ЗБІР ПЕРСОНАЛЬНИХ ДАНИХ ТА ІНФОРМАЦІЙНА БЕЗПЕКА: АДМІНІСТРАТИВНО-ПРАВОВИЙ АСПЕКТ

БОЙКО Оксана Миколаївна - науковий співробітник, Український науково-дослідний інститут спеціальної техніки та судових експертиз СБ України.

УДК 342.6:342.922(477)
DOI 10.32782/EP.2021.2.10

Початок третього тисячоріччя ознаменувався бурхливим розвитком інформаційних технологій.Проте інформація використовується як інструмент скоєння правопорушень, також активно використовується в політиці і ведені інформаційних війн, зокрема є знаряддям гібридної війни Російської Федерації проти нашої держави. Сьогоденний стан теоретико-практичного забезпечення адміністративно-правового режиму інформаційної безпеки в Україні, не в повній мірі відповідає вимогам безпекової ситуації. Мета. Метою статті є аналіз адміністративно-правових поглядів на проблему збирання персональних даних та забезпечення інформаційної безпеки в Україні, а також перспектив удосконалення інформаційної безпеки в умовах гібридної агресії Російської Федерації. Для досягнення вказаної мети було поставлено завдання: проаналізувати наявні наукові розробки і стан чинного законодавства у сфері збирання персональних даних та забезпечення інформаційної безпеки в Україні; виявити проблемні аспекти та надати пропозиції, щодо вдосконалення системи інформаційної безпеки. Результати. У процесі дослідження було проаналізовано наукові розробки і стан чинного законодавства щодо збирання персональних даних та забезпечення інформаційної безпеки в України. З позиції адміністративного права було проаналізовано поняття «збирання персональних даних» та «інформаційної безпеки» та їх співвідношення.

Було встановлено, що визначення поняття «інформаційна безпека» відсутнє в нормативно-правовій базі держави. А також той факт, що поняття «персональні данні» не корелюється з поняттям «конфіденційної інформації про особу», що міститься в Конституції України.

Також було проаналізовано сучасні проблемні моменти у гарантуванні безпеки персональних даних та причини виявлених недоліків у інформаційній безпеці України.

Розглянуто дві форми збору персональних даних: з дозволу та без відповідного дозволу. Підкреслено, що головним фактором у процесі збору, зберігання та обробки даних є захист прав і свобод людини.

Зазначимо, що збір персональних даних, у разі його здійснення у відповідності до Закону, є позитивною складовою інформаційної безпеки, а якщо це збирання (відповідно і обробка) відбувається зі злим умислом, є небезпекою для інформації.

Висновки. Проведене дослідження дає підстави для висновку, що низька правова культура громадян щодо власних персональних даних, неефективна система державного захисту цих даних та застосування Російською Федерацією технологій гібридної війни проти України призводить до неналежної інформаційної безпеки України. Подальше удосконалення комплексної системи державної інформаційної безпеки повинно включати в себе вивчення та імплементацію європейського досвіду у цій сфері. Прикладом є «Пакет захисту даних» (нові правила і порядок захисту персональних даних, затверджені Європейським Парламентом і Радою ЄС у травні 2016 року), який передбачає створення умов забезпечення потужної структури захисту персональних даних у Європейському Союзі.

Ключові слова: персональні данні, збирання, інформаційна безпека, адміністративний, правовий, аспект

Вступ

Початок третього тисячоліччя ознаменувався бурхливим розвитком інформаційних технологій. Проте такий розвиток має, окрім позитивного впливу на суспільне життя, ще й негативний – інформаційна безпека опинилася під загрозою. Вказані процеси створили більші можливості для збору, обробки та використання персональних даних. Інформація використовується як інструмент скоєння правопорушень, також активно використовується в політиці і ведені інформаційних війн. На сьогодні саме персональні дані та інформація є знаряддям гібридної війни Російської Федерації проти нашої держави. Ефективність системи захисту персональних даних та взагалі інформаційної безпеки забезпечується правовими інструментами,зокрема імплементації міжнародних та європейських стандартів захисту персональних та діяльністю уповноважених органів у цій сфері. Окрім цього, не менш важливим фактором інформаційної безпеки є рівень правової культури та обізнаність громадян у цих питаннях.

