

8. Інформатизація, право, управління (організаційно-правові питання). Монографія. – К.: НДЦ правової інформатики АпрН України, 2002.

9. Інформаційне право та інформаційна безпека / Сучасний стан, поняття та визначення змістовної частини, інкорпорація нормативних актів з правових питань у сфері інформації та її захисту. Наукове видання. /Гавловський В.Д., Коваленко О.І., Гіжевський В.К. Цимбалюк В.С. та ін. /Заг. ред. Р. Калюжного та В. Філонова. – Київ-Донецьк: Донецький інститут внутрішніх справ МВС України. Інститут економіки та права “КРОК”, 2001.

10. е-будущее и информационное право / Брыжко В.М., Цимбалюк В.С. и др. / Под. ред. д.ю.н., профессора Р.А.Калюжного и д.э.н., профессора Н.Я.Швеца. – К.: “Интеграл”, 2002. – 263 с.



В.БРИЖКО, *заслужений винахідник республіки*

УПОРЯДКУВАННЯ СУСПІЛЬНИХ ІНФОРМАЦІЙНИХ ВІДНОСИН В СФЕРІ ПЕРСОНАЛЬНИХ ДАНИХ

1. Про загальні складнощі упорядкування суспільних інформаційних відносин

Дедалі більше стає зрозуміло, що відомі юридичні підходи упорядкування суспільних інформаційних відносин не в достатній мірі здатні забезпечити соціальну регуляцію діяльності суб'єктів в інтермережах, в Інтернет.

Однієї з головних проблем інтермереж є проблема юридичного забезпечення захисту прав людини в електронно-інформаційному середовищі (е-середовищі). І тут відразу виникають питання: як забезпечити право власності на інформацію, авторські і патентні права, право на особисте життя з точки зору персональних даних людини, право на комерційні (ділові) секрети? Додаткова складність ще й у тому, що названі інститути мають різні режими охорони та захисту, різне їхнє відношення до права власності.

Так, авторське право і промислова власність хоча й близькі по колу об'єктів охорони, але вони далеко не ідентичні. Права власності у зв'язку з результатами творчої діяльності людини регулюються по-різному: за авторським правом – спочатку укладають договір, в якому вказуються права, потім створюється відповідний об'єкт; за патентним правом – спочатку створюється винахід, потім надаються права. З минулого сторіччя ці інститути не піддаються уніфікації. Єдиної Конвенції по інтелектуальній власності нема й навряд чи вона може бути.

З певністю можна сказати, що будь-яке представлення інформації в інтермережі – це інтелектуальна праця. Навіть та інформація, що не відповідає нормам охороноздатності, зокрема, персональні дані, в інтермережі набуває характер об'єктів інтелектуальної власності - в неї вкладена творча праця. Це означає, що подібна інформація повинна захищатися вже згідно законів про авторські права. Проте правових норм, що забезпечують регуляцію відносин із такою інформацією в області інтелектуальної власності, немає.

Як підходити до правового регулювання прав на гіпертекстову сторінку, що використовує багато різних елементів – текст, малюнок, товарний знак, промисловий зразок, знак найменування, аудіо, дизайн, фото тощо? Як довести свій пріоритет по окремому елементу сторінки? Відповіді на це поки що нема.

Як розв'язувати суперечки між системою індивідуалізації у формі товарного знака, торгової марки, фірмового найменування і системою індивідуалізації у вигляді доменних імен, що ввійшла у вжиток, і не надає гарантій захисту від несумлінної комерційних діяльності? Наприклад, знак фірми “Кока-Кола” коштує \$10 тис.; товарний знак “Джип” – \$60 тис. Син чоботаря, колишній полковник бундесверу, власник всесвітньо відомої корпорації Аді Дас-

лер вже не раз судився з приводу захисту своїх прав на товарний знак “Adidas” з електронними конкурентами. Можна черевики і труси не виробляти, але, скориставшись відомим ім'ям, привернути до сайту увагу і одержувати за перегляд його змісту гроші та ще й підривати престиж фірми.

Не менше складна проблема – проблема екстериторіальності інтермереж і територіальності юрисдикції. Інтернет кордонів не визнає. Із самого початку (1968 р.) він розвивався за власними законами як засіб вільного поширення інформації, на будь-якої території.

