УДК 351.9; 621.321

ПРОБЛЕМНІ ПИТАННЯ ПРАВОВОГО РЕГУЛЮВАННЯ ПОВНОВАЖЕНЬ ДЕРЖСПЕЦЗВ'ЯЗКУ УКРАЇНИ ІЗ ЗАХИСТУ ІНФОРМАЦІЇ ПРО ПЕРСОНАЛЬНІ ДАНІ

Михайло Косіцин, Едуард Плешко
Управління Держспецзв'язку в Одеській області

Анотація: **У системі національного права України досі відсутні єдина правова термінологія та понятійний апарат інформації про особу. Безпосередньо перед Держспецзв'язком постають питання термінового удосконалення нормативно-правової бази з організації власної діяльності та визначення невирішених питань серед її пріоритетів, упорядкування структури підрозділів державного контролю з метою забезпечення реального захисту персональних даних.**
Summary: **In the national law of Ukraine has not only legal terminology and conceptual apparatus of information about a person. Immediately before the State Special communication arises for urgent improvement of the legal framework to organize their own activities and identify outstanding issues among its priorities, streamlining the structure of departments of state control in order to ensure real protection of personal data.**
Ключові слова: **Захист персональних даних; удосконалення нормативно-правової бази ТЗІ.**

І ВСТУП

Права людини у сфері інформації визнаються не менш важливими ніж інтереси держави, які отримали правовий режим охорони. Україна не залишається осторонь цього процесу.

Україною будується власна система інформаційного права, у тому числі щодо технічного захисту інформації, однак, майже нещодавно прийняті закони, не встигають за бурхливим науково-технічним прогресом. Вже стають проблемними та потребують суттєвих змін питання правового регулювання щодо надання органами державної влади та місцевого самоврядування інформаційних послуг юридичним та фізичним особам з використанням мережі Інтернет, запровадження електронного документообігу та електронного цифрового підпису, дистанційного навчання, телемедицини, електронних платіжних систем, електронного бізнесу, електронних бірж, аукціонів і депозитаріїв [1].

Створення Держспецзв'язку України, як окремого спеціально уповноваженого центрального органу виконавчої влади призначеного, серед іншого, забезпечити технічний захист інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом [2], фактично співпало з оформленням нової концепції побудови інформаційного простору держави, що знайшло відображення у законі «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» [3].

ІІ ОСНОВНА ЧАСТИНА

Сьогодні інформація все більше стає найвагомішим ресурсом сучасності, а філософська категорія інформації стрімко отримує технічний та правовий виміри.

Значно зросли можливості збирання, обробки, зберігання, передачі інформації, доступу до неї. На рух інформаційних потоків вже практично не впливає наявність кордонів, а інформаційна безпека посідає важливе місце у безпековому секторі кожної держави.

На листопад 2010 року сплановано прийняття, замість існуючої більше десяти років, нової безпекової доктрини НАТО. У доповіді, підготовленій для обговорення групою міжнародних експертів, серед основних загроз одразу після тероризму визначено кібернетичні атаки та зроблено наголос на необхідності захисту інформаційних ресурсів. Визнання даного факту не тільки окремими державами, а як колективне, тим паче у нашому міжнародному регіоні, має особливе значення для світового розвитку.

Зазначимо, що останнім часом, саме в інформаційній сфері національна нормотворчість найбільш активно стикається з глобалізацією та інтернаціоналізацією інформаційного права, необхідністю постійного розширення об'єкта інформаційно-правового регулювання та потреби в адаптації і вдосконалені внутрішніх інформаційно-правових норм.

Дослідники відмічають світові суперечливості розвитку інформаційного законодавства. Так, азійські країни, наприклад, Китай та Корея завжди характеризувалися суворими адміністративними регуляторами тоталітарного спрямування на противагу західним країнам, де існували ліберальні закони щодо інформаційного простору. Але ж, нині в Азії відбувається демократизація доступу до інформації, а в Америці навпаки - регуляція інформаційних відносин стає більш жорсткою.

При цьому ніким не заперечується необхідність обмеження на підставі закону доступу до інформації окремих видів та її технічного захисту, мінімізації негативного інформаційного впливу та негативних наслідків функціонування інформаційно-комунікаційних технологій, недопущення незаконного розповсюдження, використання і порушення цілісності інформації.