Вивченням проблематики збирання персональних даних та інформаційної безпеки з позиції адміністративного права вивчали провідні науковціО.О. Золотар (2018 рік)[1], А.Ю. Нашинець-Наумова (2017 рік) [2], Т. С. Перун[3](2019 рік), А. Ю.Щербіна (2020 рік) [4]. Проте, сьогоденний стан теоретико-практичного забезпечення адміністративно-правового режиму інформаційної безпеки в Україні, не в повній мірі відповідає вимогам ситуації, що склалася у зв'язку з веденням Російською Федерацією війни проти України.

Мета роботи

Метою цієї статті є аналіз адміністративно-правових поглядів на проблему збирання персональних даних та забезпечення інформаційної безпеки в Україні, а також перспектив удосконалення інформаційної безпеки в умовах гібридної агресії Російської Федерації. Для досягнення вказаної мети було поставлено завдання: проаналізувати наявні наукові розробки і стан чинного законодавства у сфері збирання персональних даних та забезпечення інформаційної безпеки в Україні; виявити проблемні аспекти та надати пропозиції щодо вдосконалення системи інформаційної безпеки.

Методи дослідження

При проведенні наукового дослідження та розв'язанні поставлених завдань було використано загальнофілософські, загальнонаукові та спеціальні методи дослідження. Під час дослідження було використано такі загальнофілософські методи, як діалектика та формальна логіка. Використання системного загальнонаукового методу дало змогу визначити системно-структурні елементи інформаційної безпеки й окреслити напрямки вдосконалення у цій сфері. Із спеціальних методів використано формально-юридичний, який сприяв якісному аналізу нормативного та наукового матеріалу.

Результати

Проблема адміністративно-правового регулювання процесу збирання персональних даних, забезпечення інформаційної безпеки як фізичних, так і юридичних осіб зараз стоїть дуже гостро. В Україні не вироблено ефективних механізмів всеохоплюючої інформаційної безпеки, нормативно-правові акти в цій сфері є недосконалими, права людини на захист персональних даних постійно порушуються.

Дослідження адміністративно-правових аспектів «збирання персональних даних» та «інформаційної безпеки» розпочнемо з аналізу цих понять та їх співвідношення.

Так, у частині 1 стаття 12 Закону України «Про захист персональних даних» [5] визначено, що «збирання персональних даних є складовою процесу їх обробки, що передбачає дії з підбору чи впорядкування відомостей про фізичну особу». Також у Законі вказано, що «збір персональних даних, як однієї з дій по обробці персональних даних, може здійснюватися у сукупності з її реєстрацією, накопиченням, зберіганням, адаптуванням, зміною, поновленням, використанням і поширенням (розповсюдженням, реалізацією, передачею), знеособленням, знищенням цих даних, у тому числі з використанням інформаційних (автоматизованих) систем» [5].

У свою чергу, згідно з цим же Законом «персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована».

А. В. Щербіна та П. В. Макушев зазначають, що поділ персональних даних необхідно здійснити на загальну та спеціальну категорію персональних даних. До першої віднести такі дані як прізвище, ім'я, побатькові, дата і місце народження, освіта, професія тощо. До другої категорії слід віднести особливі персональні відомості: стан здоров'я, відбитки пальців, записи голосу, ідентифікаційні коди та номери, відомості про судимість, етнічна приналежність, відношення до релігії[6, с. 75].

З цією точкою зору не можна не погодитись, тому що загальні персональні дані передаються до суб'єктів владних повноважень під час отримання адміністративних послуг і потребують меншого захисту з боку держави, на відміну від спеціальних, до яких треба застосовувати більш суттєві заходи захисту.

