УДК 327:[316.774:351.862.4]

Анфіса Нашинець-Наумова,
докт. юрид. наук, доцент,
заступник декана з науково-методичної
та навчальної роботи факультету права та міжнародних відносин
Київського університету імені Бориса Грінченка

СВІТОВИЙ ДОСВІД ЗАКОНОДАВЧОЇ РЕГЛАМЕНТАЦІЇ РЕЖИМІВ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

У статті представлені результати світового досвіду законодавчої регламентації режимів конфіденційної інформації. Показана важливість використання цього досвіду для практичної реалізації процесів інформаційного забезпечення в Україні. Аналізуючи міжнародний досвід правового регулювання відносин щодо захисту конфіденційної інформації, автор визначає перспективні напрями подальшого розвитку для України в зазначеній сфері.

Ключові слова: режими конфіденційної інформації, інформаційна безпека, міжнародний досвід, законодавча регламентація.

Постановка проблеми. У процесі становлення інформаційного суспільства в умовах глобалізації, нових викликів і загроз, порушення сталого функціонування інформаційної інфраструктури потребують уточнення напрями розвитку національного законодавства. Нині відбуваються зміни і на міжнародній арені, що вимагають адекватного правового регулювання. Це особливо очевидно на прикладі розвитку Інтернету та використання його все частіше в протиправних цілях.

На основі вивчення міжнародно-правових актів, що стосуються протидії новим викликам і загрозам в інформаційній сфері, а також впливу глобалізації на визначення національної стратегії розвитку інформаційного суспільства обґрунтовується висновок про необхідність подальшої імплементації положень міжнародних правових актів, що стосуються, зокрема, забезпечення доступу до публічної і судової інформації, боротьби з корупцією, тероризмом і екстремізмом, кіберзлочинністю, і гармонізації законодавства держав.

Аналіз останніх досліджень і публікацій з цієї теми. Необхідно зазначити, що в цьому напрямі здійснювались наукові розвідки таких учених: Б.В. Авер'янова, А.І. Арістової, О.А. Баранова, К.І. Бєлякова, В.М. Брижка, П.В. Діхтієвського, Р.А. Калюжного, В.К. Колпакова, Б.А. Кормича, В.І. Курила, В.А. Ліпкана, А.І. Марущака, А.М. Новицького, Н.Р. Нижник, В.Ф. Опришка, В.Г. Пилипчука, М.Я. Швеця, В.С. Цимбалюка та інших.

Метою статті є узагальнення світового досвіду законодавчої регламентації режимів конфіденційної інформації та обґрунтування концептуальних положень щодо системи правового регулювання інформації з обмеженим доступом в Україні.

Виклад основного матеріалу. Натепер інформація стала загальнодоступною, стрімкий розвиток глобальної інформаційної мережі забезпечив можливість її передачі на практично необмежені відстані в досить великих обсягах, а також у найкоротші терміни, що дало змогу кожній фізичній і юридичній особі отримати доступ до різних інформаційних ресурсів.

Нині в Україні, як і в усьому світі, активно продовжує розвиватися інформаційне суспільство. Активно впроваджуються нові інформаційні технології, електронний документообіг, створюється електронний уряд. Своєю чергою це призводить до значного збільшення кількості процесів обігу інформації та обміну інформаційними ресурсами між державними органами, суб'єктами господарювання, фізичними особами. При цьому правова неврегульованість процесів обміну інформацією часто призводить до того, що відомості, які призначені для обмеженого доступу, стають загальнодоступними. Це завдає серйозної шкоди не тільки окремим громадянам і суб'єктам господарювання, а й системі безпеки всієї держави [1, с. 240].

Подібна неврегульованість процесів обміну інформацією характерна для більшості розвинених держав. Дослідження практики світового досвіду законодавчої регламентації режимів конфіденційної інформації свідчить, що її проблеми перебувають у національному правовому полі. Для прикладу пропонується звернутися до дослідження інформаційного законодавства різних країн, але вже в контексті законодавчої регламентації режимів конфіденційної інформації.

Так, у Сполученому Королівстві суди звузили уявлення про персональні дані, підкресливши, що такі дані мають бути значною мірою біографічними і стосуватися конкретної фізичної особи, а не будь-якої людини, угоди або заходу [2].

