УДК 340.1
DOI 10.31732/2708-339X-2023-08-65-74

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У ПЕРІОД ДІЇ В УКРАЇНІ ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ: ЗАГАЛЬНОТЕОРЕТИЧНІ АСПЕКТИ

Худолєй Я.Г.,
аспірант кафедри теорії та історії держави і права
Університету «КРОК»
вул. Табірна, 30-32, м.Київ, Україна, 03113,
e-mail: qwe1188@ukr.net
https://orcid.org/0009-0007-4024-7007

Загребельна Н.А.,
кандидат юридичних наук,
ВНЗ «Університет економіки та права «КРОК»,
вул. Табірна, 30-32, м.Київ, Україна, 03113,
e-mail:NataliaZa@krok.edu.ua
https://orcid.org/0000-0002-3390-7149

PROTECTION OF PERSONAL DATA DURING THE PERIOD OF MARTIAL LAW IN UKRAINE: GENERAL THEORETICAL ASPECTS

Khudoliei Ya.H.,
Postgraduate student of the Department of Theory and History
of the State and Law of «KROK» University.
Tabirna St., 30-32, Kyiv, Ukraine, 03113,
e-mail: qwe1188@ukr.net
https://orcid.org/0009-0007-4024-7007

Zahrebelna N.A.,
Ph.D. in Law, «KROK» University,
Tabirna St., 30-32, Kyiv, Ukraine, 03113,
e-mail:NataliaZa@krok.edu.ua
https://orcid.org/0000-0002-3390-7149

Анотація. *У статті проаналізовано сучасний стан та напрями розвитку захисту персональних даних в Україні в умовах воєнного стану. Це актуальна проблема сучасного періоду, оскільки країна не лише знаходиться в умовах активних воєнних дій, але й займається захистом прав своїх громадян на різних рівнях – інформаційному та державному.*

Потреби сьогодення в захисті громадян та їх законного права на недоторканість персональних даних є наріжним каменем для будь-якої цивілізованої, правової і демократичної країни. Через дію воєнного стану деструктивний вплив на захист персональних даних від знищення, втрати чи несанкційованої обробки постійно зростає, що додає важливості та обґрунтованості в подальшому дослідженні цього питання.

У статті визначено той факт, що, попри широкомасштабні бойові дії на фронті й те, що відбувається в тилу, права громадян на життя, свободу, гідність та недоторканість є основоположними в нашій країні. Вони повинні бути такими, які беззаперечно й безумовно дотримано всіма суб'єктами правовідносин, починаючи від державних органів чи військових структур і закінчуючи самими громадянами. Бо саме це є одним з головних критеріїв, що дозволять нам швидше інтегруватися до стандартів ЄС та НАТО й привести у відповідність загальнодержавну систему захисту персональних даних до сучасних вимог.

Стаття спрямована на розгляд та розкриття основних питань, пов'язаних з правовими аспектами захисту персональних даних під час воєнного стану, включаючи визначення обмежень прав і свобод людини, повноважень щодо обробки персональних даних, передачі даних, особистого захисту та захисту громадян від кіберзлочинів. Дослідження націлене на заповнення наукових прогалин у розкритті даної проблеми і надання теоретичного аналізу, що допоможе розширити розуміння та практичні рекомендації щодо захисту персональних даних під час дії воєнного стану в Україні.

Також авторами зазначено, що реалії воєнного стану потребують обмеження прав і свобод у межах та у спосіб, які визначено чинним законодавством в інтересах національної безпеки, добробуту, прав людини й громадянина.

***Ключові слова*:** *персональні дані, захист персональних даних, права та свободи, юридична відповідальність, система права, мережа Інтернету.*

Формул: *0, рис.: 0, табл.: 0, бібл.: 8.*

***Abstract**. The article analyzes the current state and directions of development of personal data protection in Ukraine under martial law. This is the current issue of the modern period, since the country is not only in the conditions of active military operations, but is also engaged in protecting the rights of its citizens at various levels - informational and state.*

Today's needs for the protection of citizens and their legal right to the inviolability of personal data are a cornerstone for any civilized, legal and democratic country. Due to martial law, the destructive impact on the protection of personal data from abolishment, loss or unauthorized processing is constantly increasing, which adds importance and validity to further research on this issue.