Як вважається у США, Японії, на Заході, період “романтичного” розвитку інтермереж закінчився. Всі технологічні проблеми побудови світової інформаційної інфраструктури в принципі вирішені. Розвиток інтермереж почав визначати умови електронного бізнесу або електронної комерції (е-комерції), що не так безпечний, як здається. Так, наприклад, із збільшенням у нас в країні користувачів Інтернет зарубіжні системи електронної комерції цілком можуть перетворитися у гігантські всмоктувачі грошових ресурсів як нашого населення, так і підприємств.

Більш цього, е-комерція має не тільки позитивні сторони, але й негативні. Нові засоби комунікації та технології дозволяють “стискати” час та “скорочувати” відстані, отримувати політичні, економічні, фінансові, банківські, технологічні та ін. переваги, як у плані досягнення інтересів окремої особи, так і в масштабах груп людей, країни, регіону, світової спільноти. Однак, при зазначеному набуває розвиток значно активнішої переробки у відходи природних ресурсів, що не поновлюються.

Словом, для е-середовища потрібне відповідне інформаційне право.

В різних країнах існують різні юридичні системи. Основні питання, на які за кордоном зараз намагаються знайти відповіді, полягають у пошуку надійних умов для успіху е-комерції, захисту персональних даних і прав на інтелектуальну власність в е-середовищі. У зв'язку із екстериторіальністю інтермереж вказане потребує надійних умов забезпечення захисту прав в міжнародному соціально-правовому і економічному аспектах щодо створення глобального е-середовища. Але доки країни будуть домовлятися про єдине правове регулювання, минуть десятки років. А законів для інтермереж – немає. Механізму аналізу інформаційних потоків також немає. На Заході такі технічні системи тільки будуються, а нам – “не по кишені”, надзвичайно дорогі. У даний час в Україні існує близько 6000 зареєстрованих сайтів. Тільки через одного провайдера може проходити в день 300-400 мегабайт тексту електронної пошти (до 1000 стор. маш. тексту). Відслідковувати весь обсяг трафіку практично неможливо.

В основному спроби навести порядок у взаємостосунках в е-середовищі орієнтуються на етику, на рекомендації, роз'яснення як себе вести, щоб не постраждати. Тільки провідні країни мають зачатки національного законодавства і правила в сфері інформаційного простору, в яких надто багато суперечностей. Причому недоліки і протиріччя існують на фоні геополітичних інтересів і спроб окремих країн нав'язати свій вплив іншим країнам.

Існує думка, що проблема правового регулювання полягає у забезпеченні доказу протиправних дій в умовах нестабільності електронної інформації.

Конкретні порушення є і будуть. В принципі, в мережах вони не підлягають індивідуалізації. Дуже складно дослідити навіть легальну роботу людини, яка не збирається робити нічого протиправного. Вона просто працює, але працює анонімно. Її електронні сліди мало про що говорять і, тим більше, не можуть служити доказом протиправних дій.

Проте, як відноситися до так званого “портрета особи”, що може бути зібраний з окремих відомостей персонального змісту із різних баз даних, відомостей й, які узяті з первісного контексту і, як правило, містять викривлений образ? Хто і як взагалі повинен нести відповідальність за зміст персональних даних, що розповсюджується в інтермережі? Як забезпечити доказ у випадку виникнення спірних ситуацій? Може файл вважатися доказом?

Відповіді на ці так і інші питання також немає. Є точки зору різних фахівців, полеміка і не оране електронно-інформаційне поле щодо правового регулювання відносин різних осіб.

Виник цікавий момент: порушень немає тому, що немає відповідних правових конструкцій, а значить, можна робити, що хочеш.

Що із сказаного може впливати ?

Існує реальний світ.

Виник новий світ, відмінний від реального, світ інформатизації та інтермереж, світ електронно-інформаційного простору, що передбачає новий погляд на суспільне життя і діяльність. Цей світ дістав назву – “Інформаційне суспільство”.

За визначенням, даним у 1993 році Комісією Європейського Союзу: *“Інформаційне суспільство – це суспільство, де діяльність людей здійснюється на основі послуг, що надаються з допомогою інформаційних технологій і технологій зв'язку”*. По суті, інформаційні і телекомунікаційні технології породжують нову революцію. Ця революція основана на інформації, що надає людині нові знання і створює умови формування індустрії інформації. Об'єднуючи в пул інформаційні ресурси, які традиційно розділені й віддалені один від одного на значну відстань, інформаційна інфраструктура відкриває необмежений потенціал для придбання знань, інновацій і творчості. Причому, у документах Ради Європи та Європейського Союзу чітко передбачається, що персональні дані в будь-якому випадку не повинні потрапляти до загальнодоступних інформаційних ресурсів.

