УДК 342.951
DOI https://doi.org/10.32782/2524-0374/2022-9/77

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В УМОВАХ ВОЄННОГО СТАНУ

PERSONAL DATA PROTECTION IN THE CONDITIONS OF MARTIAL LAW

Кравчук В.О., аспірант кафедри конституційного і адміністративного права
Національний авіаційний університет

У статті висвітлено основні аспекти захисту персональних даних в умовах воєнного стану, запровадженого внаслідок збройної агресії Російської Федерації проти України. Наголошено на тому, що гібридна війна, яка включає в себе постійне застосування ворогом засобів негативного інформаційного впливу на українське суспільство, у тому числі «викрадення» персональних даних, триває ще з 2014 року. Персональні дані – це інформація, за якою ідентифікується особа, її місце проживання, паспортні дані, матеріальний стан, місце народження, номер телефону тощо. Головним джерелом відритих персональних даних у сучасному інформаційному суспільстві стали соціальні мережі, при реєстрації в яких людина приймає рішення про оприлюднення тих чи інших персональних даних.

Проаналізовано правове регулювання захисту персональних даних в Україні. Зазначено, що правовий режим воєнного стану допускає обмеження певних конституційних прав громадян в інтересах держави. Встановлено, що відповідно до конституційних норм обмеження права на конфіденційність персональних даних допускається в інтересах національної безпеки. Охарактеризовано базовий нормативно-правовий акт у сфері захисту персональних даних – Закон України «Про захист персональних даних». Визначено, що зміни, внесені до Закону, під час воєнного стану, звужують обсяг права особи на конфіденційність персональних даних, проте такі зміни є прикладом обмеження права в інтересах особи, а не держави.

Встановлено, що у воєнних умовах виникли нові та ускладнилися попередні види правопорушень у досліджуваній сфері, наведено основні приклади таких правопорушень. Глобальною проблемою, яка не оминула навіть найбільш розвинені країни світі, залишається відсутність дієвих універсальних заходів з протидії кібератакам на державні бази даних. У відповідь на вказаний виклик Україна активно залучає до оборони національної безпеки ІТ-фахівців, що слід визнати позитивним кроком на шляху до забезпечення захисту персональних даних в умовах воєнного стану. Наголошено на тому, що особливу небезпеку становлять порушення захисту персональних даних осіб, що проживають на територіях, тимчасово окупованих державою-агресором. Зроблено висновок, що вирішальну роль у захисті персональних даних відіграє держава, проте не менш важливим є усвідомлення індивідами значення інформації для розвитку суспільних процесів.

Ключові слова: інформація, персональні дані, захист персональних даних, конфіденційність, воєнний стан.

The article highlights the main aspects of personal data protection in the conditions of martial law introduced as a result of the armed aggression of the Russian Federation against Ukraine. It was emphasized that the hybrid war, which includes the constant use by the enemy of means of negative information influence on Ukrainian society, including the «theft» of personal data, has been going on since 2014. Personal data – is information that identifies a person, their place of residence, passport data, financial status, place of birth, phone number, etc. The main source of open personal data in the modern information society has become social networks, upon registration in which a person makes a decision on the publication of certain personal data.

The legal regulation of personal data protection in Ukraine was analyzed. It is noted that the legal regime of martial law allows the restriction of certain constitutional rights of citizens in the interests of the state. It was established that, in accordance with the constitutional norms, the limitation of the right to the confidentiality of personal data is allowed in the interests of national security. The basic legal act in the field of personal data protection – the Law of Ukraine «On the Protection of Personal Data» is characterized. It was determined that changes made to the Law during martial law narrow the scope of a person's right to privacy of personal data, but such changes are an example of limiting the right in the interests of the person, not the state.

