Адміністративне право і процес; фінансове право; інформаційне право

УДК 34:316.776-049.5

Тарас Перун *

ШЛЯХИ ПОКРАЩЕННЯ ВЗАЄМОДІЇ МІЖ УКРАЇНОЮ ТА ЄС У СФЕРІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У статті проаналізовано законодавство Європейського Союзу та України у сфері забезпечення інформаційної безпеки. Розкрито особливості інформаційної політики Євросоюзу, де поряд з традиційними (друкованими) формами опублікування дедалі більшого розповсюдження набувають альтернативні джерела інформації, засновані на новітніх досягненнях комп'ютерної технології та інформатики.

***Ключові слова**: правове регулювання, законодавче забезпечення, інформаційна безпека, інтернет-пропаганда та інтернет-рекрутування, загрози інформаційній безпеці, інформаційно-комунікаційні технології.*

***Перун Т. С. Пути улучшения взаимодействия между Украиной и ЕС в сфере обеспечения информационной безопасности**.*

В статье проанализировано законодательство Европейского Союза и Украины в сфере обеспечения информационной безопасности. Раскрыты особенности информационной политики Евросоюза, где наряду с традиционными (печатными) формами опубликования все большее распространение приобретают альтернативные источники информации, основанные на новейших достижениях компьютерной технологии и информатики.

***Ключевые слова**: правовое регулирование, законодательное обеспечение, информационная безопасность, интернет-пропаганда и интернет-рекрутирования, угрозы информационной безопасности, информационно-коммуникационные технологии.*

Perun T. S. Ways to improve interaction between Ukraine and the EU in the field of information security.

The article analyzes the legislation of the European Union and Ukraine in the field of information security. The peculiarities of the European Union information policy are revealed, where, along with traditional (printed) forms of publication, alternative sources of information, based on the latest advances in computer technology and computer science.

Keywords: legal regulation, legislative provision, information security, Internet propaganda and internet recruitment, threats to information security, information and communication technologies.

Актуальність теми дослідження. Прискорений розвиток обчислювальної техніки та нових інформаційно-комунікаційних технологій все більше стає причиною змін у політичній, економічній та соціально-культурній сферах суспільних відносин. Експерти Всесвітнього економічного форуму 2016 року вважають, що наразі суспільство переживає четверту індустріальну революцію, яка об'єднує можливості інформаційних технологій, промислового виробництва, Інтернету речей та Інтернету послуг, а індекс конкурентоспроможності економік провідних держав має високий рівень кореляції з індексом розвитку інформаційно-комунікаційних технологій [1, с. 78]. За оцінками Бостонської консалтингової групи, однієї з найвпливовіших міжнародних компаній в області аналітики економіки та управлінського консалтингу, вплив Інтернету на ефективність діяльності організацій вищий за будь-які інші технології з часів попередньої промислової революції [2].

Після революції гідності Україна обрала курс на повноцінне входження до Європейської спільноти. Значних зусиль на цьому шляху наша держава докладає у виробленні спільних механізмів покращення інформаційної безпеки.

У цьому контексті актуальним та своєчасним вбачається формулювання на теоретичному рівні спільних шляхів щодо покращення взаємодії між Україною та Європейським Союзом у сфері забезпечення інформаційної безпеки.

Стан дослідження. Проблематика забезпечення інформаційної безпеки носить яскраво виражений міждисциплінарний характер та досліджувалася фахівцями різних галузей правової науки. Зокрема, інформаційна безпека стала об'єктом дослідження таких учених, як: Л. І. Бажан, О. Бакаєв, В. Г. Воронкова, В. Гвоздецький, О. П. Дзьобань Л. І. Кайдан, Т. Г. Кравченко, В. В. Кулик, Є. С. Ларина, В. Овчинський, В. Г. Пилипчук, О. В. Соснін, П. Д. Фролов, К. Шваб.

Водночас, питання щодо вироблення спільних механізмів ефективного забезпечення інформаційної безпеки між Україною та ЄС потребують додаткового опрацювання.