The article defines the fact that, despite the large-scale combat operations at the front line and what is happening in the rear, the rights of citizens to life, freedom, dignity and inviolability are fundamental in our country. They must be those that are undeniably and unconditionally observed by all entities of legal relations, starting from state bodies or military structures and ending with citizens themselves. Because this is one of the main criteria that will allow us to quickly integrate into EU and NATO standards and bring the national system of personal data protection into line with modern requirements.

The article is aimed at considering and revealing the main issues related to the legal aspects of personal data protection during martial law, including the definition of restrictions on human rights and freedoms, powers to process personal data, data transfer, personal protection and protection of citizens from cybercrimes. The research is aimed at filling the scientific gaps in the disclosure of this problem and providing a theoretical analysis that will help to expand understanding and practical recommendations regarding the protection of personal data during the martial law in Ukraine.

The authors also highlighted that the realities of martial law require the restriction of rights and freedoms within the limits and in the manner determined by the current legislation in the interests of national security, well-being, and human and citizen rights.

***Key words:** personal data, personal data protection, rights and freedoms, legal responsibility, legal system, Internet network.*

***Formulas**: 0, fig.: 0, tabl.: 0, ref.: 8.*

Постановка проблеми. Питання захисту персональних даних у теперішній час досить актуальне. Наша держава після верифікації Угоди про асоціацію з Європейським Союзом автоматично «стала на рейки» з демократичними державами в цьому аспекті. Для всебічного та правильного розвитку потрібно розробити й ухвалити нове законодавство в цій сфері. Першим кроком такого напрямку для удосконалення рівня захисту громадян та їх приватності стала розробка в 2021 році Законопроєкту №5628 «Про захист персональних даних». А вже 25 жовтня 2022 року Верховною Радою України задекларовано і зареєстровано більш досконалий Законопроєкт №8153, положення якого прямо адаптують чинну українську систему захисту персональних даних до міжнародних норм та стандартів і запроваджують певні нововведення, яких не було до цього.

Слід зазначити, що представлений Законопроєкт враховує особливості ситуації війни в нашій країні, тому деякі положення не є повністю відповідними «мирному» часу. Вони спрямовані на надання максимального рівня захисту персональних даних від передачі даних та кіберзлочинів. Встановлена обов'язкова вимога дозволяє органам державної влади розміщувати державні реєстри на іноземних ресурсах, що призвело до забезпечення цілісності й доступності даних, які знаходяться в цих реєстрах. Доступ до деяких реєстрів було зовсім закрито. Також цілком правильним та доцільним стало запровадження обмежень деяких конституційних прав і свобод людини й громадянина та прав і законних інтересів осіб із зазначенням строку дії цих обмежень, таких як:

- обмеження свободи переміщення: встановлення контролю над рухом осіб, обмеження на в'їзд та виїзд з певних територій, встановлення зон перебування;

- обмеження свободи зібрань та демонстрацій: заборона або обмеження проведення масових мітингів, демонстрацій, зокрема з метою забезпечення громадського порядку та безпеки;
- обмеження свободи слова: встановлення цензури, обмеження доступу до інформації, заборона розповсюдження певних матеріалів або висловлювань;
- обмеження права на приватність: проведення обшуків, перехоплення та моніторинг електронних комунікацій, збір і обробка персональних даних без належних гарантій приватності тощо.

Аналіз останніх досліджень та публікацій. Сучасники схиляються до думки про необхідність удосконалення нормативно-правової бази у питанні захисту персональних даних у мережі Інтернет. Один з представників, В. Брижко, висловлює думку, що варто вжити заходів для усунення передумов для порушень загальних прав на захист персональних даних та привести національне законодавство в цій галузі у відповідність [1, с. 42].