It has been established that new types of offenses in the researched area have arisen and become more complicated in wartime conditions, and the main examples of such offenses are given. A global problem that has not escaped even the most developed countries of the world is the lack of effective universal measures to counter cyberattacks on state databases. In response to this challenge, Ukraine actively involves IT specialists in the defense of national security, which should be recognized as a positive step on the way to ensuring the protection of personal data in the conditions of martial law. It was emphasized that violations of the protection of personal data of persons living in the territories temporarily occupied by the aggressor state pose a particular danger. It was concluded that the state plays a decisive role in the protection of personal data, but it is equally important for individuals to realize the importance of information for the development of social processes.

Key words: information, personal data, protection of personal data, confidentiality, martial law.

Постановка проблеми. Від 24 лютого 2022 року в Україні запроваджено воєнний стан внаслідок збройної агресії Російської Федерації (далі – РФ) проти України [1]. Гібридна війна, яка включає в себе постійне застосування ворогом засобів негативного інформаційного впливу на українське суспільство, у тому числі погрози «викрадення» персональних даних, триває ще з 2014 року. Наше сьогодення зосереджене в інформаційному просторі, розвиток якого породжує різноманітні ризики недобросовісного відстежування та використання інформації щодо органів державної влади та волонтерських центрів. Сьогодні кожна особа має можливість створити чи надіслати певну інформацію, яка буде розповсюджена для широкого кола користувачів. Почастішали випадки, у яких особиста інформація стає інструментом цькування чи приниження особи на веб-сайтах або інших Інтернет-ресурсах. Наявність вільного доступу до засобів створення фейкової інформації потребує механізму захисту персональних даних кожного споживача Інтернет-ресурсів. Отже, у сучасних реаліях загострюється актуальність захисту персональних даних кожного громадянина України для захисту національної безпеки держави, а також особистої безпеки та морально-психологічного самопочуття людини.

Аналіз останніх досліджень і публікацій. Дослідженням проблеми захисту персональних даних надано багато уваги такими науковцями, як: О. Г. Рогова [2], В. О. Волосецький [3], О. Мервінський [4], М. Кравчук [5], В. М. Брижко [6], Ж. В. Удовенко [7] та іншими. У сучасній юридичній науці окреслено питання, пов'язані з теоретико-правовими особливостями персональних даних, захистом персональних даних в українському та європейському законодавстві. Водночас недостатньою розробленістю характеризується питання, пов'язане із усвідомленням громадянами значення захисту персональних даних у період існування загроз національної та інформаційної безпеки.

Метою статті є визначення особливостей захисту персональних даних в Україні в умовах воєнного стану.

Виклад основного матеріалу. Забезпечення захищеності персональних даних громадян під час воєнного

стану є першочерговим завданням для нашої держави, адже така інформація про особу може використовуватися проти неї, її честі та гідності, створювати загрозу для її безпеки. Крім того, захист персональних даних є одним із основоположних методологічних підходів до створення в державі демократичного адміністрування та запровадження найкращих європейських правових принципів і цінностей [2, с. 6].

Персональні дані включають у себе дані про людину, яка ідентифікована або може бути ідентифікована на основі цих даних (або додаткової інформації), що може потрапити до особи, яка контролює дані, а які містять виражене ставлення до такої людини, вказівку на певну мету, плани щодо цієї людини з боку особи, яка контролює дані, чи іншої особи [3, с. 149].

Персональні дані – це інформація, за якою ідентифікується особа, її місце проживання, паспортні дані, матеріальний стан, місце народження, номер телефону тощо. Будь-яка інформація про особу є конференційною і не може поширюватися без її згоди. Щодо відкритих персональних даних, то особа сама вирішує, чи оприлюднювати таку інформацію. До відкритих даних фізичної особи слід віднести ім'я особи, її вік та місце проживання. Головним джерелом відритих персональних даних у сучасному інформаційному суспільству стали соціальні мережі, при реєстрації в яких людина приймає рішення про оприлюднення тих чи інших персональних даних.