Мета дослідження полягає у тому, щоб на основі аналізу європейського та національного законодавства та практики його реалізації сформулювати конкретні пропозиції щодо вироблення шляхів покращення взаємодії у сфері забезпечення інформаційної безпеки.

Виклад основних положень. Аналіз наукових публікацій щодо забезпечення інформаційної безпеки [3, с. 235; 4, с. 45; 5, с. 25; 6, с. 47; 7, с. 15; 8, с. 21–22; 9, с. 10] дає підстави твердити про її визначальну роль у сфері забезпечення безпеки національної. Наприклад, Дзьобань О. П. твердить про перенасичення інформаційних ресурсів у сучасних процесах обміну інформацією, що в кінцевому випадку може призвести до інформаційного колапсу [4, с. 47]. Той же вчений у науковій статті під назвою: «Інформаційна безпека: нові виміри загроз, пов'язаних із інформаційно-комунікаційною діяльністю» акцентує увагу на термінологічній невизначеності понять, обумовленій стрімким розвитком інформаційного суспільства, а саме: «інформаційне протиборство», «інформаційний тероризм», «кіберзлочини» [5, с. 25] тощо.

Підкреслюючи шкідливий вплив інформації на виникнення міждержавних конфліктів, В. Г. Пилипчук наголошує на ключовій ролі інформаційних ресурсів у процесі вирішення неврегульованих територіальних спорів між країнами, міжнародній конкуренції та зіткненні міжнаціональних інтересів [10, с. 87–90].

Водночас, дискусійною виглядає думка В. Гвоздецького, який під час формулювання загроз існуванню сучасного суспільства ставить в один ряд такі негативні чинники, як соціальне розшарування, корупцію та інформаційно-психологічні загрози [3, с. 235]. На нашу думку, зазначені фактори потребують більш детальної систематизації, оскільки не є однопорядковими.

На актуальності й важливості інформаційної захищеності суспільства й держави наголошується і у ч. 4 ст. 3 Закону України «Про національну безпеку», яка визначає пріоритетне спрямування державної політики держави на забезпечення інформаційної безпеки [11].

Поряд із цим, відповідно до ч. 3 ст. 3 згаданого законодавчого акта, до фундаментальних національних інтересів України належить інтеграція держави в європейський політичний, економічний, безпековий, правовий простір, набуття членства в Європейському Союзі та в Організації Північноатлантичного договору, розвиток рівноправних взаємовигідних відносин з іншими державами [11].

Таким чином, набуває актуальності питання щодо визначення ефективних шляхів взаємодії України та ЄС у напрямку забезпечення інформаційної безпеки.

Останнім часом серед багатьох європейських країн ЄС спостерігається віднесення інформації до «міжнародних ресурсів». Даний факт викликав особливий інтерес дослідників інформаційних процесів у сфері транскордонної передачі інформації, у тому числі до проблеми захисту державного суверенітету. Накопичення і обробка даних, часто конфіденційних, в одній державі про іншу можуть представляти серйозну загрозу для незалежності останньої і для здійснення її суверенних прав.

У той же час, слід констатувати, що здобутки європейських країн в інформаційній сфері, а передовсім – розуміння інформаційної безпеки, не відрізняються одноманітністю, знаходяться на різних технологічних та нормативно-правових етапах свого розвитку. У цьому контексті не є виключенням і Україна, яка тільки з прийняттям базових правових актів у згаданій сфері суспільних відносин [12–15] усвідомила значущість і важливість інформаційної безпеки для держави та розпочала процес вироблення механізмів захисту інформаційних відносин на сучасному міжнародному рівні.

Тому вироблення спільних шляхів щодо покращення інформаційної безпеки має бути наслідком уніфікації законодавства у сфері захисту інформації та усунення технологічного розриву в процесі інформатизації суспільства.