Досліджували ці питання також такі науковці, як: Ю. Базанов, О. Баранов, Ю. Гелич, О. Дмитренко, Є. Захаров, О. Заярний, А. Марущак, Р. Романов А. Тунік, А. Чернобай та інші.

Сучасним реаліям інституту захисту персональних даних і відповідних прав людини в умовах комерціалізації та цифровізації світу присвячені роботи А. Головченка, П. Діхтієвського, С. Єсімової, Т. Обуховської та ін.

Не вирішені раніше частини загальної проблеми. Як уже було зазначено, на початку розвитку питання захисту персональних даних в Україні було відсутнє належне регулювання. До 2011 року, коли було прийнято Закон України № 2997-VI «Про захист персональних даних», не існувало практичних норм, які б регулювали відносини в цьому питанні. Однак, навіть після прийняття Закону, не було належної реалізації його положень.

Відсутність практичних рекомендацій та регламентів щодо виконання норм Закону була однією з проблем, які існували тоді й продовжують існувати зараз. Мало хто був обізнаний та використовував електронні бази даних і реєстри, а також інші засоби, передбачені Законом. Поступово держава та посадові особи почали адаптуватися до нововведень.

Законодавство України в питанні захисту персональних даних потребує значного вдосконалення для його інтеграції з сучасними системами захисту, а також для його приведення у відповідність до вимог Конвенції 108 та інших норм і законів.

24 лютого 2022 року, із введенням військового стану, Україна перейшла до нового етапу в питанні захисту персональних даних. Поміж викликів, пов’язаних із військовою ситуацією, держава змушена стикатися з новими негативними факторами, зумовленими необхідністю захисту себе та громадян, їх конституційних прав у кіберпросторі. На нашу думку, важливо розробити своєрідний план дій для захисту персональних даних у сучасних умовах. Необхідно узагальнити та закріпити законодавчим шляхом такі питання:

1. Обмеження права на приватність громадян.
2. Визначення меж та повноважень осіб на всіх рівнях щодо обробки персональних даних.
3. Визначення всіх законних підстав передачі даних від їх власників до інших осіб.
4. Особистий захист персональних даних громадян від шахрайських дій та кіберзлочинів.
5. Захист громадян та виявлення загроз під час дії військового стану на окупованих територіях і загалом у країні.

Усі ці аспекти визначають актуальність досліджуваного питання як з погляду заповнення прогалин, що існували задовго до сьогоднішнього дня, так і з урахуванням нових значних викликів, що виникли протягом останніх майже двох років.

Формулювання цілей статті. Метою статті є визначення методів

захисту персональних даних особи у період дії в Україні правового режиму воєнного стану; а також розробка можливих дієвих засобів щодо дотримання прав і свобод людини та громадянина щодо цього питання в Україні.

Виклад основного матеріалу дослідження. Прагнення України до євроінтеграції вимагають упровадження змін у різних сферах національного, соціального та інших рівнів. Один з основних принципів права Європейського Союзу - це гарантування права на конфіденційність і захист персональних даних. У сучасних умовах, особливо під час воєнного стану, інформація є надзвичайно цінним ресурсом, навколо якого відбувається багато спекуляцій, обману та псевдопотреб. Наявність достовірної інформації (або її відсутність) формує загальне уявлення суспільства про реальність. Кожна особа є носієм персональної інформації й одночасно безпосереднім суб'єктом, що має право на захист своєї приватності та особистої недоторканості, гарантованих державою.

У сучасних умовах дії воєнного стану в Україні було внесено значну кількість змін і нововведень до чинного законодавства в цій сфері. Деякі з них є прогресивними заходами, спрямованими на майбутнє, тоді як інші виступають як засіб виправлення неузгоджених норм та невирішених проблем.