Разом з тим, варто погодитися з Т. П. Попович, яка визначає право на захист персональних даних в Інтернеті як втілення впевненості особи у охороні відомостей про неї. У контексті забезпечення права на захист персональних даних правові обов'язки покладаються передусім на державу. Держава повинна на законодавчому, інституціональному, організаційно-технічному рівнях забезпечити збереженість персональних даних, їх конфіденційність, за винятком законних і достатніх для цього цілей, передбачити режим обробки персональних даних, а також механізми отримання згоди від особи на обробку інформації про неї [8, с. 54].

Основними конфіденційними даними про конкретну фізичну особу є ідентифікаційний код платника податків, паспортні дані, код від банківської карти. Основними правилами використання такої інформації є недопущення 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 захисту прав людини. До конфіденційної інформації про фізичну особу також належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження [9].

У ст. 8 Конвенції про захист прав людини і основоположних свобод 1950 року, передбачено право кожного «на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції» [10]. При цьому органи державної влади не можуть втручатись у здійснення цього права, за винятком випадків, коли втручання здійснюється згідно із законом і є необхідним у демократичному суспільстві, в інтересах національної та громадської безпеки чи економічного добробуту країни, для запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або для захисту прав і свобод інших осіб.

Головним нормативно-правовим актом, що передбачає правове регулювання, спрямоване на захист персональних даних в Україні, є Конституція України [11]. Основний Закон передбачає, що кожна людина має право на повагу до гідності, право на свободу та особисту недоторканність. Правовий режим воєнного стану допускає обмеження певних конституційних прав громадян в інтересах держави. Згідно з ч. 2 ст. 32 Конституції обмеження права на конфіденційність персональних даних допускається в інтересах національної безпеки.

У зв'язку зі зростанням ролі інформації та інформаційно-комп'ютерних технологій ще у 2010 році назріла потреба створення рамкового нормативно-правового акта, що встановлював би вихідні основи захисту персональних даних в Україні. Таким документом став Закон України «Про захист персональних даних» [12]. Він регулює правові відносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних. Відповідно до Закону особа повинна знати мету обробки персональних даних та надати згоду на опрацювання даних, в законі вказана процедура відповідно до якої відбувається обробка персональних даних. Помилково вважати, що, якщо особа надала згоду на обробку персональних даних, вона не має претензій в разі їх поширення або неналежного використання, адже особа не може передбачити усі наслідки розповсюдження таких даних, у тому числі в Інтернет просторі.

У липні 2022 року Закон було доповнено ч. 2 ст. 30, у якій визначено, що в період воєнного стану та протягом 6 місяців після його припинення (скасування) розширено умови передачі персональних даних іноземним суб'єктам відносин, пов'язаних із персональними даними. Зокрема, встановлено, що така передача можлива, якщо вона необхідна для надання медичної допомоги та/або реабілітаційної допомоги із застосуванням телемедицини. Хоча вказані зміни звужують обсяг права особи на конфіденційність персональних даних, такі зміни є прикладом обмежень в інтересах особи, а не держави.

Для перевірки дотримання вимог щодо захисту персональних даних встановлена спеціальна процедура, яка регулюється Порядком здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних, затвердженим наказом Уповноваженого Верховної Ради України з прав людини від 08 січня 2014 р. № 1/02-14 [13]. Основними заходами контролю визначено проведення перевірок: планових, позапланових, виїзних та безвиїзних. Відповідно до Порядку, у разі виявлення порушення персональних даних, складається припис про їх усунення або протокол про адміністративне правопорушення.

Україна, яка прогресивно наближається до європейських стандартів, ухвалила Стратегію розвитку інформаційного суспільства в Україні, схвалену розпорядженням Кабінету Міністрів України від 15 травня 2013 року № 386. Одним із головних пріоритетів України є прагнення побудувати орієнтоване на інтереси людей, відкрите для всіх і спрямоване на розвиток інформаційне суспільство, в якому кожен міг би створювати і накопичувати інформацію та знання, мати до них вільний доступ, користуватися й обмінюватися ними, щоб надати можливість кожній людині повною мірою реалізувати свій потенціал, сприяючи суспільному й особистому розвитку та підвищуючи якість життя [14]. Відповідно до Стратегії на сьогодні в суспільства є доступ до всіх Інтернет-ресурсів, в яких особи зберігають, поширюють та створюють персональні дані. На нашу думку, цілі Стратегії розвитку інформаційного суспільства майже досягнені, проте проблема захисту особистої інформації не була розв'язана ще до початку воєнних дій на території України.