А в теперішній час маємо констатувати, що в Європейському Союзі, на відміну від України, існує система інформаційних видань і баз даних, що забезпечує поширення та доступ до процесів обговорення і прийняття нормативних актів та іншої офіційної інформації про діяльність ЄС. Поряд із традиційними (друкованими) формами опублікування дедалі більшого розповсюдження набувають альтернативні джерела інформації, засновані на новітніх досягненнях комп'ютерної технології та інформатики: електронні публікації, комп'ютерні інформаційні системи і бази даних.

Рада і Комісія ЄС прийняли рішення про створення комп'ютерних систем зберігання і поширення інформації – спеціалізованих банків даних та комп'ютерних мереж.

Наприклад, система SEBEX – універсальне джерело зберігання і поширення джерел права Європейського Союзу. Її можна розглядати в якості електронного аналога офіційного журналу. У банку даних SEBEX містяться повні тексти всіх документів, прийнятих Європейським Співтовариством та Союзом, починаючи з 1951 року. Усі вони в даній системі розподілені на 7 секторів: установчі договори; угоди; «вторинне» право Європейських Співтовариств (законодавчі акти, прийняті інститутами Союзу); документи допоміжного і підготовчого характеру (укладення Європарламенту, Комітету регіонів та ін.); парламентські питання; рішення Європейського Суду та Суду Першої Інстанції; посилання на законодавчі акти держав-членів, прийняті для виконання положень директив ЄС.

Системи SCAD, ECLAIS містять автоматизований каталог Бібліотеки Комісії в Брюсселі (центральної бібліотеки ЄС, яка має повною колекцією всіх документів Союзу на всіх офіційних мовах); EPISTOLE – включає понад 10 ТОВ публікацій про ЄС; EPOQUE – інформація про діяльність представницького органу ЄС – Європарламенту; BIAS – банк даних про діяльність всіх інститутів і органів ЄС.

Існують також системи документації права ЄС, які створюються державами-членами, комерційними організаціями і науковими інститутами: LEXUS (Великобританія), JURIS (ФРН); CD-ROM EUROPA (Нідерланди).

У системі Європейського Союзу функціонують також інформаційні центри, розташовані у великих містах Союзу. Серед них: європейські інформаційні центри, орієнтовані на підприємців, довідкові центри, що діють в університетах, європейські депозитарні бібліотеки і євробібліотеки (отримують копії офіційних публікацій ЄС); локальні міські і сільські інформаційні центри; система Європраво – складається із професійних юристів, які надають консультації громадянам і юридичним особам з різних аспектів застосування права Європейського Союзу; COLINE – представляє консультації з питань прав споживачів в Європейському Союзі; «Команда Європа» – має своїм завданням проведення лекцій з пропаганди цілей, принципів і наслідків введення внутрішнього ринку ЄС, різних аспектів внутрішньої і зовнішньої політики.

Слід також відмітити провідну роль Європейського Союзу та міжнародних організацій у регулюванні міжнародного інформаційного обміну.

Європейським Союзом розроблений ряд інформаційних систем і програм, мета яких – розширення регіональної та міжнародної співпраці в галузі інформатизації. З 1979 року в рамках ЄС діє інформаційна мережа ЄВРОНЕТ, яка поширює технічні, наукові, юридичні, соціально-економічні дані в Європейському Союзі. Створено банк даних ЄВРОБАЗА із соціально-політичних проблем розвитку західноєвропейських країн. Здійснювана ЄС програма європейського технологічного співробітництва «Еврика» також передбачає широкий обмін даними і досягненнями в області інформатизації між її учасниками. Ряд подібних програм реалізується під егідою ЮНЕСКО.

Ще наприкінці XX століття європейські законодавці стали приділяти пріоритетне значення захисту інформації. У 1980 році Рада Європи розробила Європейську конвенцію про захист фізичних осіб у питаннях, що стосуються автоматизованої обробки особистих даних, вона вступила в силу в 1985 році. Конвенція визначає порядок збору та обробки даних про особу, принципи зберігання і доступу до них.

У 1980 році в рамках Організації економічного співробітництва та розвитку (ОЕСР) був прийнятий документ «Керівні принципи захисту особистого життя і передача даних про особу через кордони», мета якого – обмежити несанкціонований збір даних про фізичних та

юридичних осіб і передачі їх за кордон для того, щоб використовувати в цілях, визнаних неправомірними в країні-відправника.

