КОНСТИТУЦІЙНЕ ТА АДМІНІСТРАТИВНЕ ПРАВО

DOI: 10.18372/2307-9061.70.18482
УДК 342.721(045)

І. М. Сопілко,
доктор юридичних наук, професор
ORCID ID: https://orcid.org/0000-0002-9594-9280

ОСОБЛИВОСТІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ТА ІНШОЇ ІНФОРМАЦІЇ ПІД ЧАС ЗБРОЙНИХ КОНФЛІКТІВ

Національний авіаційний університет
проспект Любомира Гузара, 1, 03058, Київ, Україна
E-mail: sopilko_i@ukr.net

Мета: *дослідити сутність персональних даних та особливості їх захисту у період дії режиму воєнного стану в Україні та надати рекомендації з приводу регулювання відповідних питань.* ***Методи дослідження:*** *дана наукова стаття була написана автором із залученням загальновизнаних методів наукового пізнання, а саме: аналітичного, формального, порівняльно-правового, системно-структурного та інших.* ***Результати:*** *досліджено поняття, суть, характеристики персональних даних та пов'язаних із ними категорій, вказано на проблеми забезпечення їх надійного захисту, надано пропозиції щодо подолання таких проблем шляхом вдосконалення національного законодавства, зокрема, шляхом перейняття європейського досвіду та гармонізації діючої нормативно-правової бази із стандартами ЄС.* ***Обговорення:*** *дискусія має місце у даному досліджені щодо особливостей правового регулювання захисту персональних даних під час повномасштабного вторгнення Російської Федерації в Україну та методів покращення рівня такого захисту в поточній ситуації.*

Ключові слова: *персональні дані; приватність; захист персональних даних; збройний конфлікт; правовий захист інформації; воєнний стан.*

Постановка проблеми та її актуальність. Як відомо, українці пройшли довгий та нелегкий шлях до трансформації в інформаційне суспільство, чому сприяли, серед іншого, глобалізація економіки, її цифровізація, а разом із нею - стрімкий розвиток технологій. Соціум отримав чимало переваг у зв'язку із зазначеним, але й стикнувся із серйозними проблемами, зокрема, у вигляді порушень прав людини. Відповідно, наразі, в епоху інформаційних технологій, досить проблемним правовим питанням є саме захист персональних даних фізичних осіб.

Актуальність даної проблематики є беззаперечною не тільки для України, але й для світу в цілому. Адже зазначені дані, у разі їх незахищенності, можуть бути використані зловмисниками з метою наживи, чи навіть в більш небезпечних цілях, що призведе, зокрема, до втрати коштів, чи навіть здоров'я або життя людини. Вказана персональна інформація охоплює різні види конфіденційних відомостей, а саме імена, адреси та місцезнаходження, дані документів, номери телефонів, банківські рахунки тощо. І для України, в яку Російська Федерація вчинила повномасштабне вторгнення, тема, що розглядається, є надактуальною, адже порушення захисту персональних даних людей - це загроза інформаційній безпеці країни, що є одним зі структурних елементів безпеки національної.

На жаль, сьогодні, під час дії воєнного стану в країні, українці нерідко стають адресатами погроз та переслідувань, жертвами шахраїв та навіть вбивць - і все це, зокрема, через недоско-

наліть системи захисту персональних даних. Адже останні - це не лише відомості про людину. Такі дані ми використовуємо повсякчасно та майже усюди, зокрема, на просторах Інтернет-мережі, до якої підключені наші мобільні пристрої. Саме тому витоки даних - не рідкість.

З урахуванням зазначеного достатньо уявити ситуацію, коли має місце виток персональних даних (як от логін-пароль) працівника оборонної структури країни: до яких наслідків це призведе? Як мінімум - до маніпуляції даними та несанкціонованого доступу зловмисника до важливої інформації. Відповідно, безпека держави опиниться під загрозою. Таким чином, захист персональних даних є питанням особливої важливості та актуальності для України, особливо в умовах воєнного стану та ворожих дій проти неї Росії.

Аналіз досліджень і публікацій з проблеми. Даній темі були присвячені роботи таких вітчизняних науковців як М. Блохін, О. Дяковський, О. Капля, В. Кравчук, В. Крижна, І. Кушнір, С. Онищенко, В. Світличний, Я. Худолєй; окремі аспекти захисту персональних даних були досліджені в роботах В. Філінович та інших.