Також слід зазначити норми, відповідно до яких встановлюється відповідальність за порушення поводження із персональними даними. У ст. 182 Кримінального кодексу України («Порушення недоторканності приватного життя») передбачено відповідальність за незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконну зміну такої інформації [15]. Ст. 188-39 Кодексу України про адміністративні правопорушення («Порушення законодавства у сфері захисту персональних даних») також передбачено

відповідальність за низку порушень Закону України «Про захист персональних даних», зокрема за «недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних, що призвело до незаконного доступу до них або порушення прав суб'єкта персональних даних» [16].

У воєнних умовах виникли нові та ускладнилися попередні види правопорушень у досліджуваній сфері. Яскравими прикладами таких порушень є: умисне надання правоохоронним органам персональних даних особи і недостовірної інформації щодо співпраці такої особи з державою-агресором; «злиття» персональних даних військовослужбовців Збройних Сил України, журналістів, громадських активістів, членів їхніх родин з метою їх ідентифікації та подальшого переслідування пособниками держави-агресора; створення веб-сайтів з недостовірною інформацією щодо надання громадянам України матеріальної допомоги від держави або міжнародних організацій після заповнення ними анкет персональних даних з метою подальшого розповсюдження персональних даних тощо.

Найбільшою кількістю персональних даних володіє держава, яка повинна дотримуватися суворих правил щодо збереження, обробки інформації, поводження з нею. Глобальною проблемою, яка не оминула навіть найбільш розвинені країни світі, залишається відсутність дієвих універсальних заходів з протидії кібератакам на державні бази даних. Слід наголосити, що кібератаки є небезпечним інструментом ведення війни, який доводить свою ефективність і потребує залучення невеликої кількості ресурсів. У відповідь на вказаний виклик Україна активно залучає до оборони національної безпеки ІТ-фахівців, що слід визнати позитивним кроком на шляху до забезпечення захисту персональних даних в умовах воєнного стану.

Окремі аспекти захисту персональних даних, які можуть безпосередньо вплинути як на інтереси особи, так і на національні інтереси, стосуються інформаційному обігу на територіях, тимчасово окупованих державою-агресором. Люди, які опинилися у надважких психологічних, соціальних, фінансових умовах, потребують негайної допомоги, що спричиняє численні зловживання персональними даними. Зокрема, їх збір особами, які надають неправдиву інформацію щодо своєї волонтерської діяльності, для проведення незаконних референдумів і виборів, фальсифікації їхніх результатів.

Окрім ускладнення технічного захисту персональних даних та відображення новітніх способів такого захисту в нормативно-правовій базі, ефективним методом захисту персональних даних є проведення роз'яснювальної роботи серед українського населення щодо поводження з персональними даними на період воєнного стану. Усвідомлення громадянами можливих ризиків, загроз і наслідків сприятиме зниженню кількості випадків незаконного поводження з персональними даними. Отже, на нашу думку, роз'яснювальна робота повинна стосуватися наступних аспектів проблеми:

– особи повинні усвідомлювати значення згоди на обробку персональних даних під час реєстрації на вебсайтах і інших ресурсах та враховувати її положення щодо подальшого використання ресурсом наданих даних;

– для захисту важливої інформації в соціальних мережах чи в облікових акаунтах Google слід створювати надійні паролі;

– надважливу таємну інформацію не варто поширювати в Інтернет-просторі, оскільки передбачити витік інформації неможливо;

– під час листування у соціальних мережах не варто поширювати конфіденційні персональні дані, а саме інформацію щодо ідентифікаційного коду, паспортних даних, коду банківських карт.