У Франції Національна комісія з питань обробки даних і свобод приймає запобіжні заходи до забезпечення виконання Закону про обробку даних, файлів даних. Комісія видала посібник про законну обробку персональних даних, у якому зобов'язує контролерів даних виконувати вимоги щодо надання інформації, інструкції із забезпечення безпеки персональних даних, а також подеколи отримувати попередню санкцію Комісії на обробку даних [3, с. 45].

Правові відносини щодо захисту конфіденційної інформації в Сполучених Штатах Америки регулює Верховний суд США, який визнав право на конфіденційність, спираючись на Конституцію, не зважаючи на те, що подібного чітко вираженого конституційного права немає. Положення про захист конфіденційності містяться в конституціях багатьох штатів США. Лише один американський штат – Каліфорнія – розширив сферу захисту даних і поряд із державним втручанням зробив її обов'язком приватного сектору [4, с. 40].

У Німеччині персональні дані отримуються безпосередньо від суб'єкта даних, крім тих випадків, коли дані необхідні відповідно до законодавства в чинних комерційних цілях або коли для отримання даних безпосередньо від суб'єкта потрібні невиправдано великі зусилля, немає вказівок на те, що інтереси суб'єкта даних будуть цим порушені. Крім того, в Законі про захист даних приділяється особлива увага розробленню систем захисту даних, спрямованих на мінімізацію обсягів оброблюваних персональних даних, наприклад шляхом надання суб'єкту даних анонімного статусу або використання псевдонімів [5].

У Канаді Хартія прав і свобод [6] містить право «на захист від необґрунтованих обшуків і накладення арешту на майно», розширене судами до права на захист «розумної надії фізичної особи на недоторканність приватного життя». Завдяки недавньому прецедентному рішенню Апеляційного суду в Онтаріо до загального права введено делікт вторгнення в приватне життя («порушення усамітнення»). Канадські закони не обмежують міжнародну передачу персональних даних [7], але відповідальність за будь-яку передачу несе сторона, яка розкриває (передає) дані.

У Бразилії спеціальні закони про захист даних ще не прийняті, хоча в її Конституції [8] закріплені основні права на конфіденційність і таємницю листування. У Цивільному кодексі передбачено також, що фізична особа може просити допомоги у зв'язку з будь-якою загрозою її особистих прав, а також те, що приватне життя фізичної особи є недоторканним. Широкий захист надає також Кодекс захисту прав споживачів. Він, зокрема, передбачає права споживачів на доступ до будь-яких зареєстрованих персональних даних і на внесення до них правок [9, с. 50].

Положення про захист даних закріплено в Конституції Південної Африки [10]. Право на конфіденційність міститься також у Законі про захист прав споживачів 2008 року та в Законі про електронні комунікації й договори 2002 року. Дотримання норм останнього закону має добровільний характер і має бути відображено в угоді із суб'єктом даних. На розгляд парламенту Південної Африки внесений новий законопроект про захист особистої інформації [11, с. 89].

У Конституції Об'єднаних Арабських Еміратів зазначено, що фізичній особі «гарантується свобода й конфіденційність листування, передачі телеграфних повідомлень та інших засобів зв'язку відповідно до закону». Крім того, в Кримінальному кодексі цієї країни закріплені деякі права на конфіденційність і на захист персональних даних [12, с. 60].

В Індії відсутнє конституційне право на конфіденційність, хоча Верховний суд постановив, що принцип конфіденційності варто вважати складником права на життя й особисту свободу. Збирання та оброблення персональних даних регламентуються Законом про інформаційні технології 2000 року, в якому зазначено, що компанії мають вживати адекватних заходів безпеки під час обробленя персональних даних і що в разі отримання таких даних відповідно до договору їх не можна розкривати без згоди суб'єкта [13, с. 42].

У Японії введено в дію закон про захист державних секретів, аналогічний законам, що діють в інших розвинених країнах. Він стосується всіх видів оброблення даних, однак застосовується лише тоді, коли йдеться про інформацію, що належить 5000 і більше фізичних осіб. Цей закон установлює загальні вимоги до дозволів, безпеки й надання інформації, а також додаткові вимоги щодо контролю за працівниками і третіми особами, які займаються обробленням персональних даних [14, с. 68].