Доречним буде нагадати, що Конституційний Суд України в рішенні у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України „Про інформацію" та статті 12 Закону України „Про прокуратуру" від 30 жовтня 1997 року №5-зп (справа К.Г. Устименка №18/203-97) визнав недосконаліть вітчизняного законодавства по регулюванню інформаційних правовідносин, і невідповідність його європейським стандартам в частині захисту персональних даних [4].

Більш того, ще 29 серпня 2005 року Україною підписана, але досі не ратифікована Конвенція №108 (1981 року) Ради Європи "Про захист осіб у зв'язку з автоматизованою обробкою персональних даних", яка визначає персональні дані як будь-яку інформацію про фізичну особу, що ідентифікована або може бути ідентифікованою. Саме ця Конвенція є визнаним міжнародним документом про взаємні права та обов'язки і містить загальноєвропейські норми (стандарти), що створюють умови регулювання суспільних відносин у сфері захисту персональних даних [5].

Євросоюз розглядає ратифікацію Україною зазначеної Конвенції як важливу умову для введення режиму безвізових поїздок громадян нашої країни, що наповнить іншим змістом їх право на вільне пересування та можливість його реалізації. Тобто, не тільки визнання загальноприйнятих норм в інформаційній сфері, а й їх безпосереднє застосування стає вимогою часу.

На початку червня поточного року під головуванням Віктора Януковича відбулося засідання Ради національної безпеки і оборони України, на якому під час обговорення питання стратегічної ваги – проекту Закону про засади внутрішньої і зовнішньої політики, Президент України наголосив, що ми чітко визначаємо найвищу пріоритетність європейського стратегічного курсу України. Це – основний вектор нашого розвитку, що визначає зміст суспільних перетворень і основну спрямованість нашої зовнішньої та внутрішньої політики [6].

Держспецзв'язок України, як орган, уповноважений брати участь у формуванні та реалізації державної політики у сфері технічного захисту інформації, повинен мати належне правове поле для своєї діяльності.

З цією метою, серед інших заходів можливо запропонувати першочергові кроки у вигляді змін до ст. 23 Закону України «Про інформацію» щодо обов'язковості умов технічного захисту інформації про особу при її обробці автоматизованою системою, а до Кодексу України про адміністративні правопорушення внести статтю «Порушення законодавства про захист інформації в інформаційно-телекомунікаційних системах», визначивши за такі порушення відповідальність власників інформації, у володінні яких знаходяться ІТС, що містять інформацію про особу (персональні дані).

Зазначимо, що увагу науковців привертає відсутність у системі національного права України єдиної правової термінології та понятійного апарату інформації про особу. Наприклад, Закон України "Про інформацію" визначає під інформацією про особу сукупність документованих або публічно оголошених відомостей про особу [7].

Водночас закон окремо виділяє основні (персональні) дані про особу - національність, освіту, сімейний стан, релігійність, стан здоров'я, а також адресу, дату і місце народження. Більш широке тлумачення персональних даних міститься у Законі України "Про Всеукраїнський перепис населення", який відносить до них склад та родинні стосунки членів домогосподарства; стать; вік; дату і місце народження; сімейний стан; етнічне походження; мовні ознаки; громадянство; освіту; джерела засобів існування; зайнятість; міграційну активність; житлові умови [8].

Новий Закон України «Про захист персональних даних», що набирає чинності з 1 січня 2011 року, визначає персональні дані як відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [9].

Немає в законодавстві й узгодженості щодо режиму доступу до інформації про особу. Стаття 32 Конституції України говорить про заборону збирання, зберігання, використання та поширення тільки конфіденційної інформації про особу [10]. Закон України «Про захист персональних даних» зазначає, що доступ до персональних даних третій особі не надається, якщо зазначена особа відмовляється взяти на себе зобов'язання щодо забезпечення виконання вимог цього Закону або неспроможна їх забезпечити, а Закон України "Про інформацію" забороняє доступ сторонніх осіб до будь-яких відомостей про особу.

Можна погодитися з деякими дослідниками, що останнє виглядає більш доцільним, оскільки у різних конкретних ситуаціях будь-яка інформація про особу може мати конфіденційний характер. Такий стан речей деякою мірою виправдовується тим, що інформація як предмет правового регулювання не належить до традиційних правових категорій і законодавцям необхідно розробляти базові поняття в цій сфері. У зв'язку з

цим існує нагальна потреба усунути вказані неузгодженості в законодавстві та юридично закріпити в одному законі правовий режим інформації про особу [11].