Перед лицем справді видатних технологічних досягнень й економічних можливостей, що з'являються, передові країни переглядають свої стратегії і шляхи ведення бізнесу.

Досвід Європейського Союзу наочно переконує, що альтернативи Інформаційному суспільству немає. Ми зобов'язані усвідомити глобальну природу змін, сучасниками і діючими особами яких є, і почати до них пристосовуватися. Від того, яким чином ми будемо реагувати на світові тенденції і можливості, перетворюючи їх в реальність і вигоду, буде залежати як швидко ми вийдемо з кризи і чи скоро будемо жити в європейському Інформаційному суспільстві.

Ми маємо усвідомити, що новий світ вимагає нових підходів у соціальній регуляції. Для нового середовища необхідні нові юридичні механізми, що відповідають природі і розвитку процесів у е-середовищі.

У цьому плані в Україні передбачається прийняття Закону України “Про захист персональних даних” та приєднання до Конвенції № 108 Ради Європи “Про захист осіб у зв'язку з автоматизованою обробкою персональних даних” 1981 року й Додаткового протоколу від 08.11.2001 до неї щодо створення органів нагляду в сфері захисту персональних даних.

2. Питання захисту персональних даних

У різних європейських країнах по-різному складається ситуація в області захисту персональних даних. Загальним є наступне:

- * 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 в сфері захисту персональних даних.

З метою більш тісної співпраці, захисту прав і основних свобод людини, країни-учасниці Ради Європи підписали Конвенцію № 108 “Про захист осіб у зв'язку з автоматизованою обробкою персональних даних” (м. Страсбург, 28.01.81 р.). Конвенція № 108 Ради Європи зобов'язала країн-учасниць здійснити коригування національних законодавств в частині втілення встановлених нею основних принципів захисту персональних даних.

Слід відмітити, що у більшості європейських країн закони щодо захисту персональних даних носять назву – “закон про захист даних”. Це приводить до термінологічної плутанини,

оскільки термін “захист даних” може розглядатися як комплекс захисту всіх видів інформаційних ресурсів. Проте стаття 1 Конвенція № 108 Ради Європи однозначно встановлює, що *“метою Конвенції є забезпечення на території країни-учасника для кожної приватної особи ... його права на недоторканність приватного життя по відношенню до автоматизованої обробки даних, що містять відомості про приватну особу (“захист даних”)”*. Звідси, поняття “захист даних” (date protection) повинно тлумачитися тільки в значенні “захисту відомостей про приватну особу”. Що стосується всієї решти “даних”, то на міжнародному рівні використовують термін “безпека даних” (date security).

Принципи, що визначено у Конвенції, конкретизовані у Директиві 95/46/ЄС Європейського парламенту та Ради Європейського Союзу “Про захист осіб у зв’язку з обробкою персональних даних та вільним обігом цих даних” від 24.10.1995 р., а також у Директиві 97/66/ЄС Європейського парламенту та Ради Європейського Союзу “Про обробку персональних даних та захист прав осіб у телекомунікаційному секторі” від 15.12.1997 р.

У теперішній час усі зазначені акти є міжнародними стандартами, що визначають принципи гармонізації національних законодавств в сфері захисту персональних даних не лише для європейських, а й для інших країн світу.

Рада Європи ухвалила також Додатковий протокол від 08.11.2001 р. до Конвенції про захист осіб у зв’язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних.

Щодо організаційно-правового аспекту – у Раді Європи затверджена посада Комісара по захисту даних, який у відповідності зі статтею 18 Конвенції № 108 Ради Європи обирається Консультативним Комітетом та затверджується Генеральним секретарем Ради Європи. Він є інстанцією, яка функціонує у тісній взаємодії з Уповноваженим по правах людини Ради Європи, але наділений автономністю у вирішенні завдань забезпечення захисту персональних даних.

Виходячи із вищевикладеного, перед Україною виникла проблема привести нормативно-правову і організаційну базу у відповідність до зазначених Конвенцій, Додаткового протоколу до Конвенції № 108 Ради Європи і Директив, що визначають європейське уявлення про права людини та основні свободи в сфері захисту персональних даних в умовах формування Інформаційного суспільства.

Сьогодні в Україні діє більш двох десятків законодавчих актів, які регулюють суспільні відносини, що пов’язані зі збиранням, зберіганням, використанням та поширенням інформації про фізичних осіб, серед них: Конституція України, Закони України “Про інформацію”, “Про нотаріат”, “Про адвокатуру”, “Про зв’язок”, “Про організаційно-правові основи боротьби з організованою злочинністю”, “Про міліцію”, “Про банки і банківську діяльність”, “Основи законодавства України про охорону здоров’я” та ін.

