгляді з'явилося 8 зауважень.

*МВС*: перший розгляд – 18 зауважень, другий – 4, третій – 1, четвертий і п'ятий – законопроект узгоджено.

*СБУ*: перший розгляд – 19 зауважень, другий – 4, третій – 3, четвертий – 7, п'ятий – 23 зауваження.

На кінець 1999 р. було враховано понад 250 зауважень та пропозицій і законопроект, погоджений з усіма державними органами влади, за винятком Мінюсту і СБУ, був 27 грудня спрямований до Кабінету Міністрів України (вих. № 5555 Держкомзв'язку).

Після внесення поправок профільними відділами секретаріату КМУ законопроект в котре був розісланий на узгодження до тих самих органів влади, а також до Міністерства освіти і науки та Міністерства закордонних справ.

До окремих особливостей експертизи в міністерствах і комітетах можна віднести:

- відсутність системності і послідовності в організації роботи по проведенню експертизи. Це полягало в тому, що у зв'язку із змінами керівництва органів та виконавців експертиза виконувалася різними особами і зауваження часто повторювалися;
- нерідко виконавці мали туманне уявлення про предмет експертизи, що було зрозуміло з формулювань зауважень, а також запитань у процесі телефонних розмов;
- заперечення Мін'юстом можливості введення в законодавство нової юридичної категорії – “права власності фізичної особи на свої персональні дані”<sup>7</sup>, не зважаючи на розвиток комерції з персональними даними. Іншими словами, нами пропонувалося додати людині повноваження на її персональні дані, властиві праву власності, та в межах визначених Конституцією. Проте, в висновках Мін'юсту (зокрема, вих. № 23-9-4450 від 27.06.00 і № 23-9-7900 від 2.11.00 р.) наголошувалося те, що вказана пропозиція “...свідчить про недостатній рівень опрацьованості проекту та суперечливе розуміння авторами проекту поняття власності”.

Зазначимо при цьому, що не так давно (!) Єврокомісія визнала за доречне дослідити цю нашу юридичну новацію на предмет введення до законодавства ЄС.

<sup>7</sup> Див. книгу “Защита персональных данных”, видану у 1998 році [15], в якій представлено першу версію законопроекту (С. 81-96) та надано відповідну аргументацію механізмів його реалізації, зокрема щодо власності на персональні дані (С. 41-42). У подальшому процес удосконалення рішень розглядався та доводився нами до громадськості у наукових статтях, зокрема [16 – 23] та книгах [2, 24 – 29].

До липня 2000 р. законопроект “Про захист персональних даних” в Україні підписали керівники наступних органів влади: Мінфінансів, Мінекономіки, Міносвіти і науки, Державної податкової адміністрації, МВС, СБУ, МЗС, Держкомзв’язку, після чого знову було спрямовано до Кабінету Міністрів України.

Через шість років, після того як законопроект пройшов додаткову експертизу юристів інших міністерств, комітетів та громадських організацій, був підтриманий спеціалістами у сферах інформаційного та адміністративного права, інформатизації, та інформаційної безпеки, які мають наукові ступені та звання (академіки та члени-кореспонденти НАН України та НАПрН України – 9; доктора наук – 18; кандидати наук – 24), врахував понад 600 зауважень та пропозицій, отримав позитивний висновок Головного науково-експертного управління Апарату ВР України, 16 березня 2006 р. він був прийнятий у другому читанні та в цілому абсолютною більшістю народних депутатів України (згідно поіменного голосування: За – 287; Проти – 0; Утрималися – 1; Не голосували – 108. Всього – 396 депутатів), але потім Закон... зник.

Зауважимо, за роки розробки проект Закону України “Про захист персональних даних” обговорювався на численних конференціях, семінарах, “круглих столах” тощо (за загальним підсумком – понад 40). Про першу версію автори проекту (В. Брижко та О. Баранов) доповіли на засіданні експертів “Впровадження міжнародних стандартів із захисту приватності інформації персонального характеру в Україні” у присутності Комісара Ради Європи із захисту даних, виконавчого члена Комісії Австрії у питаннях захисту даних пані Вольтраут Кочі.