Проте варто пам'ятати, що існують загальні норми захисту, які тільки зазнають змін під впливом обставин. Основу законодавства, яке стосується захисту персональних даних, складає Закон України «Про захист персональних даних». У цьому Законі зазначено, що будь-які дії щодо персональних даних повинні бути обґрунтованими та базуватися на вільному волевиявленні особи, яка про це інформована (п. 1, 3 ч. 1 ст. 11). Закон визначає вичерпний перелік законних способів і підстав для обробки даних (п. 1, 3 ч. 1 ст. 11). Кожен суб'єкт має право відмовитися від надання своїх даних або відкликати дозвіл на їх обробку на певних законних підставах. В окремих випадках обробка даних може здійснюватися без особистої згоди респондента (п. 2 ч. 1 ст. 11 Закону), наприклад, при наданні публічної інформації чи адміністративних послуг.

В умовах воєнного стану збір та обробка персональних даних здійснюються згідно з п. 4 ч. 1 ст. 11 зазначеного Закону з метою захисту особливо важливих інтересів володільця цих даних. У такому випадку попередня згода не є обов'язковою. Проте, якщо є можливість отримати таку згоду в майбутньому, відповідний орган повинен звернутися до першоджерела з проханням про її надання.

Основними моментами при здійсненні збору, обробки та зберігання персональних даних суб'єктами владних повноважень на основі їх законодавчо визначених повноважень в умовах дії режиму воєнного стану є таке:

- право на обробку здійснюється органами, які визначені у Законі України «Про правовий режим воєнного стану»;
- не повинен бути перевищений строк, форма та порядок обробки даних;
- має діяти тільки щодо певного набору даних та в межах повноважень.

Відповідно до Указу Президента України № 64/2022 від 24.02.2022 року про введення воєнного стану Кабінет Міністрів України затвердив «План запровадження та забезпечення заходів здійснення правового режиму воєнного стану в Україні» від 24.02.2022 № 181 і визначив подальші дії та зміни в питаннях, що стосуються інформаційної безпеки громадян, наприклад, перевірки особистих документів й огляду речей і транспортних засобів громадян, а також їх житла та інших приміщень. Ці зміни дещо обмежили обсяг конституційних прав, проте їх упровадження було необхідним кроком для запровадження і виконання нових заходів державної безпеки.

Відповідно до п. 5 Постанови Кабінету Міністрів України «Про затвердження Порядку перевірки документів в осіб, огляду речей, транспортних засобів, багажу та вантажів, службових приміщень і житла громадян під час забезпечення заходів

правового режиму воєнного стану» від 29 грудня 2021 р. № 1456 [3] чітко визначено перелік компетентних органів щодо проведення перевірки документів громадян. А саме: Національна поліція, Служба безпеки України, Національна гвардія, Державна митна служба, підрозділи Збройних сил України (за наказом коменданта).

Для цих органів визначено перелік підстав проведення перевірок документів:

- за умови наявності в особи *зовнішніх ознак, схожих на ознаки особи, яка перебуває в розшуку чи є безвісно зниклою;*

- *за умови представлення достатніх доказів щодо наміру особи вчинити правопорушення, факту його вчинення, а також факту причетності до вчинення;*

- *незаконне перебування на об'єкті зі спеціальним режимом доступу;*

- *за наявності в особи боєприпасів, зброї, наркотичних чи інших речовин із забороненим або обмеженим обігом;*

- *перебування особи в місці вчинення правопорушення чи ДТП;*

- *порушення умов для території, де запроваджено режим воєнного стану.*

Якщо в особи, щодо якої проводиться перевірка відповідними органами, при собі будуть відсутні документи, що посвідчують її особу та підтверджують громадянство України, то до неї може бути застосовано спосіб примусу у вигляді затримання уповноваженою особою для встановлення її особистості на умовах, передбачених Кодексом України про адміністративні правопорушення.