Україна – не перша країна, яка вирішує проблеми розміщення конфіденційної інформації і її збору в Інтернеті, тим більше, що цьому сприяє технічна основа мережі (її прозорість, відкритість, доступність, масовість учасників). Значна робота в цьому напрямку проведена і в країнах Європейського Союзу (ЄС). Вона пов'язана, наприклад, із регулюванням порядку обробки персональних даних.

Наприклад, Директива ЄС № 95/46 / ЄС [16] детально регулює питання захисту конфіденційної інформації. Зокрема, документ встановлює, що громадяни ЄС в принципі не мають права на зберігання секретної інформації; будь-яка особа, що виступає в якості об'єкта збору інформації, має право знати, яка інформація про неї зберігається і як вона використовується; у такої особи повинна бути також можливість запобігти використанню без її згоди персональної інформації про неї тільки з чітко визначеною метою; вона повинна мати можливість виправляти інформацію, що зберігається; організація, що створює, підтримує, використовує і поширює таку інформацію, повинна забезпечити її достовірність щодо зазначених цілей і вживати заходів, спрямованих на запобігання зловживанню такими даними.

У європейських країнах збір персональних даних пов'язаний з виконанням ряду додаткових умов. Найбільш поширеною вимогою є обов'язок особи, що збирає таку інформацію, реєструватися (в Німеччині, Нідерландах та ін.), або повідомляти орган, уповноважений в даній країні стежити за дотриманням правил про збереження даних (у Великобританії, Іспанії, Італії, Франції та ін.). Повідомлення такого органу до вчинення дій з персональними даними передбачено і Директивою ЄС № 95/46/ЄС. Невиконання зазначеного обов'язку іноді карається серйозним штрафом або навіть розглядається як кримінальний злочин (наприклад, у Великобританії, Італії, Нідерландах, Франції).

Для забезпечення полегшення відвідувачам оцінки сайту з точки зору збереження конфіденційної інформації, деякі компанії ввели спеціальні сертифікати, які може отримати лише той сайт, який дотримується певних правил поводження з одержуваної конфіденційною інформацією (на сайті в цьому випадку розміщується особливий логотип такого сертифіката). Із найбільш відомих можна назвати сертифікати TRUSTE і BBBOnline, але вони ще не набули широкого поширення в нашій країні.

Доцільним в цьому контексті вбачається необхідність законодавчого врегулювання порядку сертифікації інтернет-сайтів в Україні, що сприятиме більш ефективному захисту інформації.

Слід зазначити, що процес передачі персональних даних в ЄС досить докладно регламентований на законодавчому рівні. Предметом правового регулювання у даному напрямку в країнах Європейського Союзу також виступає: заборона на прослуховування, перехоплення повідомлень, їх зберігання без згоди особи, за винятком, коли це дозволено законодавством для забезпечення національної безпеки, оборони, розслідування злочинів і т.д. (Директива ЄС № 97/66 ЄС від 15 грудня 1997 року) [17]; правовий режим «копіювання» інформації, коли Директива ЄС № 2000/31/ЄС (Directive on electronic commerce) [18] звільняє особу від відповідальності за здійснення такого копіювання в разі, якщо копіювання робиться автоматично, має «проміжний» і тимчасовий характер, і його єдиною метою є забезпечення більш ефективної передачі інформації (ст. 13); визначення правил роботи провайдерів з конфіденційною інформацією.

Так, Директива ЄС № 97/66 / ЄС від 15 грудня 1997 року стосовно передачі персональних даних та захисту особистої сфери в секторі телекомунікацій встановлює, що дані, пов'язані з передачею інформації, повідомлені користувачами для встановлення з'єднання і збереження провайдером, що забезпечує використання публічної телекомунікаційної мережі та (або) загальнодоступних телекомунікаційних послуг, повинні бути пошкоджені або зроблені анонімними після розриву з'єднання (за деякими винятками, наприклад, коли інформація зберігається в цілях підготовки рахунків користувачеві на оплату наданих послуг).