Лише у 2010 році проект закону без суттєвих змін знову внесено на розгляд та голосування депутатів. Згідно з поіменним голосуванням у другому читанні та в цілому проголосувало народних депутатів України: За – 355; Проти – 0; Утрим. – 0; Не голосували – 61. Всього – 416 депутатів. Підписаний Президентом України Закон № 297-VI від 01.06.10 р. набрав чинності з 01.01.11 р.

### ***Висновки та окремі пропозиції.***

1. Законодавство про захист персональних даних практично в жодній країні світу не отримало своєї зрілості, навіть на термінологічному рівні. Повна адекватність національних законодавств про захист персональних даних ще не досягнуто.

Основною проблемою нормативно-правового упорядкування відносин у сфері захисту персональних даних є протиріччя між прагненням максимального використання персональних даних у державних та корпоративних інтересах й, одночасно, особисте бажання кожної людини максимально захистити свої права.

Теоретично ідея захисту персональних даних виходить з необхідності захисту індивідуума і гарантій верховенства його інтересів над “державними та суспільними інтересами”. Зазначені інтереси, звичайно, можуть бути спрямовані на виконання волі одного керівника (лідера) із силою і невідворотністю натовпу. Проте будь-яке насильство повинне застосовуватися процедурно, згідно загальносвітових принципів визначених Конвенцією Ради Європи № 108 “Про захист осіб у зв’язку з автоматизованою обробкою персональних даних” від 28.01.81 р.

2. Можна стверджувати, що Закон України “Про захист персональних даних” відповідає принципам, закладеним у Конвенції Ради Європи № 108 від 28.01.81 р.

Головна проблема на національному рівні полягає у відсутності ефективного правового механізму щодо адміністративно-організаційного регулювання відносин (який детально надавався у [30]) та відповідальності у сфері захисту персональних даних. Незважаючи на санкції, введені Законом України “Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення

законодавства про захист персональних даних” (набрав чинності 01.01.12 р.), практична відповідальність за порушення закону продовжує носити декларативний характер.

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. По-друге, зайва деталізація упорядкування відносин у цій сфері в умовах розвитку інформаційного суспільства може знижувати попит на розробку нових інформаційно-комп’ютерних технологій. Це обумовлена мотивація для “бізнес-софт-індустрії”, яка не буде зацікавленою у технологіях, здатних забезпечити сильний захист.

3. У повсякденному житті фізична особа виступає у двох іпостасях: як “людина” та як “громадянин” (як зауважував Ш. Монтескьє: “Свобода личности и свобода гражданина не всегда совпадают”). У принципі, для створення умов більш сильного захисту персональних даних у законодавстві це потребує їх розмежування.

Захист прав “людини” від несанкціонованої комерційної діяльності з її даними має здійснюватися завдяки засобам потужного “інституту власності” (через тріаду повноважень – користування, володіння, розпорядження). Це надає можливість безпосереднього залучення людини до процесу захисту своїх персональних даних на визначених законом умовах.

Підкреслимо, зазначений захист має стосуватися лише того аспекту, коли мова йде про “людину” персональні дані якої використовують з комерційною метою: збирання даних з різних джерел, створення баз персональних даних та їх поширення на комерційних засадах, здійснення чого в обов’язковому порядку повинно враховувати добре відоме оголошення: *Стій! Приватна власність. Вхід заборонено.*

Діяльність органів державної влади, зокрема функціонування її силових структур, не є можливою без персональних даних. Для органів влади фізична особа виступає як “громадянин”, використання даних якого повинно здійснюватися у межах повноважень наданих Конституцією та галузевими законами.