Мета статті. Автор цього наукового дослідження ставить собі за мету розкрити суть і особливості поняття «персональні дані» та інших, пов'язаних із ним термінів, зробити розбір структурних елементів головного поняття, запропонувати рекомендації щодо удосконалення діючого законодавства та подолання прогалин у ньому з метою забезпечення адекватного рівня захисту персональних даних в період дії режиму воєнного стану в Україні.

Виклад основного матеріалу дослідження. Забезпечення високого рівня захисту персональних даних - важлива задача кожної держави, адже наразі в світі витоки даних та інші порушення у цій сфері трапляються щоденно. Відповідно, вказане впливає самим негативним чином на рівень життя в країні, особливо там, де економіка рухається по цифровим рейкам - недовіра та невдоволеність владою серед населення зростає. Як вже було зазначено, для України питання захисту персональних даних є актуальним, особливо в контексті повномасштабного вторгнення РФ, а тому аналіз сьогоденної ситуації та рекомендації щодо її покращення будуть надані в даному науковому дослідженні.

Щоб здійснити такий аналіз, необхідно надати визначення основним правовим категоріям. Україна рухається за євроінтеграційним вектором, а тому відповідні визначення варто перейняти у країн Європи. Так, персональними даними, відповідно до Статті 4(1) Загального регламенту захисту даних (від англ. General Data Protection Regulation, також - GDPR, далі - Регламент) є «будь-яка інформація, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати». Така особа, відповідно до Регламенту, є суб'єктом даних [1].

Дане визначення було взято за основу при розробці законодавства про захист персональних даних багатьох країн світу, тим не менш, деякі його елементи потребують уточнення, а саме:

- «будь-яка інформація» - тут йдеться про будь-які об'єктивні чи суб'єктивні відомості, які стосуються конкретного суб'єкта даних, в будь-якій якості та незалежно від технічного носія, на якому вони містяться [2]. В цьому визначенні вбачається деяка технологічна нейтральність;

- «що стосується» - Дж. Сіман вбачає в цьому вислові наявність мети, змісту або результату для встановлення того, чи «стосується» ця інформація конкретної людини [2]. Альтернативність зазначених умов передбачає, що певні дані можуть одночасно стосуватися різних персоналій, а тому все залежить від конкретних обставин;

- «яку ідентифіковано чи можна ідентифікувати» - йдеться про можливість відрізнити конкретну людину від групи інших людей за існуючим унікальним ідентифікатором, для цілей чого не потрібна додаткова ідентифікація. І навіть якщо такого ідентифікатора немає, але віргодіно, що його отримують, то і особа буде вважатися такою, яку можна ідентифікувати [3, с. 167];

- «фізична особа» - йдеться саме про живу людину, фізичну, а не юридичну особу; право на для визначення правосуб'єктності кожної такої особи гарантовано Загальною декларацією

прав людини, незалежно від місцезнаходження такої особи [4].

Щодо національного законодавства у відповідній сфері, то воно представлене, в першу чергу, Законом України «Про захист персональних даних» № 2297-VI (від 01.06.2010 р.). Відповідно до Статті 2 зазначеного нормативно-правового акту (далі - НПА) «відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована» становлять собою персональні дані [5]. Угода про співробітництво між нашою державою та Європейською організацією з питань юстиції у п. n Статті 1 містить аналогічне GDPR визначення персональних даних [6]. Україна також ратифікувала у 2010 році Страсбурзьку Конвенцію про захист осіб у зв'язку з автоматизованою обробкою персональних даних. Її положення (Стаття 2, п. а) щодо визначення головного концепту даного дослідження за своєю суттю співпадають із попередніми актами [7].

Отже, персональними даними слід вважати будь-яку інформацію, що допоможе відрізнити одну конкретну людину від інших, а саме: імена та прізвища, номери телефонів та адреси (фізичні та електронної пошти, IP) тощо. Але на визначення приналежності відомостей до персональних даних може впливати контекст й характеристик кожної окремої їх обробки.

Визначивши поняття головного концепту даного наукового дослідження, слід перейти до особливостей їх захисту під час воєнних конфліктів, особливо в період дії воєнного стану в Україні. Актуальність даного питання підкреслюють і представники академічних кіл, зокрема, В. Світличний наголошує на тому, що відповідний захист є пріоритетним завданням наших можновладців, адже від нього залежить як інформаційна безпека країни загалом, так і права та свободи українців [8, с. 227].