Визначення того, що складає інформацію про особу, дано в статті 23 Закону України “Про інформацію”: *“це сукупність документованих або публічно оголошених відомостей про особу”*. В частині 1 статті 23 Закону дається вичерпний перелік відомостей, які законодавець відносить до “даних про особу (персональних даних) – національність, освіта, сімейний стан, віросповідання, стан здоров’я, а також адреса, дата і місце народження”.

Зрозуміло, що цей перелік не є повним і не охоплює всі відомості про осіб, на які міг би розповсюджуватися правовий режим захисту, що визначений в частині 4 статті 23 Закону України “Про інформацію”. І це підтверджується тим, що в окремих нормах інших законів вищезазначений перелік доповнюється.

В статті 9 Закону України “Про адвокатуру” дається визначення предмету адвокатської таємниці: *“питання, по яких громадянин або юридична особа звернулися до адвоката, суть консультацій, порад, роз’яснень і інших відомостей, отриманих адвокатом при виконанні своїх професійних обов’язків”*. Громадяни звертаються до адвоката з питань, які торкаються їх особисто, і повідомляють йому відомості про себе, а суть консультацій, порад, роз’яснень ад-

воката, у свою чергу, також освітлює особисте життя громадян, тобто йдеться про відомості, які можуть бути віднесені до персональних даних.

В частині 2 статті 14¹ КПК України до даних про особу законодавець відносить набагато ширше коло відомостей: *“особисте життя громадян, таємниця листування, телефонних переговорів і телеграфних повідомлень охороняється законом”*.

Щодо паспортних даних до відомостей персонального змісту, згідно державного стандарту України ДСТУ 3389-96, віднесено: *“фото громадянина, ідентифікаційний номер, прізвище, ім'я та по батькові, стать, місце і дата народження, особистий підпис, місце проживання (прописка), відношення до військової служби, група крові, родинний стан і дані про дітей”*.

Відповідно до статті 9 Закону України “Про оперативно-розшукову діяльність” під захист закону підлягають не просто відомості про особисте життя людини, але і відомості, які торкаються його *“честі і гідності”*.

Цей перелік можна продовжувати й далі.

Із зазначеного можна зробити загальний висновок про те, що в статі 23 Закону України “Про інформацію” законодавець недостатньо чітко дав визначення даних про особу, тобто персональних даних, хоча це поняття несе гносеологічне навантаження: саме на його базі повинні формуватися гіпотези та диспозиції норм, що регулюють суспільні відносини у зв'язку із захистом тих або інших персональних даних.

Теорія і практика інших країн виробила достатньо загальне визначення поняття персональних даних. В статті 2 Конвенції № 108 Ради Європи “Про захист осіб у зв'язку з автоматизованою обробкою персональних даних” наступне визначення персональних даних: *“персональні дані” означають будь-яку інформацію, яка стосується конкретно визначеної особи або особи, що може бути конкретно визначеною (“суб'єкт даних”)*. Рекомендації Ради Європи відзначають, що особа не повинна розглядатися як “ідентифікована”, якщо ідентифікація вимагає непомірних витрат часу, засобів та сил.

Відповідно до статті 2 проекту Закону, **персональні дані – це окремі відомості про фізичну особу чи сукупність таких відомостей, що ідентифікована чи може бути ідентифікованою** (Примітка: тут та далі підкреслення та виділення автора роботи).

Ідентифікованою вважається фізична особа, особистість якої може визначатися прямо чи побічно, зокрема, через ідентифікаційний номер чи через кілька специфічних елементів фізичного, фізіологічного, психічного, економічного, культурного чи соціального ототожнення. Під відомостями розуміється інформація, що має достовірний зміст. Останнє важливо з погляду не допущення обробки випадкових, у тому числі, і анонімних даних.

Зазначене визначення дозволяє надати правову “парасольку” захисту практично для будь-яких персональних даних і однозначно встановити режим захисту, що надає можливість усунути деякі суперечності сучасного законодавства. Наприклад, в Законі України “Про запобігання захворювань СНІДом і соціальний захист населення” інформація про зараження вірусом імунодефіциту людини або про захворювання оголошується службовою таємницею. В той же час відповідно до статті 40 “Основ законодавства України про охорону здоров'я” така інформація віднесена до лікарської таємниці. Правові наслідки розголошення службової таємниці і лікарської таємниці різні. Порядок віднесення інформації і до лікарської таємниці, і до службової таємниці чітко не визначений.