Серйозним засобом захисту інформації, переданої за допомогою Інтернету, є використання програм шифрування, однак і це часто не захищає користувача мережі та спонукає

державу шукати підходи до правового регулювання використання сучасних механізмів шифрування. При цьому спостерігається все більше прагнення держави «впорядкувати» роботу Інтернету, «зарегулювати» діяльність громадян в даній світовій мережі. Це стосується не тільки України, але і більшості країн Євросоюзу. Наприклад, у Великій Британії легалізований порядок надання права державним органам вимагати від провайдерів журнали мережевого трафіку і перехоплювати передані повідомлення. В Італії діє механізм накладення штрафних санкцій за порушення порядку розголошення персональних даних і т.д.

Нескладно припустити, що у зв'язку і під приводом посилення терористичної загрози, держава і надалі буде не завжди виправдано намагатися обмежувати вільне переміщення інформації в Інтернеті. Разом з тим, очевидно й інше – вільний обмін інформацією в Інтернет не повинен завдавати шкоди громадянам, їх права на конфіденційність повинні бути надійно захищені в демократичному суспільстві за допомогою законодавства і новітніх технологій, програмного забезпечення інформаційних процесів тощо.

Висновки. На підставі викладеного можемо констатувати наступне. По-перше, аналіз законодавства ЄС дає підстави для висновку, що законотворча робота щодо посилення інформаційної безпеки успішно здійснювалася ще наприкінці XX століття. В Україні процес правового регулювання інформаційних відносин та захисту інформації розпочався відносно нещодавно, що й обумовлює факт відставання нашої держави в інформаційно-телекомунікаційному просторі від країн-членів ЄС.

По-друге, в країнах Євросоюзу достатньо докладно регламентовано відносини щодо обігу персональних даних та конфіденційної інформації, чого не можна сказати про національне законодавство.

По-третє, важливість питань інформаційної безпеки для України, на відміну від країн Євросоюзу, набула практичного значення в контексті захисту суверенітету та територіальної цілісності після вторгнення РФ на територію нашої держави. До того ж, прийнятий Верховною Радою України Закон України «Про національну безпеку» лише побіжно торкається питань щодо визначення шляхів взаємодії з Європейським Союзом у напрямку посилення інформаційної безпеки.

Водночас, необхідною умовою щодо подальшого формування шляхів взаємодії між Україною та ЄС у сфері забезпечення інформаційної безпеки є безумовне виконання центральними органами виконавчої влади, зокрема МЗС України, положень Доктрини інформаційної безпеки, затвердженої Указом Президента України від 25.02.2017 р. № 47/2017.

Список використаних джерел:

1. Schwab K. The fourth industrial revolution. Foreign Affairs. 2016. Vol. 12., P. 78.

2. The economic impact of shutting down Internet and mobile phone services in Egypt. OECD Directorate for Science, Technology and Industry. URL: http: www.oecd.org/sti/ieconomy/theeconomicimpactofshuttingdowninternetandmobilephoneservicesinegypt.htm (available at: 13.07. 2018).

3. Гвоздецький В. Зміст та сутність корупції у сучасному світі. *Університетські наукові записки* (*Часопис Хмельницького університету управління і права*). 2011. № 1 (37). С. 234–239.

4. Дзьобань О.П., Соснін О.В. До проблеми визначення місця й ролі інформаційних аспектів безпеки у соціальних процесах. *Науковий вісник Інституту міжнародних відносин НАУ. Серія: Економіка, право, політологія, туризм*. 2011. Вип. 1 (3). С. 45–49.

5. Дзьобань О.П., Соснін О.В. Інформаційна безпека: нові виміри загроз, пов'язаних із інформаційно-комунікаційною діяльністю. *Гуманітарний вісник Запорізької державної інженерної академії*. 2015. Вип. 61. С. 24–34.

6. Інформаційний вплив: теорія і практика прогнозування : монографія / за ред. П.Д. Фролова. Київ : Міленіум, 2011. 303 с.