Сьогодні потенційними жертвами витоку та злому персональних даних є кожна людина, зокрема, як зазначає В. Філінович, держателі банківських карток, отримувачі пенсійних відрахувань та медичних послуг, вкладники банків, власники матеріальних активів тощо [9, с. 47]. Тобто кожен із нас є потенційною жертвою.

У період воєнного стану дане питання є особливо актуальним, адже відповідно до даних Держспецзв'язку, порівняно з 2022 роком, у 2023 році кількість кібератак збільшилась на майже 16% (2543 інцидентів) [10]. А, як відомо, обробка персональних даних має мати законні підстави, тому особливо у період дії правового режиму воєнного стану важливо забезпечити громадянам належний рівень захисту їхніх прав у відповідній сфері.

Вже згаданий Регламент ЄС, хоч ще і не діє в Україні, але є фундаментом для оновлення національного законодавства щодо персональних даних. В цьому контексті варто розглянути також Угоду про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони (далі - Угода про асоціацію), в Статті 15 якою зазначається, що відповідні сторони цього акту домовились співробітничати задля забезпечення належного рівня захисту персональних даних у відповідності до найвищих європейських та міжнародних стандартів. Таке співробітництво може передбачати також обмін інформацією та експертами. В ч. 2 Статті 129 також є вимога до кожної із Сторін про вжиття адекватних спеціальних заходів задля захисту права на приватне життя, зокрема у зв'язку з передачею персональної інформації [11]. А загадана вище Угода про співробітництво з питань юстиції вимагає від сторін гарантувати хоча б рівноцінний тому, про який йдеться у вищезазначеній Страсбурзькій Конвенції, Рішенні щодо Євроюсту й у Регламенті Євроюсту рівень захисту персональних даних [6].

Як зазначає Я. Худолєй, є такі особливості щодо взаємодії відповідних органів із персональними даними в умовах воєнного стану в Україні:

- право на їх обробку реалізується органами, що визначені у Законі «Про правовий режим воєнного стану»;

- діє по відношенню до конкретного набору даних й у межах повноважень зазначених владних суб'єктів;

- порядок, форма та строки обробки не мають бути надмірними [12, с. 78].

Наразі можна виділити наступні проблеми, які виникають у сфері захисту персональних даних, зокрема у воєнний час:

- відсутність адекватної технічної бази для захисту інформації захисту від несанкціонованого доступу;

- відсутність внутрішньо-робочої культури роботи із даними на підприємствах та в організаціях та широке недотримання вимог внутрішніх нормативних документів таких структур;

- відсутність посади або безпосередньо людини на ній, яка б відповідала за зберігання зазначеної інформації, як це передбачено у європейському законодавстві;

- серйозні прогалини у вітчизняному законодавстві та відчутні його недоліки у порівнянні із європейським.

Варто розуміти, що відповідно до Статті 32 Конституції України, людина не має зазнавати втручання в своє особисте і сімейне життя, в тому числі заборонено збирати, поширювати чи використовувати конфіденційні дані про особу без її на те згоди, інакше як задля забезпечення нацбезпеки, економічного добробуту та дотримання прав людини. Тим не менш, Стаття 64 Основного Закону дозволяє обмеження деяких прав і свобод людей, якщо в країні встановлено воєнний стан [13], що нині діє відповідно до Указа Президента України № 64/2022 (від 24.02.2022). Тобто де-юре обмеження прав по Статті 32 Конституції є законними.

Також вищезазначена Стразбурзька Конвенція у ч. 2 Статті 9 передбачає можливість відхилення від положень статей 5,6 та 8 (щодо якості та особливих категорій даних, а також додаткових гарантій для суб'єктів), якщо відповідне передбачено у законодавстві Сторони й є необхідним для захисту прав і свобод інших людей, державної і громадської безпеки та фінансових інтересів чи протидії кримінальними правопорушеннями [7].

Подібні положення містить і Стаття 26 Закону № 2297-VI; також у його Статті 11 окрім згоди суб'єкта даних на обробку, його інформація може оброблятися і такої без згоди. Більше того, навіть обробка так званих «особливо чутливих даних» (в т.ч. про расове, етнічне походження, сексуальну орієнтацію, біометрично-генетичні відомості тощо) дозволяється, відповідно до ч. 2 Статті 7 Закону про захист персональних даних, якщо відповідна обробка потрібна для виконання завдань оперативно-розшукової чи контррозвідувальної діяльності, а також боротьби з тероризмом чи щодо судового вироку. Єдина вимога в цьому випадку - державні органи, які проводять таку обробку, мають діяти суто в межах своїх повноважень за законом [5]. Таку вимогу ставить і ч. 2 Статті 19 Основного Закону [13].