Отже, питання захисту персональних даних набувають особливої актуальності не лише з огляду на епоху цифрових технологій, а й з огляду на ігнорування окремими суб'єктами міжнародного права загальноприйнятих гуманістичних цінностей. В умовах воєнного стану нових шляхів вирішення потребують протиріччя між відкритістю та конфіденційністю інформації, між приватними та публічними інтересами. У свою чергу право на захист персональних даних потребує особливого захисту від посягань, оскільки загостреність суспільних протиріч породжує нові види зловживань і порушень у цій сфері. Хоча вирішальну роль у захисті персональних даних відіграє держава, не менш важливим є суспільне усвідомлення значення інформації та вміння поводитися з нею.

ЛІТЕРАТУРА

1. Про введення воєнного стану в Україні : Указ Президента України від 24.02.2022 р. № 64. URL: https://www.president.gov.ua/documents/642022-41397 (дата звернення: 01.09.2022 р.)
2. Рогова О.Г. Захист персональних даних у законодавстві Європейського Союзу та України. *Теорія та практика державного управління*. 2011. Вип. 3. С. 464-471.
3. Волосецький В. О. Іноземний досвід правового регулювання захисту персональних даних. *Міжнародний науковий журнал «Інтернаука»*. 2016. № 12(1). С. 148-151.
4. Мервінський О. «Чутливі» персональні дані. Як вони захищені? *Юрінком Інтер*. 2018. URL: https://yurincom.com/legal_practice/analitychna_yurysprudentsiia/chutlyvi-personalni-dani-iak-vony-zakhyshcheni/ (дата звернення: 01.09.2022 р.)
5. Кравчук М. М. Міжнародний досвід правового регулювання захисту персональних даних в мережі Інтернет. *Наукові записки Інституту законодавства Верховної Ради України*. 2013. № 3. С. 123-126.
6. Брижко В.М. Захист персональних даних: реалії та практика сучасності. *Інформація і право*. 2013. № 3(9). С. 31-49.
7. Удовенко Ж.В. Сутність інформації про особисте життя та її види. *Paradigm of Knowledge*. 2014. № 1. URL: https://naukajournal.org/index.php/Paradigm/article/view/285 (дата звернення: 01.09.2022 р.)
8. Попович Т.П. Право особи на захист персональних даних в Інтернеті: теоретико-правові аспекти. *Аналітично-порівняльне правознавство*. 2021. № 2. С. 51-54.
9. Про інформацію : Закон України від 02.10.1992 р. № 2657XII . *Відомості Верховної Ради України*. 1992. № 48. ст. 650.
10. Конвенція про захист прав людини і основоположних свобод : Європейська конвенція з прав людини від 17.07.1997 р. URL: http://zakon4.rada.gov.ua/laws/show/995_004 (дата звернення: 01.09.2022 р.)
11. Конституція України від 28.06.1996 р. *Відомості Верховної Ради України*. 1996. № 30. ст. 141.
12. Про захист персональних даних : Закон України від 13.01.2011 р. № 2939-VI . *Відомості Верховної Ради України*. 2010. № 34. ст. 481.
13. Про затвердження документів у сфері захисту персональних даних : Наказ Уповноваженого Верховної Ради України з прав людини від 08.01.2014 р. № 1/02-14. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#n92 (дата звернення: 01.09.2022 р.)
14. Стратегія розвитку інформаційного суспільства в Україні : розпорядження Кабінету Міністрів України від 15.05.2013 р. № 386 р. *Урядовий кур'єр*. 2013. № 105.
15. Кримінальний кодекс України : Закон України від 05.04.2001 р. *Відомості Верховної Ради України*. 2001. № 5. Ст. 131.
16. Кодекс України про адміністративні правопорушення : Закон України від 18.12.1984 р. *Відомості Верховної Ради УРСР*. 1984. № 40. Ст. 1122.