Підтримуємо пропозицію, що за основу слід взяти стандарти Ради Європи, згідно з якими інформація про особу за своїм характером належить до відомостей з обмеженим доступом, при одночасному виокремленні особливих категорій даних, які мають підвищений рівень конфіденційності: расову приналежність, політичні або релігійні чи інші переконання, стан здоров'я, відомості про статеве життя тощо.

Визначення правових підстав режиму захисту інформації тягне за собою необхідність удосконалення окремих діючих правових норм, що безпосередньо регулюють діяльність Держспецзв'язку України.

Так, передбачена законодавством для службових осіб Держспецзв'язку можливість складання лише протоколів, значно погіршує оперативність усунення виявлених недоліків та фактично надає змогу порушникам тривалий час порушувати права громадян та інтереси держави, що охороняються законом. Тому назріла необхідність внести зміни до ст. 17 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України», передбачивши можливість для належного реагування на виявленні адміністративні порушення та недотримання вимог щодо технічних умов експлуатації ІТС вносити попередження про необхідність усунення порушень або припису про заборону експлуатації ІТС.

Постає питання про врахування вищенаведеного та внесення змін до Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених Постановою Кабінету Міністрів України від 29.03.2006 №373 [12], щодо розкриття терміну «конфіденційна інформація про особу» з урахуванням конкретних відомостей, які містять конфіденційну інформацію, та змін, які б регулювали відносини державних органів влади, місцевих органів виконавчої влади, органів місцевого самоврядування, судів, органів прокуратури, органів військового управління, територіальних органів центральних органів виконавчої влади, інших державних органів, підприємств, установ та організацій, юридичних, фізичних осіб, які пов'язані з обробкою конфіденційної інформації про особу з використанням ІТС.

В сучасних базах даних автоматизованих систем вже міститься широке коло відомостей, включаючи і відомості про особисте та сімейне життя громадян - від облікових даних - національності, освіти, сімейного стану, релігійності, адреси, місця і дати народження до інформації про банківські рахунки, відомості медичного характеру, інформація про арешти, членство в політичних організаціях, відомості пов'язані з комерційною діяльністю і т. ін. [13].

Нажаль, навіть державні органи, не завжди поспішають виконувати вимоги щодо технічного захисту інформації при застосуванні нових технологій з наступною ідентифікацією персональних даних. Наприклад, широкого суспільного резонансу набуло використання ДАІ МВС України пристрою автоматичної фіксації порушень правил дорожнього руху «Візир», який процедур державної експертизи або сертифікації у сфері захисту інформації не проходив та офіційного підтвердження про неможливість довільної зміни попередньо зафіксованої інформації не мав, а навпаки це дозволяв, що змусило Держспецзв'язку інформувати МВС України про необхідність забезпечення захисту інформації (вих. №8/1 від 13.11.2008р.).

Цікавим є недавній експеримент британського дослідника Марка Гассона (Mark Gasson) з університету міста Редінг (University of Reading). На підтвердження визначеної потенційної загрози життю людей, що використовують високотехнологічні медичні пристрої (кардіостимулятори, дефібрилятори и кохлеарні імплантати, що повертають слух глухим, перспективні розробки електронних пристроїв для незрячих та інші), він вшив собі до лівої руки мікрочіп управління, пов'язаний із системою контролю у відповідній клініці. В наступному, чип з персональними даними підвергся впливу комп'ютерного вірусу та не тільки перестав функціонувати за призначенням, а й через безпровідний доступ порушив роботу усіх комп'ютерів клініки.

Під час формування та роботи з інформаційними ресурсами, що розглядаються, обов'язковим повинно стати правове регулювання застосування безпечних інформаційних технологій, за допомогою яких обробляються дані. Більш поширеним засобом державного контролю має бути відповідний атестат Держспецзв'язку, відсутність якого слід визнати, серед іншого, підставою для відповідальності.

До речі, регламентація наказом Голови Держспецзв'язку №100 від 29.05.07р. складання протоколів про адміністративні правопорушення тільки у сфері держтаємниці, без встановлення такого порядку для інших випадків, фактично не забезпечує належного захисту прав та свобод громадян, безпідставно робить їх другорядними [14].

Уваги заслуговує й правовий досвід окремих розвинених країн, що пройшов тривалу апробацію та може бути запозичений із незначною доробкою.

Так, у Великій Британії запроваджено ведення реєстру осіб, які збирають і зберігають персональні дані, а також осіб, які мають комп'ютерні бюро і надають послуги щодо персональних даних.