Входження до Ради Європи викликає необхідність урахування системи цінностей, яка панує в цьому співтоваристві.

Найважливішою із задач сьогодення має стати обґрунтоване визначення пріоритетів зовнішньої політики в розвитку відносин з Радою Європи і приєднання до Конвенції № 108 “Про захист осіб у зв'язку з автоматизованою обробкою персональних даних”. Останнє важливо для України виходячи з того, наскільки:

* широко і масштабно буде проводитися в державі автоматизована обробка персональних даних з різною метою – фінансовою (банки, страхові товариства, фонди), правоохорон-

ною, соціальною (охорона здоров'я, соціальна допомога малозабезпеченим, пенсійне забезпечення) тощо;

* реальна загроза нанесення збитку особі в результаті несанкціонованого використання або несанкціонованої модифікації персональних даних.

Ці обставини актуальні для нашого суспільства вже зараз. Так, наприклад, в даний час функціонує Державний реєстр фізичних осіб – платників податків і інших обов'язкових платежів. Можна припустити, який інтерес виявляється до змісту подібних реєстрів, іноді без законних на те підстав. При цьому існує цілком реальна загроза несанкціонованої зміни даних в реєстрі, реалізація якої може завдати конкретній особі серйозних матеріальних збитків у вигляді неправильно нарахованих податків і штрафів, позначитися на здоров'я.

Вказане повною мірою торкається і інших масштабних проєктів – єдиної системи обробки даних у митній службі, електронного депозитарію цінних паперів, єдиної паспортної системи тощо. А участь України в міжнародному процесі обміну інформацією, в різних міжнародних проєктах, заснованих на використанні інформаційно-комп'ютерних технологій (Партнерство задля миру, банківські технології, ІНТЕРПОЛ і т.п.), об'єктивно вимагає забезпечення захисту даних, у тому числі і персональних, за їх автоматизованої обробки і поширення.

Немає необхідності нагадувати про те, що на всіляких базарах і ринках вже “процвітає” торгівля CD-ROMами, що містять персональні дані, отримані часто далеко не законним шляхом. Для будь-якого бізнесу (не кажучи про квартирні крадіжки тощо) персональні дані – зручне, а зараз і необхідне доповнення у всьому тому, що надається через Інтернет. На Заході вже функціонують цілі фірми, що спеціалізуються на зборі і продажу адресних списків персональних даних, які коштують чималі гроші.

На своєму життєвому шляху ми ненавмисно залишаємо сліди інформації про себе, а за нами слідують “пилососи-комп'ютери”, які підбирають, класифікують і зберігають персональні дані в базах даних для подальшого використання. Придбання будь-яких товарів, користування послугами служб прокату, оплата рахунків кредитними картками змушує надавати персональні дані. Кожного разу, підключаючись до мережі і відвідуючи Веб-сайти, ми мимоволі залишаємо свої інформаційно-електронні сліди. Те, про що ми розмовляємо з лікарем, які ліки нам прописують, може перешкодити отримати роботу. Репутація може постраждати і від власної необережності при розмові по телефону. Реєстрація виборця, оплата штрафу, податкова декларація, підписка на газету, відправка листа і багато що інше — все може служити предметом, за допомогою якого поповнюється архів відомостей про нас у невідомій нам базі персональних даних.

Таким чином, навіть приблизна оцінка ситуації із захистом персональних даних вимагає активності в політичному вирішенні питання про приєднання України до Конвенції № 108 Ради Європи “Про захист осіб в зв'язку з автоматизованою обробкою персональних даних” 1981 року і приведення всієї законодавчої бази у відповідність з її положеннями.

3. Проєкт Закону України “Про захист персональних даних”

Початок розробки проєкту базового (рамкового) Закону України “Про захист персональних даних” було покладено в 1996 р. Практична необхідність розробки закону обґрунтовується наступним:

* стан нормативно-правової бази України не в повній мірі забезпечує захист прав людини у сфері персональних даних. Нормативна база має слабку кореляцію з вимогами статей 3, 23, 31, 32, 34 Конституції України і міжнародних стандартів;

* діючі у цей час більш як 20 законів України, пов'язані зі збором, використанням і передачею інформації про фізичних осіб, не мають однозначного, єдиного визначення - що це за інформація. Визначення має бути вихідним і нести гносеологічне навантаження: саме на

його основі повинні формуватися гіпотези норм, регулюючих відносини щодо захисту персональних даних.