У частині 2 статті 32 Конституції України вказано: «Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини»[7], тобто в Основному Законі фігурує поняття «конфіденційної інформації про особу». Проте в Законі України «Про захист персональних даних» визначення конфіденційної інформації відсутнє.

Саме «інформаційна безпека» згадується у великій кількості нормативно-правових актів, зокрема в Доктрині інформаційної безпеки[8], проте його визначення відсутнє. Для його розуміння звернемось до наукових роздумів учених у цій сфері.

Під інформаційною безпекою В. С. Цимбалюк, А. В. Бабінська розуміють «стан захищеності її національних інтересів в інформаційній сфері, що визначаються сукупністю збалансованих інтересів особи, суспільства та держави» [9].

На думку Л. О. Кочубей, «інформаційна безпека – це такий стан захищеності життєво важливих інтересів, а отже, й інформаційної озброєності держави, суспільства, особистості, за якого жодні інформаційні впливи на них неспроможні викликати деструктивні думки і дії, що призводять до негативних відхилень на шляху стійкого прогресивного розвитку названих суб'єктів» [10, с. 221-222].

Для конкретизації поняття «інформаційна безпека», доцільно погодитися з думкою О. Г. Яреми та С. С. Єсімова, що принциповим «є визначення інформаційної безпеки як самостійного правового утворення, оскільки має власну складну структуру, що охоплює інститут віднесення інформації до категорії з обмеженим доступом, інститут захисту інформації та ліцензування цієї діяльності, а також інститут відповідальності за правопорушення в інформаційній сфері. Структурна складність пояснюється предметною безліччю правовідносин, що виникають під час забезпечення захищеності інтересів особистості, суспільства та держави в інформаційній сфері» [11, с. 247- 248].

Т.С. Перун, розглядаючи інформаційну безпеку як об'єкт адміністративно-правової охорони, вказав на те, «що вона є не тільки станом захищеності, а й системою суспільних відносин, які сприяють виникненню стану захищеності або безпеки. Водночас, під інформаційною безпекою доцільно розуміти сукупність суспільних відносин, що складаються в процесі захисту конституційних прав і свобод від внутрішніх і зовнішніх загроз в інформаційній сфері» [3, с. 34].

Можливість захисту персональних даних є одним з основоположних конституційних прав людини. Сьогодні життя людини пов'язане з наданням інформації про себе державним органам, установам, організаціям, приватним підприємствам, це, з одного боку, спрощує реалізацію інформаційних прав громадян, з іншого – великий ризик несанкціонованого втручання в особисте життя людини і неправомірне використання персональних (конференційних) даних особи.

Збір інформації може відбуватися як із дозволу власника персональних даних: заповнення інформації для отримання дисконтних карт торгівельних мереж, надання довідок в різні інстанції, автоматичний збір

персональних даних у соціальних мережах. Так і без отримання такого дозволу «в інтересах національної безпеки, економічного добробуту та прав людини» (ч. 6 ст. 6 Закону України «Про захист персональних даних»[5]).

Проте, головним фактором у процесі збору, зберігання та обробки даних є захист прав і свобод людини та дотримання принципів:

– невтручання в особисте життя під час обробки персональних даних;

– необхідності «обробки лише в цілях законних інтересів, переслідуваних контролером чи третьою стороною або сторонами, для яких надаються дані, крім випадків, коли над такими інтересами переважають інтереси основних прав і свобод суб'єкта даних»[5].

Збирання персональних даних з порушенням законодавства щодо захисту персональних даних призводить до негативних наслідків: агресивний маркетинг («спам», повідомлення про рекламні акції), так і випадки масштабних витоків персональних даних. Яскравим прикладом є гучний скандал із діджиталізацією та додатком «Дія» у квітні 2020 року, коли у «Telegram» з'явивсяпрофіль «Ua Baza BOT», котрий торгував базою водійських посвідчень, комбінованою із даними вседержавних сервісів із мобільними телефонами, реквізитами банківських карток та паролями соцмереж [12]. Частина експертів під час обговорювання цього питання наполягали, що витік інформації стався з баз даних МВС України.