Серед його основних принципів відзначимо такі:

– держава має використовувати цей закон для зміцнення дипломатичної та національної безпеки;

– одночасно особлива увага має бути приділена практиці застосування закону, щоб громадяни не відчули якогось обмеження своїх прав.

Закон, спеціально призначений для захисту секретних даних, який посилив покарання державних службовців за «злив» секретної інформації, що стосується національної безпеки, набув чинності. У Японії вже є закони, що регулюють захист державних секретів, включаючи національний закон про цивільну службу, правила спеціального захисту секретів відповідно до угоди від 1954 року між Японією і США про взаємну оборону. Діє також низка правових норм щодо захисту секретної інформації в Силах Самооборони. Але, як визнають експерти, ці закони натепер не забезпечують адекватного захисту важливої секретної інформації, тому секрети в Японії легко «витікають» [14, с. 69]. Новий закон забезпечує досконалий і комплексний захист державних секретів, що стосуються оборони та дипломатії.

Коротке ознайомлення з міжнародним досвідом захисту показує, що правове забезпечення захисту інформації в різних країнах здійснюється по-різному.

У більшості європейських країн, у країнах Азії, Близького Сходу, Латинської Америки, США до кінця XX ст. прийняті або зазнали редакції чинні закони, пов'язані із захистом конфіденційної інформації. В одних випадках це закони про конкуренцію, в інших – спеціальні закони про конфіденційну інформацію. У деяких країнах обмежуються кодексами (кримінальними, цивільними) та різними договорами й угодами.

Закінчуючи наш огляд тенденцій зарубіжного законодавства, можна резюмувати, що в цей час немає законодавства у сфері конфіденційності, однаково обов'язкового до виконання в усіх країнах світу. Закони про конфіденційність і захист даних уже прийняли понад 90 країн, при цьому багато хто з них розглядають регулювання міжнародних потоків даних як механізм захисту недоторканності приватного життя фізичних осіб і забезпечення виконання національної політики.

Однак правова регламентація режимів конфіденційної інформації залишається дуже складною правовою категорією. Складність ця передусім зумовлена відсутністю єдиного розуміння конфіденційної інформації. Процеси уніфікації, характерні для сучасного права, лише частково торкаються категорії конфіденційної інформації. Найбільш перспективним для вивчення в цьому контексті є досвід регулювання режимів конфіденційної інформації в рамках права Європейського Союзу. Європейська модель прекрасно ілюструє проблеми, з якими стикаються бізнес та економіка у зв'язку з відсутністю ясних і послідовних законів, які можуть бути втілені в життя, незважаючи на державні кордони. Ця гіпотеза не нова для сучасного законотворчого процесу.

У звіті «Тенденції в реформуванні електрозв'язку, 2016 рік» [15] подано огляд нормативно-правової бази в галузі конфіденційності та захисту даних, що є в Європейському Союзі й низці розвинених країн, а також країн, що розвиваються. У цьому огляді ілюструються та аналізуються проблеми й можливості, з якими стикаються сучасні державні органи ІКТ через розширення послуг, конвергенцію платформ і підготовку мережевими операторами своїх інфраструктур до переходу до наступного покоління інформаційноємних технологій, починаючи від рухомого зв'язку 5G до Інтернету речей. Найбільш повний із наявних у світі огляд «Тенденції в реформуванні електрозв'язку, 2016 рік» включає аналітичні матеріали, представлені широким колом провідних світових експертів, щоб допомогти державним органам, аналітикам у сфері ІКТ та журналістам, які висвітлюють пов'язані з технологіями питання, більш глибоко розуміти ті проблеми, з якими стикаються все більш широке коло учасників галузі ІКТ і споживачі. Також відповідно до положень цього звіту багато країн, що прийняли нормативні акти у сфері конфіденційності або розглядають можливість їх прийняття, орієнтуються на європейську модель, тому становище в Європі розглянуто в огляді найбільш детально. Європейська модель також відмінно ілюструє проблеми, з якими стикаються бізнес та економіка у зв'язку з відсутністю ясних і послідовних законів, що регулюють правовідносини у сфері захисту конфіденційної інформації.