Таким чином, в період дії режиму воєнного стану обробка даних може відбуватися навіть без погодження із суб'єктом таких даних, і це є законним. Тим не менш, важливо забезпечити відповідний захист відомостей, оброблюваних на законних підставах. Зокрема, це, перш за все стосується саме законної роботи з даними хоча б на одній із підстав, що зазначені в Статті 7 Закону № 2297-VI. Об'єм інформації, що оброблюється має відповідати меті обробки.

Важливо під час обробки діяти за принципами, що встановлені GDPR, а саме: законності, транспарентності та справедливості, мінімізації даних, обмеження мети їх збору та термінів зберігання, цілісності та конфіденційності, точності, а також підзвітності. На нашу думку, норми Регламенту в частині принципів є більш суворими, ніж вимоги Закону № 2297-VI, а тому саме їх варто взяти за основу обробки.

Дотримання норм законодавства щодо забезпечення надійного рівня інформаційної та кібербезпеки можна вважати основою при роботі із інформацією, в тому числі, із персональними даними. А тому важливо, щоб законотворці постійно працювали над покращенням нормативної бази у цій галузі, а уряди - над розробкою відповідних політик, що відповідають аналогічним політикам провідних країн світу, із запозиченням відповідного досвіду.

Не менш важливими є й неправові аспекти захисту персональних даних, особливо в період дії режиму воєнного стану, коли найбільше страждають вимушені переселенці, військові та члени їх родин, а також громадські активісти та представники ЗМІ. Серед таких аспектів слід,

перш за все, зазначити важливість фізичного захисту об'єктів інформаційної інфраструктури, що полягає у забезпеченні через технічні, організаційні та подібні заходи безпеки тих об'єктів, які містять дані [12, с. 77-78]. Основою такого є безпека приміщень, в яких розміщено відповідні інформаційна техніка та обладнання; важливо також забезпечити відповідне навчання персоналу і адекватне реагування на різні кіберінциденти [8, с. 230].

Як зазначає В. Світличний, важливе місце посідає розробка екстрених процедур реагування на інциденти, які покликані зменшити наслідки таких інцидентів та допомогти скоріше відновити роботу інформаційних та інших систем. До відповідних процедур він відносить, виявлення, класифікацію, аналіз та безпосереднє вирішення наявної проблеми. При якісній взаємодії можливо зменшити об'єм даних, що втрачаються та захистити людей від небажаних наслідків інцидентів. В умовах воєнного стану такі екстрені процедури під неусипним контролем, постійно піддаватися перевіркам на відповідність та дієвість, бути адаптованими до поточної ситуації в країні [8, с. 231].

Не менш важливим, на нашу думку, є міжнародне та регіональне співробітництво. Здійснюване з метою обміну досвідом у сфері захисту персональних даних, воно є пріоритетним для можновладців нашої країни не тільки в частині саме персональних данихз, але й для забезпечення інформаційної безпеки країни, що є невід'ємним елементом безпеки національної.

Наостанок варто зазначити також дуже важливий елемент у захисті персональних даних - особисту відповідальність. Саме ми, як субєкти даних маємо опікуватися своєю інформацією, слідкувати за її використанням та обробкою. Для цього варто ознайомитися із основами інформаційної та кібергігієни, а також ставитися до своїх даних як до матеріального активу, адже саме такі активи ми звикли захищати найсильніше.

Висновки. Правовий аналіз персональних даних та пов'язаних із ними категорій дав автору даного наукового дослідження дійти наступних висновків. По-перше, визначення персональних даних, що міститься у національному законодавстві та міжнародно-правових актах є прийнятним, але містить певні спірні моменти в частині його структурних елементів, зокрема словосполучення «будь-яка інформація».

По-друге, для України, що потерпає від зухвалих та підступних дій ворога, зокрема в інформаційному та кібернетичному просторі, захист персональних даних на достатньому рівні став необхідною умовою стабільності всієї інформаційної системи країни як невід'ємного елементу національної безпеки. Неможливість або недосконаліть забезпечення відповідного захисту в період дії режиму воєнного стану робить безпеку держави вразливою. Пол-третє, задля забезпечення відповідного захисту, важливо постійно оновлювати та вдосконалювати національний нормативно-правовий інструментарій у відповідній сфері, для чого варто перейняти досвід провідних країн світу та імплементувати європейські стандарти. У тому ж ключі мають розроблятися відповідні державні політики.