Перша версія законопроекту була підготовлена у 1998 року. В цей же час була видана книжка під однойменною назвою. По суті, в ній викладена відповідна концепція.

Законопроект 4 рази розглядався в різноманітних міністерствах і комітетах: Мінекономіці, Мінфіні, Мінюсті, в МВС, СБУ, Комітеті з питань державних секретів, Податковій адміністрації, в Раді національної безпеки і оборони, Уповноваженим ВР України з прав людини. Було висловлено понад 160 зауважень і пропозицій.

На кінець 1999 р. законопроект погодили всі відомства і 27 грудня 1999 р. він був спрямований до Кабінету Міністрів України. Після внесення правок профільними відділами Кабміну, законопроект в 5-ий раз був розісланий на погодження до тих же органів влади, а також до Міністерства освіти і науки, Міністерства закордонних справ. Було отримано понад 50 зауважень, після врахування яких керівники всіх відомств затвердили останню версію законопроекту і 20 грудня 2000 року він був переданий до Кабінету Міністрів України.

У січні місяці 2003 року законопроект зареєстрований у Верховній Раді України (реєстраційний № 2618 від 10.01.2003 р.). Ініціатори реєстрації проекту Закону України “Про захист персональних даних” – Народні депутати України Родіонов М.К., Ніколаєнко С.М., Юхновський І.Р., Толочко П.П., Ситник К.М.

На цей час законопроект розглянутий у першому читанні та прийнятий за основу (Постанова Верховної Ради України від 15.05.2003 р. № 784-IV).

Ідейна суть законопроекту формулювалася на базі норм міжнародного права, які визначені у головному документі – Конвенції № 108 Рада Європи “Про захист осіб у зв’язку з автоматизованою обробкою персональних даних” 1981 р.

Конвенція № 108 Ради Європи виходить з того, що права й інтереси особи в умовах застосування новітніх інформаційних технологій, комп’ютерних і телекомунікаційних засобів можуть бути порушені в результаті несанкціонованого збору, обробки, зберігання і розповсюдження персональних даних їй на шкоду, завдяки цьому звівши нанівець її природні, життєві права, що є основою свободи, загальної справедливості і миру. Означені права слід захищати владою закону.

Як зазначалося, принципи Конвенції № 108 Ради Європи уточнюються і конкретизуються в Директиві 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 жовтня 1995 р. Директива була підготована в 1994 році групою фахівців під керівництвом члена Європейської Комісії Мартина Бангемана (на той час Комісар РЄ по захисту (персональних) даних) на замовлення Європейської Ради і на основі аналізу розвитку ринкових відносин. Звіт групи М.Бангемана є, так мовити, маніфестом побудови Інформаційного суспільства і має назву: “Європа і глобальне Інформаційне суспільство. Рекомендації Європейській Раді”. Згідно Директиви 95/46/ЄС зміст європейської моделі захисту персональних даних можна визначити як “забезпечення єдиними механізмами виконання”.

Європейський Союз прагне до того, щоб суб’єкти персональних даних мали чітко визначені права і реальну можливість звернутися до посадової особи або органу, що зобов’язаний вжити дії для їхнього захисту. Кожній країні, що є учасником Євросоюзу, рекомендовано створити інститут Уповноваженого по захисту персональних даних. Країни інших континентів, з якими співробітничать держави-учасники ЄС, будуть мати аналогічний, уніфікований рівень контролю за діяльністю у сфері захисту персональних даних.

Із метою поглиблення галузевого принципу захисту персональних даних, проголошеного Конвенцією № 108 Ради Європи та Директивою 95/46/ЄС в 1997 році була затверджена Директива 97/66/ЄС Європарламенту і Ради Євросоюзу від 15 грудня 1997 р. “Про обробку персональних даних і захист прав людини в телекомунікаційному секторі”. Вона

доповнює і конкретизує правила обробки даних в операційних системах, що збираються операторами під час надання телекомунікаційних послуг.

В Україні побутує думка, що проблема захисту персональних даних у наш час не актуальна у зв'язку з нерозвиненістю громадянського суспільства, наявності менталітету примата держави і низьким рівнем інформатизації. Парадоксальність ситуації у тому, що потреба в захисті особистого і родинного життя громадян об'єктивно існує, але вона суспільством серйозно не сприймається.