Саме, у статті 25 Закону України «Про Національну поліцію», у частині 2 вказано, що «поліція в рамках інформаційно-аналітичної діяльності:1) формує бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України;2) користується базами (банками) даних Міністерства внутрішніх справ України та інших органів державної влади;-3) здійснює інформаційно-пошукову та інформаційно-аналітичну роботу;4) здійснює інформаційну взаємодію з іншими органами державної влади України, органами правопорядку іноземних держав та міжнародними організаціями»[13].

Тому зазначимо, що збір персональних даних, у разі його здійснення у відповідності до Закону, є позитивною складовою інформаційної безпеки, а якщо це збирання (відповідно і обробка) відбувається зі злим умислом, є небезпекою для інформації.

Ще одним небезпечним аспектом «застосування Російською Федерацією технологій гібридної війни проти України». «Саме проти України Російська Федерація використовує найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України» [8].У 2017 році Служба безпеки України встановила, що менеджмент компанії «Яндекс Україна» незаконно збирав, накопичував та передавав до Росії персональні дані українських громадян, а саме: особисті дані, рід занять, спосіб життя, місця перебування, проживання, роботи, дозвілля, джерела та розміри доходів, номери телефонів, електронних адрес та акаунтів у соціальних мережах. Зокрема, передавались дані співробітників правоохоронних та спеціальних органів, військовослужбовців Збройних Сил України, інших підрозділів, які беруть участь в антитерористичній операції на сході України, працівники органів державної влади та управління. «За даними СБУ, інформація передавалась спеціальним службам РФ для планування, організації та проведення розвідувальних, диверсійних, інформаційно-підривних операцій в нашій країні на шкоду суверенітетові України, територіальній цілісності та недоторканості» [14].

Реальний стан захисту персональних даних в Україні аналізувався Національним інститутом стратегічних досліджень при Президентові України, та було отримано наступні висновки:

– «сучасні інформаційно-комунікаційні технології активно сприяють постійному збільшенню обсягів та несанкціонованому поширенню персональних даних громадян, які обробляються, у т.ч. без їх відома;

– сучасна модель не дає жодних гарантій захисту персональних даних;

– пересічні громадяни демонструють байдужість до власних персональних даних і недостатній рівень розуміння необхідності їх захисту;

– стрімко поширюється прірва між безпрецедентними можливостями сучасного Інтернет-середовища і традиційними, «доцифровими» юридичними нормами і практиками, базованими на традиційному уявленні про межі й засоби забезпечення приватності життя людини»[15].

Загалом, за оцінками В.Г.Пилипчук таВ.М. Брижко, «у сфері захисту персональних даних в Україні головна проблема нині полягає у відсутності ефективної загальнодержавної системи захисту персональних даних, належного організаційно-правового механізму регулювання відносин та відповідальності за здійснення правопорушень у цій сфері»[16, с. 10]. Також можна додати, що принцип балансу інтересів особи, суспільства та держави в інформаційній сфері законодавчо в Україні дотепер не визначений.

Нашинець-Наумова А.Ю. зазначає, що «інформаційна безпека України є однією зі складових національної безпеки України та впливає на захищеність національних інтересів України в різних сферах життєдіяльності суспільства і держави»[2, с. 93].

Як справедливо визначає у своїй дисертації О.О. Золотар:«Інформаційна безпека в якості ключової складової національної безпеки охоплює напрями: забезпечення захисту інформаційного простору, що підтримує справедливий розподіл благ і ресурсів; сприяння процесу переходу до стійкого розвитку світового інформаційного середовища, що формується; стан захищеності культурного генофонду людства в умовах глобалізації»[1, с. 36-37].

Т.С. Перун у своїй дисертації вказує, що «в останні десятиліття інформація набуває властивостей потужного засобу впливу на суспільно-політичні, ідеологічні та соціально-економічні процеси, стає свого роду зброєю, яке вимагає створення системи протидії, захисту інформаційних ресурсів, що належать державним органам, що становлять державну, лікарську, особисту і ніші види таємниць»[3, с. 27].