Така постановка справи, з одного боку, надає законодавству в сфері захисту персональних даних нову якість, системність та перспективність, про що детально йдеться у [15, с. 40-42; 23, с. 169-176; 24, с. 38-42; 22, с. 45-54; 24, с. 12-25; 25, с. 66-68; 29, с. 65-69].

З іншого – ця новація у повному обсязі відповідає положенню статті 11 Конвенції РЄ № 108 “Жодне з положень цієї глави (Глава II – Основоволожні принципи захисту даних – від Авт.) не тлумачиться як таке, що обмежує або іншим чином перешкоджає можливості Сторони забезпечувати суб’єктам даних більший ступінь захисту, ніж передбачений цією Конвенцією” [1, с. 68].

До вказаного додамо наступне.

До теперішнього часу законодавство не дає відповідь на питання – кому належать майнові блага від використання персональних даних будь-якої конкретної особи?

Згідно зі статтею 8 Закону України “Про захист персональних даних” від 01.06.10 *суб’єкт персональних даних має особисті немайнові права на персональні дані.* Й це у той час, коли їх *не санкціоновано* збирають та *продають*.

Зазначимо, що поняття “особисті немайнові права” залучено з Цивільного кодексу України і запроваджено лише у нашій країні. У міжнародному праві, праві Європейської Спільноти, а також у законодавстві європейських країн його і не існує. При цьому, ані в Конституції України, ані в ЦКУ поняття “персональні дані” не вживається. А слово “особистих”, що пристосовано у ЦКУ до “немайнових прав”, взагалі зайве. Зазначене поняття сприймається як “масло-масляне” та сприяє підтримці “системи”, яка в умовах е-середовища може працювати лише формально та адміністративно-суб’єктивно.

4. Проблема реєстрації баз персональних даних в Україні потребує додаткових досліджень та врахування практичного досвіду, який мають провідні європейські держави, наприклад, *Великобританія*.

Інститут Уповноваженого з питань захисту персональних даних у Великобританії функціонує на основі Закону “Про захист даних ” від 12.07.84 р. Він визначив посади Міністра по захисту даних, Реєстратора по захисту даних і утворив Суд по захисту 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 обов’язки:

- ведення реєстру осіб, які збирають і зберігають персональні дані, а також мають комп’ютерні бюро і надають послуги щодо персональних даних;
- вручення повідомлень про порушення закону, про скасування реєстрації або про заборону передачі даних;
- розгляд скарг про порушення закону.

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

Основними елементами системи захисту персональних даних у Великобританії є:

- ведення реєстру баз персональних даних та осіб, які надають послуги щодо персональних даних;
- перевірка і контроль діяльності з персональними даними;
- вручення повідомлення про порушення, про скасування реєстрації, про заборону передачі даних;
- адміністративне і судове оскарження у зв’язку із захистом даних.

5. Виходячи з практики розділення повноважень та функцій структур Уповноваженого з прав людини (Омбудсмена) та Уповноваженого з питань захисту персональних даних (Комісара із захисту персональних даних), які існують в адміністрації Ради Європи і європейських країнах, є необхідність оцінки такої підходу, шляхом практичного ознайомлення та вивчення відповідного досвіду, наприклад у *Німеччині*.

У цій країні Інститут Комісара почав формуватися в 1970 році, коли в Землі Гессен вперше у світі був прийнятий Закон “Про захист даних ”. Закон установив державну посаду Комісара із захисту даних на правах єдиначальності. Цьому виборному державному службовцю закон надав і забезпечив право повної незалежності від владних структур, а також надав право спостереження за діяльністю щодо персональних даних.

Сьогодні захист персональних даних у країні визначається положеннями Федерального Закону “Про подальший розвиток обробки і захисту даних” від 20.12.90 р. Згідно із законом за поданням Федерального уряду Бундестаг на строк 5 років обирає Федерального уповноваженого з питань захисту даних, який потім призначається на посаду Президентом.