Так, відповідно до Європейської директиви про захист даних [16] обов'язки щодо захисту даних зазвичай покладаються на контролерів, тоді як до тих, хто обробляє дані, висуваються лише конкретні вимоги у сфері безпеки. Але з огляду на відмінності у визначеннях, що використовуються в різних європейських країнах, а також неясності із зарахуванням постачальників хмарних послуг до контролерів або тих, хто обробляє дані, виникає невизначеність.

Мета договору про конфіденційність у європейському праві – трансформація зобов'язання про нерозголошення інформації третім особам. Цей процес може супроводжуватися передачею певної інформації або відкриттям доступу до певної інформації. Європейська практика свідчить також, що

договори про конфіденційність здебільшого підписуються навіть у разі появи будь-якої (навіть найменшої) можливості отримання або розголошення інформації певною особою або групою осіб [17, с. 93].

Показово, що в мережі Інтернет така можливість є практично між усіма користувачами одночасно. Очевидно, що в ситуаціях неможливості укладення договору з усіма особами компанії і приватні особи на своїх веб-ресурсах розміщують правове застереження (disclaimer). До них зараховуємо також і договори про конфіденційність у вигляді договорів приєднання, що набувають чинності з моменту доступу до ресурсу.

Крім зазначеної директиви, в Європейському Союзі конфіденційність інформації регулюється за допомогою низки угод і директив, таких як директиви 2002/58/ЄС та ETS108, ETS181, ETS185, ETS189. Зокрема, Конвенція «Про злочинність у сфері комп'ютерної інформації» (ETS № 185) [18] спрямована на стримування в тому числі дій, спрямованих проти конфіденційності комп'ютерних даних і комп'ютерних мереж, систем. Відповідно до цієї Конвенції для протидії злочинам проти конфіденційності, доступності й цілісності комп'ютерних даних і систем кожна сторона вживає таких законодавчих та інших заходів, які потрібні для того, щоб кваліфікувати це як кримінальний злочин згідно з її внутрішнім законодавством. До таких заходів ми зараховуємо:

– протизаконний доступ;
– неправомірне перехоплення;
– вплив на дані;
– вплив на функціонування системи;
– протизаконне використання пристроїв.

Згідно з Конвенцією «Про захист фізичних осіб у разі автоматизованої обробки персональних даних» (ETS № 108) [19], сторони зобов'язані дотримуватися таємності або конфіденційності під час використання персональних даних.

Зараз більшість іноземних компаній висувають украй жорсткі вимоги щодо дотримання угод про конфіденційність, особливо якщо справа стосується передачі виняткових прав на результати інтелектуальної діяльності. Штрафи обговорюються заздалегідь і можуть доходити до сотень тисяч доларів. Підписуючи такі угоди, вітчизняні компанії не можуть не замислюватися над забезпеченням конфіденційності отриманих відомостей. Специфіка забезпечення інформаційної безпеки в медіа-бізнесі така, що в компаніях цієї сфери, як правило, працюють творчі люди, у чималій кількості використовуються мультимедійні дані великих розмірів, а також тиражуються типові IT-системи. Стандартні технології захисту, які історично застосовувалися в медійному бізнесі, такі як використання «сліпого дубляжу», обмеження на доступ акторів озвучення до всього матеріалу, черговість надання серій правовласником, так само, як і традиційні методи охорони, нині вже не забезпечують необхідної захищеності, і технології інформаційної безпеки могли б у цьому допомогти. Можна довіряти власному персоналу, але контроль робочої діяльності співробітників має здійснюватися на рівні, адекватному ризикам порушення інформаційної безпеки, які досить високі. Мінімально необхідні дії для захисту включають запровадження систем моніторингу інформаційних потоків і запобігання витокам даних. Це сувора рекомендація міжнародних стандартів і кращих практик у сфері забезпечення інформаційної безпеки [20].

Висновок

Законодавча регламентація режимів конфіденційної інформації продовжує бути дуже складною правовою категорією. Складність ця передусім зумовлена відсутністю єдиного розуміння конфіденційної інформації. Процеси уніфікації, характерні для сучасного права, лише частково торкаються категорії конфіденційної інформації. Найбільш перспективним для вивчення в цьому контексті є досвід регулювання режимів конфіденційної інформації в рамках права Європейського Союзу. Європейська модель прекрасно ілюструє проблеми, з якими стикаються бізнес та економіка у зв'язку з відсутністю ясних і послідовних законів, які можуть бути втілені в життя, незважаючи на державні кордони.