Щодо неправових методів захисту, то серед них виділється технічно-організаційний захист об'єктів інформаційної інфраструктури, міжнародне та регіональне співробітництво, залучення провідних установ та експертів для оперативного реагування на відповідні інциденти щодо даних, а також впровадити систему освітніх заходів населення задля підвищення його обізнаності у цій сфері.

Якісне та дієве забезпечення належного рівня захисту персональних даних - непростий та ресурсоємний процес. До нього варто залучити не лише профільні державні органи та представників юридичних кіл, але й відповідних технічних спеціалістів та іноземних фахівців.

Література

1. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квіт. 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних): Регламент Європ. Союзу від 27.04.2016 р. № 2016/679. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 12.03.2024).

2. Seaman J. GDPR: The difference between Personally Identifiable Information (PII) and Personal Data. *LinkedIn*. URL: https://www.linkedin.com/pulse/gdprthe-difference-between-personally-identifiable-jim-seaman (дата звернення: 12.03.2024).

3. Purtova N. From knowing by name to targeting: the meaning of identification under the GDPR. *International Data Privacy Law*. 2022. Т. 12, № 3. С. 163–183. URL: https://doi.org/10.1093/idpl/ipac013 (дата звернення: 12.03.2024).

4. Загальна декларація прав людини: Декларація Орг. Об'єдн. Націй від 10.12.1948 р. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text (дата звернення: 14.03.2024).

5. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI: станом на 27 жовт. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 14.03.2024).

6. Угода про співробітництво між Україною та Європейською організацією з питань юстиції: Угода Україна від 27.06.2016 р.: станом на 8 лют. 2017 р. URL: https://zakon.rada.gov.ua/laws/show/984_024-16#Text (дата звернення: 19.03.2024).

7. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних: Конвенція Ради Європи від 28.01.1981 р.: станом на 6 лип. 2010 р. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text (дата звернення: 19.03.2024).

8. Svitlychnyi V.A. Protection of personal data under martial law in Ukraine. *Law and Safety*. 2023. Vol. 90, No. 3. P. 226–236. URL: https://doi.org/10.32631/pb.2023.3.19 (date of access: 14.03.2024).

9. Filinovych V. Data breach and data leakage as pressing cybersecurity threats. *Information security of Ukraine: 30 years of independence*: monograph. Budapest, 2021. С. 40–71.

10. Жарикова А. Кількість кібератак у 2023 році зросла на 16% - Держспецзв'язку. *Економічна правда*. URL: https://www.epravda.com.ua/news/2024/01/31/709355/ (дата звернення: 15.03.2024).

11. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони: Угода Україна від 27.06.2014 р.: станом на 30 листоп. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/984_011#Text (дата звернення: 15.03.2024).

12. Khudoliei Y.H., Zahrebelna N.A. Protection of personal data during the period of martial law in Ukraine: general theoretical aspects. *Legal Bulletin*. 2023. Т. 84, № 8. С. 75–82. URL: https://doi.org/10.31732/2708-339x-2023-08-75-82 (дата звернення: 19.03.2024).

13. Конституція України: від 28.06.1996 р. № 254к/96-ВР: станом на 1 січ. 2020 р. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (дата звернення: 20.03.2024).

References

1. Rehlament Yevropeys′koho Parlamentu i Rady (YES) 2016/679 vid 27 kvit. 2016 roku pro zakhyst fizychnykh osib u zv'yazku z opratsyuvannyam personal′nykh danykh i pro vil′nyy rukh takykh danykh, ta pro skasuvannya Dyrektyvy 95/46/YES (Zahal′nyy rehlament pro zakhyst danykh): Rehlament Yevrop. Soyuzu vid 27.04.2016 r. № 2016/679. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (data zvernennya: 12.03.2024).

2. Seaman J. GDPR: The difference between Personally Identifiable Information (PII) and Personal Data. LinkedIn. URL: https://www.linkedin.com/pulse/gdprthe-difference-between-personally-identifiable -jim-seaman (data zvernennya: 12.03.2024).