6. Через те, що законодавство відстає від розвитку технологій та можливостей Інтернету, а корпоративні засоби захисту персональних даних не завжди відповідають принципам європейських правових стандартів, захист прав людини у сфері персональних даних вимагає визначення особливих повноважень та можливостей із контролю та регуляції інформаційних відносин різних суб’єктів незалежним від владних структур Уповноваженим із захисту персональних даних в Україні (можливо на прикладі Німеччини – подвійне підпорядкування: Бундестагу (щорічний звіт та отримання завдань) та Міністру внутрішніх справ (нагляд за діяльністю та допомога у перевітках).



Щодо України, то однією з важливих функцій Уповноваженого має стати постійне відстеження змін в розвитку нових інформаційно-комп'ютерних технологій та оперативне вживання заходів захисту персональних даних.

7. Вирішення завдання створення в Україні цілісної системи ефективного захисту персональних даних є однією з головних складових загальної соціально-політичної та економічної проблеми, пов'язаною з побудовою інформаційного суспільства. У правовій, соціальній державі це визначається потребою в узгоджені суперечливих але взаємопов'язаних аспектів упорядкування соціальних та економічних інформаційних відносин за умов забезпечення інформаційної безпеки. Зазначене регулювання не можна обмежувати тільки нормами Конституції та окремими не дуже пов'язаними між собою статтями деяких чинних законів.

Для сфери захисту персональних даних в Україні необхідними є додаткові галузеві закони, у яких принципи рамкового Закону України “Про захист персональних даних” мають бути деталізовані, не порушуючи при цьому юридичні рамки його цільового та функціонального призначення.

8. У загальному плані для створення в Україні цілісної системи ефективного захисту персональних даних слід запровадити Судову палату з питань захисту персональних даних та почати підготовку кваліфікованих фахівців для цієї сфери.

### Використана література

1. Системна інформатизація правоохоронної діяльності: європейські нормативно-правові акти та підходи до упорядкування суспільних інформаційних відносин у зв'язку з автоматизованою обробкою даних у правоохоронній діяльності : посібник. – Кн. 2 / [В. Брижко, М. Швець та ін.] ; за ред. д.е.н., професора М. Швеця. – К. : ТОВ “Пан Тот”, 2006 р. – 509 с.
2. е-майбутнє та інформаційне право / [В. Брижко, Ю. Базанов та ін.] ; за ред. д.е.н., професора М. Швеця. – [2-е вид., доп.]. – К. : ТОВ “Пан Тот”, 2006. – 234 с.
3. Прослушивание телефонов в международном праве и законодательстве одиннадцати европейских стран ; сост. Е.Е. Захаров. – Х. : “Фолио”, 1999. – 152 с. – (Харьковская правозащитная группа).
4. – Режим доступу : [//www.domik.kontrakty.ua](http://www.domik.kontrakty.ua)
5. – Режим доступу : [//www.kmu.gov.ua/kmu/control/uk/publish/article?art\\_id=246581344&cat\\_id=223223535](http://www.kmu.gov.ua/kmu/control/uk/publish/article?art_id=246581344&cat_id=223223535)
6. – Режим доступу [//www.dengi.ua/news/123868\\_Associaciya\\_s\\_ES\\_ne\\_grozit\\_Ukraine\\_poterej\\_ekonomicheskoy\\_nezavisimosti\\_-\\_evrokomissar.html](http://www.dengi.ua/news/123868_Associaciya_s_ES_ne_grozit_Ukraine_poterej_ekonomicheskoy_nezavisimosti_-_evrokomissar.html)
7. Расколота база. – Режим доступу : [//www.aferizm.ru/bb\\_bd.htm](http://www.aferizm.ru/bb_bd.htm)
8. Цена персональных данных. – Режим доступу : [//www.i2r.ru/article.shtml?id=1384](http://www.i2r.ru/article.shtml?id=1384)
9. Проблема правовой защиты персональных данных. – Режим доступу : [//www.kiev-security.org.ua/box /4/136.shtml](http://www.kiev-security.org.ua/box /4/136.shtml)
10. Законспирированный оборот. – Режим доступу : [//www.privasi.hro.org/risk/data/index](http://www.privasi.hro.org/risk/data/index)
11. Киберпреступность сильнее полиции // Обзор. – 2006. – № 103(128). – С. 6.
12. – Режим доступу : [//www.khpg.org/index.php?id=1186147137](http://www.khpg.org/index.php?id=1186147137)
13. – Режим доступу : [//www.khpg.org/index.php?id=1186147137](http://www.khpg.org/index.php?id=1186147137)
14. Баранов А.. Персональные данные : есть проблемы? / Зеркало недели, 15.06.96 г.
15. Брыжко В.М. Защита персональных данных / [А.А. Баранов, В.М. Брыжко, Ю.К. Базанов]. – К. : Национальное агентство по вопросам информатизации при Президенте Украины, 1998. – 128 с.
16. Баранов А.А., Брыжко В.М. Защита персональных данных / Деловая Украина, 08.10.97 г.
17. Персональні дані та право власності // Українське право. – 2002. – № 1. – С. 152-157. – (Українська правнича фундація).