Є три основні причини для руху в напрямку створення законодавчої бази щодо захисту персональних даних, із яких виходять європейські та інші країни:

- * усунення несправедливості, допущеної в минулому;
- * розвиток е-комерції (е-торгівлі);
- * гармонізація національних законодавств відповідно до норм європейського, континентального права.

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

- * великою активністю в формуванні баз даних (соціального, фінансового, маркетингового, медичного, екологічного, адміністративного, правоохоронного та ін. змісту);
- * розвитком і розповсюдженням автоматизованих засобів і засобів збору, обробки, зберігання і поширення інформації;
- * використанням інформаційних технологій кримінальними структурами, що підривають зусилля по розвитку і зміцненню демократичної, правової держави.

Потреба приведення норм права вітчизняного законодавства до вимог міжнародних стандартів є і в аспекті участі України в міжнародному процесі обміну інформацією, в міжнародних проектах, що засновані на використанні нових інформаційних технологій у різних секторах економічної, соціальної і науково-технічної діяльності.

Метою Закону “Про захист персональних даних” є усунення недоліків нормативно-правового забезпечення в Україні по захисту персональних даних і приведення його у відповідність з положеннями вказаних Конвенцій і Директив, які віддзеркалюють європейське уявлення про права і свободи людини у сфері захисту персональних даних.

Закон базується на 3 моментах, які передбачають:

- * пріоритет інтересів і права власності людини на персональні дані;
- * забезпечення балансу прав особи, суспільства і держави;
- * сприяння умовам розвитку процесів у е-середовищі.

Захист осіб передбачається як для автоматизованої обробки персональних даних, так і для систем ручної обробки, в яких відбувається маніпулювання персональною інформацією, що реалізує індивідуальні ресурси даних, мови і зображень.

Перший розділ Закону визначає сферу його чинності, вказує на суб'єкти і об'єкти захисту персональних даних, вводить загальні вимоги відносно дій з персональними даними, засерегіає джерела персональних даних.

Другий розділ вводить право власності людини на свої персональні дані і визначає обсяг повноважень власника персональних даних.

В третьому розділі надається визначення права на використання персональних даних іншими суб'єктами, підстави виникнення їхнього права на використання стосовно збору, накопичення, зберігання і розповсюдження персональних даних.

Четвертий розділ визначає режим доступу до персональних даних, права й обов'язки суб'єктів по запиту, відстрочці, оскарженню і відмові в задоволенні доступу, а також додаткові права володільця персональних даних.

В п'ятому розділі надані умови внесення змін і доповнень у персональні дані.

Шостий розділ упорядковує організацію захисту персональних даних, а також визначає обмеження дій окремих статей.

Сьомий розділ визначає види відповідальності й умови відшкодування матеріальних і моральних збитків, порядок оскарження протиправних дій.

Восьмий розділ встановлює принципи міжнародного співробітництва і взаємодії України з іншими державами та підтримки громадян України, які проживають за кордоном.

Прикінцеві положення встановлюють час набуття чинності закону, а також вносять зміни до законодавства країни

Введення в дію Закону та інструментів його реалізації дає можливість позбавитися від соціальних наслідків і економічних втрат для України та досягти таких результатів як:

- ліквідувати існуючі і потенційні втрати від неупорядкованості суспільних інформаційних відносин при збиранні, зберіганні, використанні та поширенні персональних даних, як всередині країни, так і при транскордонному їх поширенні;
- створити умови збалансованого правового упорядкування суспільних інформаційних відносин людини, суспільства і держави щодо захисту персональних даних;
- сприяти розвитку внутрішнього та зовнішнього ринків інформаційних ресурсів, інформаційних продуктів, інформаційних технологій і інформаційних послуг з урахуванням захисту персональних даних в умовах розвитку комп'ютерно-інформаційних технологій та телекомунікаційних мереж;
- сприяти розвитку та зміцненню приватної власності на інформаційні ресурси, інформаційні продукти та інформаційні технології;
- розширити можливості для боротьби з комп'ютерною злочинністю та недобросовісною конкуренцією, підтримки забезпечення суверенітету, економічного добробуту та національної безпеки держави, у контексті приватної власності;
- забезпечити умови рівноправного та взаємовигідного міжнародного співробітництва у сфері захисту персональних даних;
- сприяти поглибленню в суспільстві морально-етичності, духовності, культури і гуманності в умовах розвитку процесів інформатизації та переходу до Інформаційного суспільства.

Стосовно реалізації норм права, які визначені у законі, тобто – правових інструментів забезпечення захисту персональних даних, можна зазначити наступне.