*Але у будь-якому разі, незалежно від обмежень, що встановлені правовим режимом воєнного стану, переважна більшість способів отримання, обробки та зберігання персональних даних повинні базуватися на умовах добровільності й поінформованості. В іншому випадку можна вважати дані недостовірними, а їх використання неправомірним (*ч. 2 ст. 7 та ч. 1 ст. 13 Закону України «Про доступ до публічної інформації»*). Що стосується оприлюднення публічної інформації в період дії воєнного стану, то за ст. 6* Закону України «Про доступ до публічної інформації» це відбуваються лише:

- в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи кримінальним правопорушенням, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя;

- коли розголошення інформації може завдати істотної шкоди інтересам;

- коли шкода від оприлюднення інформації переважає суспільний інтерес.

Власник персональних даних несе презумпцію відповідальності за законне використання та збереження отриманих даних. Для забезпечення безпеки даних необхідно мати захищені автоматизовані системи зберігання і створити відповідні умови для повної інформованості щодо мети, підстав та умов передачі персональних даних стороннім особам. *Слід зазначити також, що потребують удосконалення процедури не лише збирання, а й ліквідації персональних даних. Тому слід окремо визначити їх перелік. Ними можуть бути: закінчення терміну зберігання чи обробки,* припинення правовідносин розпорядника персональних даних та володільця, а також наявність рішення суду про знищення даних.

Після набуття чинності 12.03.2022 року Постанови Кабінету Міністрів України «Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану» було заборонено для обробки даних використовувати центри обробки даних та хмарні середовища, розташовані на тимчасово окупованих територіях України. Навпаки, для забезпечення

додаткових гарантій безпеки і захисту даних, було рекомендовано перенести всі ресурси до закордонних центрів.

Не оминули змін і положення кримінально-процесуального законодавства. Набули чинності закони, що спрощують характер дій слідчих органів в умовах воєнного стану та розширюють повноваження відповідних органів щодо процедур огляду місця події, обшуку комп'ютерних систем доступу до даних. Відтепер огляд комп'ютерних систем дозволено проводити прокуратурою і слідчими органами за допомогою фото-, відеофіксації чи в паперовому вигляді. Такі слідчі дії можуть провадитися як за санкцією суду, так і без неї. За умови достатніх підстав у слідчого вважати, що об'єкти огляду та дані, які там знаходяться, мають прямий стосунок до кримінального провадження. Однак слід зазначити, що в новому Законопроєкті не визначено критеріїв доступу до даних. Наприклад, не закріплено як і який саме обсяг даних потребує вилучення, а сама процедура огляду потребує уточнень та доопрацювань.

По суті, єдиним способом щодо отримання даних з електронних носіїв, який використовується на практиці, є вилучення й їх арешт за ухвалою суду. За даними статистики, лише до 5% слідчих мають відповідні технічні знання та навички, щоб обійти системи захисту електронних носіїв чи коректно провести процедуру вилучення даних, необхідних для ведення провадження, а також організувати копіювання даних для передачі їх володільцю за вимогою.

У новому законодавстві також передбачено положення щодо зняття показань із камер спостереження, що встановлені в публічних місцях, без отримання особистої згоди особи, яка потрапила до запису. Проте, необхідно чітко прослідковувати та доводити зв'язок між конкретним кримінальним провадженням і самим записом, щоб використовувати його як доказовий матеріал.

Після введення правового режиму воєнного стану були внесені зміни, які дозволяють прокурорам отримувати спрощений доступ до лікарської та банківської таємниць, що раніше не було можливим, а також до даних провайдерів телекомунікацій, включаючи інформацію про дзвінки, маршрутизацію, зміст і тривалість цих даних.

У проєкті нового Закону встановлено розширені вимоги щодо обробки персональних даних, а також додаткові вимоги щодо отримання згоди та форми такої згоди на обробку. Оператори персональних даних зобов'язані забезпечувати обробку даних на рівні «за замовчуванням», тобто вони повинні застосовувати заходи захисту даних за замовчуванням без необхідності окремих додаткових згод або дій користувача.