Список використаних джерел:

1. Нашинець-Наумова А.Ю. Інформаційна безпека суб'єктів господарювання: проблеми теорії та практики правозастосування : монографія / під заг. ред. д.ю.н. В.І. Курила. Херсон : Видавничий дім «Гельветика», 2017. 386 с.

2. Защита данных и конфиденциальность. URL: https://itunews.itu.int/Ru/Note.aspx?Note=3690.

3. Сергеев М.П. Законодательство Франции в сфере защиты персональных данных и информационной безопасности. *Международное право*. 2010. № 3. С. 45–46.

4. Ласихин В.А. «Патриотический акт»: юридический анализ. *Информационное право*. 2007. № 6. С. 32–47.

5. Сергеев М.П. Законодательство Германии в сфере защиты персональных данных и информационной безопасности. *Международное право*. 2009. № 1.

6. Canadian Charter of Rights and Freedoms. URL: laws-lois.justice.gc.ca/eng/Const/page-15.html.

7. Гон Р. Право Канады. Москва : VSD, 2013.

8. Конституция Бразилии 1988 года. URL: http://www.russobras.ru/constitution.php.

9. Павлов И.Ю. Правовое обеспечение доступа к официальной информации : диссертация на соискание ученой степени кандидата юридических наук. Специальность 12.00.14 «Административное право; Финансовое право; Информационное право» / Науч. рук. В.Н. Монахов; Российская академия наук. Институт государства и права. Москва, 2008. 223 с.

10. Конституция Южно-Африканской республики 1996 года. URL: http://worldconstitutions.ru/archives/78.

11. Лопатин В.Н. Правовая охрана и защита служебной тайны. *Государство и право*. 2000. № 6. С. 85–91.

12. Захер М. Межарабская правовая система и проблема арабского единства. Москва : Наука, 2007. 197 с.

13. Ибрагимов М.Т. Об арбитражной и судебной практике в Индии. *Международное право*. 2007. № 7. С. 42–43.

14. Еремин В.Н. К вопросу о характеристике современного японского права. *Государство и право*. 2007. № 3. С. 67–69.

15. Trends in Telecommunication Reform 2016: Regulatory Incentives to Achieve Digital Opportunities. URL: https://www.itu.int/net/pressoffice/press_releases/2016/pdf/12-ru.pdf.

16. Про захист фізичних осіб у разі обробки персональних даних і про вільне переміщення таких даних : Директива 95/46/ЄС Європейського Парламенту і Ради від 24 жовтня 1995 року. URL: http://zakon3.rada.gov.ua/laws/show/994_242.

17. Основные институты гражданского права зарубежных стран. Сравнительно-правовое исследование / Под ред. В.В. Залесского. Москва : Норма, 2009. 214 с.

18. Конвенция о преступности в сфере компьютерной информации (ETS N 185). от 23.11.2001. URL: http://zakon3.rada.gov.ua/laws/show/994_789.

19. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data CETS №: 108 URL:https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?

20. Манжай О.В. Порівняльний аналіз забезпечення безпеки оперативно-розшукової інформації за допомогою інституту державної та службової таємниці в окремих країнах світу. *Форум права*. 2012. № 1. С. 591–600. URL: http://nbuv.gov.ua/j-pdf/ FP_index.htm_2012_1_91.pdf.

В статье представлены результаты мирового опыта законодательной регламентации режимов конфиденциальной информации. Показана важность использования этого опыта для практической реализации процессов информационного обеспечения в Украине. Анализируя международный опыт правового регулирования отношений по защите конфиденциальной информации, автор определяет перспективные направления дальнейшего развития для Украины в указанной сфере.

Ключевые слова: режимы конфиденциальной информации, информационная безопасность, международный опыт, законодательная регламентация.

The article presents the results of world experience in the legislative regulation of confidential information regimes. The importance of using this experience for the practical implementation of information support processes in Ukraine is shown. Analyzing the international experience of legal regulation of relations with regard to the protection of confidential information, the author determines the perspective directions of further development for Ukraine in this area.

Key words: confidential information regimes, information security, international experience, legislative regulation.