18. Про приєднання України до Конвенції № 108 Ради Європи // Право України. – 2003. – № 1. – С. 34-37.
19. Організаційно-правовий захист персональних даних // Бюлетень з обміну досвідом роботи. – 2003. – № 144. – С. 27-33. – (Міністерство внутрішніх справ України).
20. Перспективи приєднання України до Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних // Проблеми пенітенціарної теорії і практики. – 2003. – № 8. – С. 136-140. – (Бюлетень МВС України та КІВС).
21. Упорядкування суспільних відносин у сфері захисту персональних даних // Правова інформатика. – 1/2003. – С. 43-47.
22. Про економічний аспект захисту персональних даних у контексті права власності на інформацію // Правова інформатика. – № 1(9)/2006. – С. 45-48.
23. До питання е-торгівлі та захисту персональних даних // Правова інформатика. – № 1(13)/2007. – С. 12-25.
24. Права человека и защита персональных данных / [А.А. Баранов, В.М. Брыжко, Ю.К. Базанов]. – Харьков: ХПГ-Фолио, 2000. – 280 с. – (Издана при содействии Харьковской правозащитной группы и Национального фонда поддержки демократии США).
25. Правовий механізм захисту персональних даних / В.М. Брижко : монографія ; за заг. ред. д.е.н., професора М.Я. Швеця та д.ю.н., професора Р.А. Калюжного. – К. : Парламентське видавництво, 2003. – 120 с.
26. Інформаційне право та правова інформатика у сфері захисту персональних даних : монографія / [В. Брижко, М. Гуцалюк, М. Швець та ін.] ; за ред. д.е.н., професора М. Швеця. – К. : ТОВ “Пан Тот”, 2005. – 333 с.
27. Електронний банкінг у контексті захисту персональних даних : монографія / [В. Брижко, Ю. Базанов та ін.] ; за ред. д.е.н., професора М. Швеця. – К. : ТОВ “ПанТот”, 2008 р. – 141 с.
28. Методологічні та правові засади упорядкування інформаційних відносин : монографія / В.М. Брижко. – К.: ТОВ “ПанТот”, 2009. – 418 с.
29. Основи систематизації інформаційного законодавства : теоретичні та правові засади : монографія / В.М. Брижко. – К. : ТОВ “ПанТот”, 2012 р. – 304 с.
30. Організаційно-правові питання захисту персональних даних : дис. на здобуття наук. ступеня канд. юрид. наук : 12.00.07 – теорія управління; адміністративне право і процес; фінансове право; інформаційне право / Брижко Валерій Михайлович ; Національна академія державної податкової служби України. – К., 2004. – 251 с.

~~~~~ \* \* \* ~~~~~