Також розроблено чіткі алгоритми дій, які потрібно виконувати у разі несанкціонованого витоку даних, і встановлено межі відповідальності за порушення норм приватності. Це означає, що оператори персональних даних несуть юридичну відповідальність за будь-які порушення, які можуть виникнути в результаті невідповідності вимогам щодо обробки та захисту персональних даних.

Проєкт нового Закону враховує сучасну реальність і наголошує на необхідності не лише отримання дозволів на обробку персональних даних, але й чіткому визначенні обсягу таких даних. Основний акцент зроблено на тому, що під обробку підлягають лише дані, які безпосередньо стосуються мети обробки. Це означає, що не можна вимагати або обробляти дані, які виходять за рамки цього обсягу. Особлива увага в Проєкті нового Закону приділена питанням захисту персональних даних в умовах кібернебезпеки, особливо в контексті воєнного часу. Злочини, зокрема фішинг, стають усе більш актуальними, оскільки значна частина діяльності суспільства здійснюється через Інтернет.

Як зазначає О.П. Радкевич, ці злочини набувають усе більшої важливості й розповсюдженості, оскільки значна кількість людей активно взаємодіє в онлайн-середовищі [8, ст. 215].

Захист персональних даних у такому випадку залежить здебільшого від особи, що їх надає, заповнюючи форми реєстрації на сайтах чи відкриваючи різноманітні посилання в електронних листах від незнайомців [4, ст. 52].

Ситуація у країні вимагає від громадян свідомого ставлення до своїх даних. Необхідно користуватися лише перевіреними та офіційними джерелами інформації, а також проводити постійне резервування даних на різних носіях.

У контексті воєнних дій важливим стає питання щодо загрози незаконного використання та обробки персональних даних на тимчасово окупованих територіях. Центр протидії дезінформації в Україні займається інформуванням населення про різні незаконні дії, які здійснюються окупаційною владою з метою отримання даних. Часто це відбувається під прикриттям фальшивих переписів населення або надання гуманітарної допомоги. Цим шляхом збирають дані про певні категорії населення, такі як військовослужбовці та їх сім'ї, громадські активісти, журналісти. Після цього, використовуючи ці дані, здійснюється політика цькування або залякування. Тому важливо реєструвати факти таких порушень та, якщо можливо, повідомляти правоохоронні органи.

Окрім державного контролю за захистом персональних даних, громадянам належним чином потрібно особисто використовувати всі можливі способи та засоби. Громадянам необхідно постійно направляти запити щодо одержання інформації про локацію перебування своїх персональних даних, а також мету їх обробки. Відкритою повинна бути інформація про місце перебування володільця чи розпорядника персональних даних.

Важливо контролювати терміни отримання відповідей на свої запити. Якщо існують підстави для зміни чи знищення персональних даних, необхідно висунути відповідну вимогу до розпорядника цих даних або відкликати згоду на обробку і повернути персональні дані. Таким чином, особа має можливість контролювати використання своїх персональних даних і забезпечувати їх захист у випадку виявлення підстав для зміни, видалення або відкликання згоди на обробку даних.

Висновки. На сьогодні інститут захисту персональних даних знаходиться на етапі становлення та адаптації до реалій правового режиму воєнного стану. Необхідно приймати нові нормативно-правові акти, що будуть корелювати з нормами Європейського Союзу.

Загалом, основний принцип законної обробки персональних даних полягає в отриманні згоди від суб'єкта на їх обробку. В умовах воєнного стану діють особливі правила, які має враховувати кожна сторона, тому варто зробити такі висновки: необхідно перевіряти достовірність та правовий статус організацій, яким надаються персональні дані; обережно поводитися з електронними ресурсами і носіями, щоб уникнути витоку даних та злому систем безпеки; бути відповідальним у соціальних мережах, обмежувати надання особистої інформації й перевіряти надійність джерел інформації; забезпечувати захист персональної банківської інформації та перевіряти контрагентів перед передачею важливих даних; бути обачним при використанні системи QR-кодів, оскільки через їх швидкість і спрощеність може відбуватися зловживання та злочинні дії. Усі ці висновки мають на меті підвищити рівень захисту персональних даних у контексті воєнного стану й забезпечити особисту безпеку користувачів.