3. Purtova N. From knowing by name to targeting: the meaning of identification under the GDPR. International Data Privacy Law. 2022. Т. 12, № 3. S. 163–183. URL: https://doi.org/10.1093/idpl/ipac013 (data zvernennya: 12.03.2024).

4. Zahal′na deklaratsiya prav lyudyny: Deklaratsiya Orh. Ob'yedn. Natsiy vid 10.12.1948 r. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text (data zvernennya: 14.03.2024).

5. Pro zakhyst personal′nykh danykh: Zakon Ukrayiny vid 01.06.2010 r. № 2297-VI: stanom na 27 zhovt. 2022 r. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (data zvernennya: 14.03.2024).

6. Uhoda pro spivrobitnytstvo mizh Ukrayinoyu ta Yevropeys′koyu orhanizatsiyeyu z pytan′ yustytsiyi: Uhoda Ukrayina vid 27.06.2016 r.: stanom na 8 lyut. 2017 r. URL: https://zakon.rada.gov.ua/laws/show/984_024-16#Text (data zvernennya: 19.03.2024).

7. Konventsiya pro zakhyst osib u zv'yazku z avtomatyzovanoyu obrobkoyu personal′nykh

danykh: Konventsiya Rady Yevropy vid 28.01.1981 r.: stanom na 6 lyp. 2010 r. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text (data zvernennya: 19.03.2024).

8. Svitlychnyi V.A. Protection of personal data under martial law in Ukraine. Law and Safety. 2023. Vol. 90, no. 3. P. 226–236. URL: https://doi.org/10.32631/pb.2023.3.19 (date of access: 14.03.2024).

9. Filinovych V. Data breach and data leakage as pressing cybersecurity threats. Information security of Ukraine: 30 years of independence: monograph. Budapest, 2021. S. 40–71.

10. Zharykova A. Kil′kist′ kiberatak u 2023 rotsi zrosla na 16% - Derzhspetszv″yazku. Ekonomichna pravda. URL: https://www.epravda.com.ua/news/2024/01/31/709355/ (data zvernennya: 15.03.2024).

11. Uhoda pro asotsiatsiyu mizh Ukrayinoyu, z odniyeyi storony, ta Yevropeys′kym Soyuzom, Yevropeys′kym spivtovarystvom z atomnoyi enerhiyi i yikhnimy derzhavamy-chlenamy, z inshoyi storony: Uhoda Ukrayina vid 27.06.2014 r.: stanom na 30 lystop. 2023 r. URL: https://zakon.rada.gov.ua/laws/show/984_011#Text (data zvernennya: 15.03.2024).

12. Khudoliei Y.N., Zahrebelna N.A. Protection of personal data during the period of martial law in ukraine: general theoretical aspects. Legal Bulletin. 2023. T. 84, № 8. S. 75–82. URL: https://doi.org/10.31732/2708-339x-2023-08-75-82 (data zvernennya: 19.03.2024).

13. Konstytutsiya Ukrayiny: vid 28.06.1996 r. № 254k/96-VR: stanom na 1 sich. 2020 r. URL: https://zakon.rada.gov.ua/laws/show/254k/96-vr#Text (data zvernennya: 20.03.2024).

Iryna Sopilko

FEATURES OF THE PROTECTION OF PERSONAL DATA AND OTHER INFORMATION DURING ARMED CONFLICTS

National Aviation University
Liubomyra Huzara, 1, 03680, Kyiv, Ukraine
E-mail: sopilko_i@ukr.net

Purpose: *to study the essence of personal data and the peculiarities of their protection during the period of martial law in Ukraine and to provide recommendations on the regulation of relevant issues.* ***Research methods:*** *this scientific paper was written by the author with the use of generally recognized methods of scientific knowledge, namely, analytical, formal, comparative-legal, systemic-structural, and the like.* ***Results:*** *the concept, essence, and features of personal data and related categories were analyzed, the problems of ensuring their reliable protection were pointed out, and proposals were made to overcome such difficulties by improving national legislation, in particular, by adopting European experience and harmonizing the current legal framework with EU standards.* ***Discussion:*** *the discussion takes place in this study regarding the peculiarities of the legal regulation of personal data protection during the full-scale invasion of the Russian Federation into Ukraine and methods of improving the level of such protection in the current situation.*

Key words: *personal data; privacy; protection of personal data; armed conflict; legal protection of information; martial law.*

Стаття надійшла до редакції 20.03.2024