7. Ларина Е., Овчинский В. Кибервойны XXI века: о чем умолчал Эдвард Сноуден. М. : Книжный мир, 2014. 349 с.

8. Методи, моделі і інформаційні технології в управлінні економічними системами різних рівнів ієрархії : монографія / О.О. Бакаєв, Л.І. Бажан, Л.І. Кайдан, Т.Г. Кравченко, В.В. Кулик ; за ред. О.О. Бакаєва. Київ : Логос, 2008. 127 с.

9. Новітні інформаційні технології і системи в економіці (до Дня науки) : матеріали наук.-практ. конф. (20.05.2009 р.). Ірпінь, 2009. 120 с.

10. Пилипчик В.Г., Дзьобань О.П. Інформаційне суспільство: філософсько-правовий вимір : монографія. Ужгород : ІВА, 2014. 282 с.

11. Про національну безпеку : Закон України від 21.06.2018 № 2469-19. URL: http://zakon2.rada.gov.ua/laws/show/2469-19 (дата звернення: 15.07.2018).

12. Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» : Указ Президента України від 1 травня 2014 року № 449/2014. *Офіційний вісник України*. 2014. № 37. Ст. 28.

13. Стратегія забезпечення кібернетичної безпеки України / Національний інститут стратегічних досліджень. URL: http://www.niss.gov.ua/public/File/2013_nauk_an_rozrobku/kiberstrateg.pdf. (дата звернення: 15.07.2018).

14. Проект Концепції інформаційної безпеки України / Міністерство інформаційної політики України. URL: http://mip.gov.ua/documents/30.html. (дата звернення: 15.07.2018).

15. Про внесення змін до деяких законів України щодо захисту інформаційного телерадіопростору України : Закон України від 05.02.2015 № 159-VIII. *Відомості Верховної Ради України*. 2015. № 18. Ст. 131.

16. Директива ЄС № 95/46 / ЄС «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року. URL: http://zakon5.rada.gov.ua/laws/show/994_242. (дата звернення: 15.07.2018).

17. Директива ЄС № 97/66 / ЄС «Стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі» від 15 грудня 1997 року. URL: http://zakon3.rada.gov.ua/laws/show/994_243. (дата звернення: 15.07.2018).

18. Директива ЄС № 2000/31 / ЄС «Про деякі правові аспекти інформаційних послуг, зокрема, електронної комерції, на внутрішньому ринку» («Директива про електронну комерцію») від 8 червня 2000 року. URL: http://zakon5.rada.gov.ua/laws/show/994_224. (дата звернення: 15.07.2018).

* ***Перун Тарас Степанович – помічник-консультант народного депутата України, асистент кафедри адміністративного та інформаційного права Навчально-наукового інституту права та психології Національного університету «Львівська політехніка».***

Стаття надійшла до редакції 19 вересня 2018 р.

УДК 35.077.6+342.9

Микола Самбор *

ДИСКРЕЦІЙНІ ПОВНОВАЖЕННЯ ЩОДО СКЛАДЕННЯ ПРОТОКОЛІВ ПРО АДМІНІСТРАТИВНІ ПРАВОПОРУШЕННЯ

У статті розглядаються актуальні питання дискреційних повноважень посадових осіб, уповноважених складати протоколи про адміністративні правопорушення. Досліджується співвідношення права суб'єкта, уповноваженого складати протоколи про адміністративні правопорушення з його обов'язками та повноваженнями, якими такий суб'єкт наділений у зв'язку із виконанням функцій держави та наданням відповідних адміністративних чи поліцейських послуг. Аналізуються норми чинного законодавства України щодо визначення розсуду поліції на складання протоколів про адміністративні правопорушення.

***Ключові слова**: дискреційні повноваження, адміністративний розсуд, протокол про адміністративне правопорушення.*

Самбор Н. А. Дискреционные полномочия по составлению протоколов об административных правонарушениях.

В статье рассматриваются актуальные вопросы дискреционных полномочий должностных лиц, уполномоченных составлять протоколы об административных правонаруше-