Наведені приклади щодо незаконного збору та використання персональних даних не переконують людей не залишати особисті дані про себе, не будучи впевненими в дотримання безпеки цієї інформації. Тому державний контроль за дотриманням правил збору, зберігання та захисту персональної інформації повинен враховувати всі сучасні тенденції, проте без порушення прав та свобод громадян.

Державним органом, який наділений повноваженнями щодо захисту персональних даних, є Департамент з питань захисту персональних даних Секретаріату Уповноваженого Верховної Ради України з прав людини[17], основним завданням якого є «забезпечення реалізації повноважень Уповноваженого Верховної Ради України з прав людини зі здійснення парламентського контролю за дотриманням прав людини і громадянина та вимог законодавства у сфері захисту персональних даних, а також здійснення нормативно-правового забезпечення, організація та участь у здійсненні нормопроектувальної роботи у цій сфері»[17].

Також 19 березня 2021 року з метою «протидії поточним і прогнозованим загрозам національній безпеці та національним інтересам України в інформаційній сфері, забезпечення інформаційної безпеки України, ефективної протидії пропаганді, деструктивним дезінформаційним впливам та кампаніям, недопущення маніпулювання громадською думкою», указом Президента України у складі Ради національної безпеки і оборони України було створено Центр протидії дезінформації [18].

Висновки

Проведене дослідження дає підстави для висновку, що низька правова культура громадян щодо власних персональних даних, неефективна система державного захисту цих даних та застосування Російською Федерацією технологій гібридної війни проти України призводить до неналежної інформаційної безпеки України. Подальше удосконалення комплексної системи державної інформаційної безпеки повинно включати

в себе вивчення та імплементацію європейського досвіду у цій сфері. Прикладом є «Пакет захисту даних» (нові правила і порядок захисту персональних даних, затверджені Європейським Парламентом і Радою ЄС у травні 2016 року), який передбачає створення умов забезпечення потужної структури захисту персональних даних у Європейському Союзі.

Зазначені питання потребують додаткових наукових дискусій в аспекті розвитку адміністративно-правового забезпечення захисту персональних даних та інформаційної безпеки в умовах формування Національного безпекового простору.

Література

1. Золотар О. О. Правові основи інформаційної безпеки людини : дис…доктора юрид. наук. 12.00.07. Київ,Харків, 2018.- 499 с.

2. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ, 2017. 168 с.

3. Перун Т. С. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні: дис…канд. юрид. наук. 12.00.07. Львів, 2019. 268 с.

4. Щербина А.О. Адміністративно-правове регулювання використання персональних даних суб'єктами владних повноважень в Україні: дис…. канд. юрид. наук. 12.00.07. Запоріжжя, 2020. 232 с.

5. Про захист персональних даних : Закон Українивід 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення 15.04.2021).

6. Щербіна А.В., Макушев П.В. Поняття персональних даних та загальні правові засади їх використання: іноземний досвід. *Право і суспільство*. 2013. № 2. С. 70-76.

7. Конституція України від 28 червня 1996 р. № 254к/96-вр. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення 14.04.2021).

8. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: указ Президента України від 25 лютого 2017 року№ 47/2017. URL: https://www.president.gov.ua/documents/472017-21374(дата звернення 14.04.2021).

9. Цимбалюк В. С., Бабінська А. В. Правове регулювання інформаційної безпеки в Україні: проблеми теорії та практики. *Адміністративне право і процес*. 2014. № 2 (8). URL. http://applaw.net/index.php/journal/article/download/418/365/ (дата звернення 12.04.2021).

10. Кочубей Л.О. Інформаційна безпека держави: інструменти захисту українського інформаційного поля (на прикладі особливостей інформаційно-комунікаційних технологій у сучасному Донбасі. *Наукові записки Інституту політичних і етнонаціональних досліджень імені І. Ф. Кураса*. 2015. Вип. 3.- С. 220-237.