Виходячи з загальної практики країн Європи, вимог європейських стандартів, зокрема, статті 13 Конвенції № 108 Ради Європи, яка зобов'язує держави-члени Конвенції створювати Уповноважені органи нагляду за захистом (обробкою) персональних даних, перелік головних нормативно-правових документів, які першочергово необхідні для функціонування системи захисту персональних даних в Україні, повинен передбачати документи щодо:

* функціонування спеціально Уповноваженого органу нагляду з питань захисту персональних даних в Україні. Крім положення про Уповноважений орган слід розробити його структуру, здійснити розрахунок матеріально-технічного та фінансового забезпечення;

* порядку надання дозволу на здійснення діяльності в сфері захисту персональних даних. Зазначений порядок є найважливішим привентивно-регулятивним засобом захисту від несанкціонованого збору, обробки, реєстрації, накопичення, збереження та поширення персональних даних. Процес регулювання діяльності передбачає визначення мети дій з персональними даними, оцінку стану техніко-технологічної бази та заходів захисту персональних даних, встановлення рівня правової та професійної підготовки претендентів на право займатися діяльністю по наданню послуг у сфері персональних даних тощо;

* реєстрації баз персональних даних, систем автоматизованої обробки персональних даних і систем обробки картотек персональних даних. Порядок, який визначається цим документом, також є одним із головних привентивно-регулятивних засобів захисту від несанк-

ціонованого збору, обробки, реєстрації, збереження і поширення персональних даних. Процес регулювання діяльності передбачає визначення мети формування баз персональних даних, оцінку стану техніко-технологічних можливостей захисту персональних даних тощо;

* сертифікації засобів технічного захисту персональних даних. Враховуючи те, що кураторство питань технічного захисту інформації покладено на спеціалізовану структуру державної влади (СБУ України), рішення щодо створення проектів зазначених у цьому пункті документів повинно бути прийнято окремо, на рівні Кабінету Міністрів України.

Разом з тим, повноцінний захист персональних даних у різних організаціях (фірмах) тощо, а також робота Уповноваженого органу неможлива без ряду інших підзаконних нормативно-правових актів, що покликані деталізувати окремі напрямки захисту персональних даних. Загальний аналіз та оцінка практики європейських країн дозволяє визначити перелік основних документів для створення системи захисту персональних даних та діяльності Уповноваженого органу нагляду в Україні. Це не менше як 20 документів. В цьому випадку з'являються реальні можливості нагляду і контролю захисту персональних даних.

Аналіз і попередні розрахунки свідчать, що витрати по створенню і функціонуванню Уповноваженого органу складатимуть приблизно 116,8 тис. дол. З урахуванням максимальної вартості системи управління базою даних загальні витрати по створенню та функціонуванню Уповноваженого органу складатимуть приблизно 1,616 млн. дол.

При наданні Уповноваженому органу права на збір за надання послуг (50% від суми пропонується направляти до державного бюджету), кількості організацій, що обробляють персональні дані в різних базах даних (приблизно 32.000 організацій, підприємств, фірм) і представлених в роботі розцінок можна очікувати вихід Уповноваженого органу з питань захисту персональних даних на повну самооплатність через 4 – 6 років.

Отже, проект Закону “Про захист персональних даних” та правовий механізм його реалізації є самоокупними і дозволяють компенсувати витрати бюджету від їх впровадження, зумовити доходи до державного бюджету, а також унеможливити застосування нетарифних обмежень експорту послуг з України.

Використана література

1. Конституція України. Прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 року. – К.: Інформаційно-видавниче агентство “ІВА”, 1996.
2. Конвенція № 108 Ради Європи “Про захист осіб у зв'язку з автоматизованою обробкою персональних даних” Страсбург, 28.01.1981 р. Серія “Європейські угоди”, № 108. //conventions.coe.int/treaty/en/Treaties/Html/108.htm. Офіційний переклад 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 засвідчено МЗС України від 01.07.2002 р.
4. 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.
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. Брижко В.М. Правовий механізм захисту персональних даних: Монографія. / За заг. ред. доктора економічних наук, професора, заслуженого діяча науки і техніки України М.Я. Швеца та доктора юридичних наук, професора, заслуженого юриста України Р.А.Калюжного – К.: “Парламентське видавництво”, 2003. – 120 с.
7. Брыжко В.М., Цимбалюк В.С. и др. e-будущее и информационное право / Под ред. д.ю.н., профессора Р.А.Калюжного и д.э.н., профессора Н.Я.Швеца. – К., “Интеграл”, 2002. – 263 с.