Література:

1. Брижко В. М. Захист персональних даних: реалії та практика сучасності. Інформація і право. № 3 (9). 2013. С. 31-49.

2. Головченко В. Правові основи захисту персональних даних. URL: http://yur-gazeta.com/publications/practice/inshe/pravovi-osnovi-zahistu-personalnihdanih.html (дата звернення: 11.07.2023).

3. Постанова від 29 грудня 2021 р. № 1456 «Про затвердження Порядку перевірки документів в осіб, огляду речей, транспортних засобів, багажу та вантажів, службових приміщень і житла громадян під час забезпечення заходів правового режиму воєнного стану». URL: https://ips.ligazakon.net/document/kp211456 (дата звернення: 11.07.2023).

4. Злив персональних даних українців: що сталося і як захиститися. Радіо Свобода. 2021. URL: https://www.radiosvoboda.org/a/zlyvdanyx-i-diya/30610626.html (дата звернення: 11.07.2023).

5. Погребна А. Коментар до Закону України «Про захист персональних даних». Юридичний журнал. 2010. №7. URL: http://www.justinian.com.ua/article.php?id=3579 (дата звернення: 11.07.2023).

6. Попович Т. П. Право особи на захист персональних даних в Інтернеті: теоретико-правові аспекти. Електронне наукове видання «Аналітично-порівняльне правознавство». Львів. 2021. № 2. С. 51-54.

7. Про захист персональних даних: Закон України від 01.06.2010 року №2297-VI. Дата оновлення від 27.10.2022, підстава - 2438-IX. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 11.07.2023).

8. Радкевич О. П. Конфіденційність персональної інформації в соціальних мережах. Вісник Вищої ради юстиції. Київ. 2012. С. 215-224.

References:

1. Bryzhko V. M. (2013), «Protection of personal data: realities and modern practice, Informatsiya i pravo. Vol. 3 (9). Pp. 31-49.

2. Holovchenko V. (2018), «Legal basis of personal data protection», available at: http://yur-gazeta.com/publications/practice/inshe/pravovi-osnovi-zahistu-personalnihdanih.html (Accessed on July 11, 2023).

3. «Resolution of December 29, 2021 № 1456 «On the approval of the Procedure for checking documents of persons, inspecting things, vehicles, luggage and cargo, office premises and citizens' housing during the provision of measures of the legal regime of martial law» (2021), available at: https://ips.ligazakon.net/document/kp211456 (Accessed on July 11, 2023).

4. «Draining of personal data of Ukrainians: what happened and how to protect yourself» (2021), Radio Svoboda, available at: https://www.radiosvoboda.org/a/zlyvdanyx-i-diya/30610626.html (Accessed on July 11, 2023).

5. Pohrebna A. (2010), «Statement on the Law of Ukraine «On Personal Data Protection», Yurydychnyy zhurnal. Vol. 7, available at: http://www.justinian.com.ua/article.php?id=3579 (Accessed on July 11, 2023).

6. Popovych T. P. (2021) «The right of a person to protect personal data on the Internet: theoretical and legal aspects», Elektronne naukove vydannya «Analitychno-porivnyalne pravoznavstvo». Vol. 2. Pp. 51-54.

7. «On the protection of personal data: Law of Ukraine of June 1, 2010 № 2297-VI. Updated on 10/27/2022, basis for updating- 2438-IX», available at: https://zakon.rada.gov.ua/laws/show/2297-17#Text (Accessed on July 11, 2023).

8. Radkevych O. P. (2012), «Confidentiality of personal information in social networks», Visnyk Vyshchoyi rady yustytsiyi. Pp. 215-224.

Стаття надійшла до друку 12.07.2023 року