11. Ярема О. Г., Єсімов С. С.. Предмет правового забезпечення інформаційної безпеки в інформаційному праві. *Науковий вісник Львівського державного університету внутрішніх справ*. 2016. № 2. С. 244-252.

12. Додаток «Дія» звинуватили у «зливі» персональних даних українців. Влада заперечує. URL: https://www.bbc.com/ukrainian/news-52636988 (дата звернення 14.04.2021).

13. Про Національну поліцію: Закон України від 02.07.2015 № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text (дата звернення 14.04.2021).

14. СБУ: «Яндекс» передав персональні дані українців спецслужбам РФ. URL: https://www.pravda.com.ua/news/2017/05/29/7145337/(дата звернення 13.04.2021).

15. Гнатюк С.Л. Особливості захисту персональних даних у сучасному кіберпросторі : правові та техніко-технологічні аспекти : аналітична доповідь. Київ, 2014. С. 52-55. URL: //www.niss.gou.ua/content/articles/druk_Gnatuk 1/indd-8b6f2pdf.

16. Пилипчук В.Г., Брижко В.М. Реформування і розвиток системи захисту персональних даних в Україні. *Інформація і право*. 2017. № 3(22). С. 5-20.

17. Інформація про Департамент у сфері захисту персональних даних. URL: https://www.ombudsman.gov.ua/ua/page/zpd/info/ (дата звернення 14.04.2021).

18. Про рішення Ради національної безпеки і оборони України від 11 березня 2021 року «Про створення Центру протидії дезінформації»:указ Президента України від 19 березня 2021 року№ 106/2021. URL: https://www.president.gov.ua/documents/1062021-37421 (дата звернення 14.04.2021).

PERSONAL DATA COLLECTION AND INFORMATION SECURITY: ADMINISTRATIVE AND LEGAL ASPECT

Introduction. The beginning of the third millennium was marked by the rapid development of information technology. However, information is used as a tool for committing offenses, is also actively used in politics and information wars, in particular, is an instrument of hybrid war of the Russian Federation against our state. The current state of theoretical and practical support of the administrative and legal regime of information security in Ukraine does not fully meet the requirements of the security situation.

Aim. The aim of the article is to analyse the administrative and legal views on the problem of personal data collection and information security in Ukraine, as well as prospects for improving information security in the context of hybrid aggression of the Russian Federation. The following objectives were set to achieve this aim: analyse the existing scientific developments and the current legislation in the field of personal data collection and information security in Ukraine; identify problematic aspects and provide suggestions for improving the information security system.

Results. Scientific developments and the state of the current legislation on personal data collection and information security in Ukraine were analysedin the course of the research. From the standpoint of administrative law, the concepts of "collection of personal data" and "information security" and their relationship were studied.

It was found that the definition of "information security" is missing in the legal framework of the state. As well as the fact that the concept of "personal data" does not correlate with the concept of "confidential personal information" contained in the Constitution of Ukraine.

The existing problems in ensuring the security of personal data and the reasons for the identified shortcomings in information security of Ukraine were also analysed.

Two forms of personal data collection are considered: with consent and without consent. It is emphasized that the main factor in the process of data collection, storage and processing is the protection of human rights and freedoms.

It is noted that the collection of personal data, in case it is carried out in accordance with the Law, is a positive component of information security, and if this collection (andfurther processing) has malicious intent is insecure to information.

Conclusions. The conclusion is drawn that the low legal culture of citizens regarding their own personal data, inefficient system of state protection of these data and the use of hybrid warfare technologies against Ukraine by the Russian Federation leads to inadequate information security of Ukraine. Further improvement of the integrated system of state information security should include the study and implementation of European experience in this field. An example is the Data Protection Package (new rules and procedures for personal data protection, approved by the European Parliament and the Council of the EU in May 2016), which provides for the creation of a strong framework for personal data protection in the European Union.

Keywords: personal data, collection, information security, administrative, legal, aspects.