У Німеччині здійснюється ведення переліку пристроїв і нагляд за застосуванням програм обробки даних, а також встановлено обов'язок будь-яких організацій (більше 5 чоловік), що обробляють дані, призначати уповноваженого організації із захисту персональних даних [15].

ІІІ ВИСНОВКИ

Наведеного достатньо для висновку про те, що в Україні назріла гостра необхідність удосконалення законодавства, яке регулює відносини в інформаційній сфері щодо надійного захисту від протиправного втручання в особисте життя людини.

Безпосередньо перед Держспецзв'язком постають питання термінового удосконалення нормативно-правової бази з організації власної діяльності та визначення висвітлених питань серед її пріоритетів, упорядкування структури підрозділів державного контролю з метою забезпечення реального захисту персональних даних.

За основу удосконалення нормативно-правової бази слід взяти стандарти Ради Європи, згідно з якими інформація про особу за своїм характером належить до відомостей з обмеженим доступом, при одночасному виокремленні особливих категорій даних, які мають підвищений рівень конфіденційності: расову приналежність, політичні або релігійні чи інші переконання, стан здоров'я, відомості про статеве життя тощо.

Література: ***1.*** *Панова І. В. Тенденції розвитку інформаційно-правових норм. Див. Матеріали ІІ міжнародної науково-практичної конференції «Роль та місце ОВС у розбудові демократичної правової держави» // ОДУВС - Одеса – 2010. – С.170.* ***2.*** *Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України // Відомості Верховної Ради України. – 2007. - №12. – Ст.102.* ***3.*** *Про державну службу спеціального зв'язку та захисту інформації: Закон України // Відомості Верховної Ради України. – 2006. - №30. – Ст.258.* ***4.*** *Рішення Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України «Про інформацію» та статті 12 Закону України «Про прокуратуру» від 30 жовтня 1997 року №5-зп (справа К.Г. Устіменка № 18/2003-97) // Вісник Конституційного Суду України. – 1997. - № 2. – С.31-34.* ***5.*** *Конвенція №108 Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних». Страсбург, від28 січня 1981 року: [Електронний ресурс] – Режим доступу: //http://www.evropa.eu.int/ISPO/legal/en/dataprot/direktiv/ direktiv.html.* ***6.*** *Під головуванням Президента України відбулося засідання РНБО: Офіційне інтернет – представництво Президента України. 01.06.2010 10:52. [Електронний ресурс] – Режим доступу: //http://www.president.gov.ua/news/17274.html.* ***7.*** *Про інформацію: Закон України // Відомості Верховної Ради. – 1992. - № 48. – Ст. 650.* ***8.*** *Про Всеукраїнський перепис населення: Закон України // Відомості Верховної Ради. – 2000. - № 51-52. – Ст. 446.* ***9.*** *Про захист персональних даних: Офіційне інтернет – представництво Президента України. 24.06.2010 [Електронний ресурс] – Режим доступу: //http://www.president.gov.ua/documents/11965.html.* ***10.*** *Конституція України: Основний Закон України // Відомості Верховної Ради. – 1996. - № 30. – Ст. 141.* ***11.*** *Омельченко В. І. Проблеми правового захисту інформації про особу: Матеріали ІІ міжнародної науково-практичної конференції «Роль та місце ОВС у розбудові демократичної правової держави» // ОДУВС - Одеса – 2010. – С. 47.* ***12.*** *Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах // Постанова Кабінету Міністрів України // Офіційний Вісник України. 2006 - № 13 – Ст. 878.* ***13.*** *Омельченко В. І. Проблеми правового захисту інформації про особу: Матеріали ІІ міжнародної науково-практичної конференції «Роль та місце ОВС у розбудові демократичної правової держави» // ОДУВС - Одеса – 2010. – С. 48.* ***14.*** *Про затвердження Інструкції про порядок оформлення та складання Державною службою спеціального зв'язку та захисту інформації України матеріалів про адміністративні правопорушення: Наказ Держспецзв'язку від 29.05.2007 №100 // Офіційний Вісник України. 2007. - № 43 – Ст. 1747.* ***15.*** *Брижко В. М. Становлення правової охорони і захисту персональних даних: див. Цимбалюк В. С., Гавловський В. Д., Брижко В. М. та ін. «Основи інформаційного права України» // навчальний посібник за ред. Швеця М. Я., Калюжного Р. А., Мельника П. В. // 2-ге вид. – К.: Знання, 2009. – С. 282-284.*