Зінич Л.В.
ORCID: 0000-0002-2562-1036

СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В УМОВАХ ВОЄННОГО СТАНУ

УДК 351.746:007:004.056.5:342.7(477)”36”

Актуальність теми дослідження. В умовах російської агресії виникає нагальна потреба у забезпеченні ефективного захисту персональних даних. Головною метою на цьому етапі є запобігання незаконній обробці та використанню персональних даних військовослужбовців, цивільних осіб, учасників гуманітарних акцій та інших громадян, які можуть бути використані ворожими силами або втратити конфіденційність, а також запобігання кібератакам та кіберзагрозам щодо цілісності персональних даних. Як видається, це завдання неможливо здійснити без комплексної, цілеспрямованої політики держави, яка повинна супроводжуватися пошуком нових форм, засобів і методів захисту персональних даних.

Неабиякий вплив на здійснення реформ у цій сфері також має європейська інтеграція України. Наша держава мусить ухвалити низку законів у сфері захисту персональних даних, у якому повинні бути втілені положення основних європейських актів у відповідній галузі (GDPR, «Конвенції 108») [1].

Постановка проблеми. Сьогодні сфера захисту персональних даних в умовах війни потребує вдосконалення щодо організаційно-правових заходів їх обробки й використання.

Окреслені обставини зумовлюють актуальність розгляду питання про сучасний стан та перспективи захисту персональних даних в умовах воєнного стану.

Стан дослідження. Деяким аспектам захисту персональних даних в умовах воєнного стану приділяли увагу такі науковці, як Боровий О., Олексюк О. В., Юсипенко І. О., Порядчук Л. Б.

Разом із тим проведені дослідження не розкривають у повному обсязі проблематики захисту персональних даних в умовах воєнного стану в Україні.

Метою статті є розкриття особливостей правового регулювання захисту персональних даних, аналіз проблемних питань та внесення пропозицій щодо їх вирішення в цій сфері.

Виклад результатів дослідження. Правовий режим воєнного стану зумовив внесення змін до законодавства, яке стосується захисту персональних даних. Зокрема, були внесені зміни до Закону України «Про захист інформації в інформаційно-комунікаційних системах» [2] щодо можливості зберігання публічних реєстрів, інформаційних джерел на хмарних ресурсах, що перебувають за межами України, протягом дії воєнного стану та шість місяців після його скасування. Таке ж саме положення було прийнято Національним банком України з метою захисту персональних даних користувачів банківських послуг. Крім того, обмежено або закрито доступ до більшості державних реєстрів. Такі заходи були спрямовані на гарантування безпеки персональних даних.

Також уряд прийняв рішення про взаємодію між державними реєстрами в системі «Трембіта» зі сповіщенням громадян в «Дії» про запити на обробку персональних даних, що забезпечує більш прозору роботу з реєстрами [3].

Зробимо акцент на тому, що відповідно до статті 64 Конституції України передбачено: в умовах воєнного або надзвичайного стану можуть встановлюватися окремі обмеження прав і свобод із зазначенням строку їхньої дії. Згідно із Законом України «Про правовий режим воєнного стану» [4], воєнний стан передбачає надання відповідним органам державної влади, військовому командуванню, військовим адміністраціям та органам місцевого самоврядування повноважень, необхідних для запобігання загрозі, відсічі збройної агресії та гарантування національної безпеки, усунення загрози небезпеки державній незалежності України, її територіальній цілісності. Обробка персональних даних має здійснюватися з урахуванням викладених вище положень законодавства України. Ця процедура повинна бути пропорційною та здійснюватися для конкретних і законних цілей.

Як зазначає А. В. Федорончук, «ті зміни, які відбулися у різних сферах життєдіяльності держави після введення воєнного стану, не вплинули на функціонування та подальший розвиток нашої держави, а тому це також підтверджує можливість введен-

ня воєнного стану на більш ранньому етапі російської агресії» [5, с. 32].

Кібербезпека персональних даних в умовах війни. Кібербезпека персональних даних стає особливо важливою в умовах війни, оскільки конфлікт може спричинити зростання кількості кібератак та загроз для цифрової інфраструктури.

Відповідно до Закону «Про основні засади забезпечення кібербезпеки України» [6], «кібербезпека — це захищеність життєво важливих інтересів людини й громадянина, суспільства та держави під час використання кіберпростору, за якого забезпечується сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання, нейтралізація реальних і потенційних загроз національній безпеці України в кіберпросторі».

Доречно вказати, що про необхідність розробки стратегії інформаційної кібербезпеки науковці говорили протягом тривалого часу. Тому передбачення таких положень у законодавстві є позитивним кроком. Варто якнайскоріше її розробити та почати впроваджувати [7, с. 18].

В умовах війни співпраця між державними органами, експертами з кібербезпеки, приватним сектором та окремими державами є важливою. Обмін інформацією про виявлені загрози та кібератаки допомагає швидко реагувати на них та гарантувати колективну кібербезпеку.

Для прикладу наведемо досвід Естонії у сфері захисту персональних даних. Естонія докладає зусиль для поліпшення кібербезпеки за такими напрямками, як боротьба з кіберзлочинами, розвиток критичної інфраструктури, електронних послуг та підвищення рівня національної безпеки. Загальносвітовою тенденцією сьогодні є створення в державах підрозділів кіберполіції та Центрів реагування на комп'ютерні інциденти, основним завданням яких є боротьба з кіберзлочинами [8, с. 32-33].

Умови війни можуть спричинити збільшення кількості кібератак на критичну інфраструктуру, включаючи мережі зв'язку, енергетичні системи, банківські установи тощо. Захист їх від кіберзагроз є критичним для гарантування безпеки персональних даних.

Проблеми захисту персональних даних. Варто вказати, що в умовах воєнного стану є чимало питань щодо захисту персональних даних, зокрема можна їх умовно поділити на проблемні питання законодавства у сфері захисту персональних даних та проблеми правозастосування в цій галузі.

Сьогодні основною проблемою є відсутність законодавчих актів, які б відповідали міжнародним стандартам.

Серед проблемних питань законодавства у сфері захисту персональних даних в умовах воєнного стану варто виділити відсутність плану дій у випадку несанкціонованого доступу до персональних даних внаслідок кібератак.

За численними повідомленнями в засобах масової інформації громадяни України постійно стають жертвами хакерських атак з боку ворожих кіберзловмисників. Відбувається надсилання електронних листів, повідомлень у месенджерах від начебто державних органів, банків, служб безпеки тощо з рекомендаціями перейти за вказаними в листах/повідомленнях посиланнями. Після завантаження вкладеного файлу шахраї мають змогу отримати доступ до персональних даних, що містяться в електронному пристрої користувача.

Розробка систем моніторингу та виявлення кіберінцидентів є важливою для реагування на можливі атаки та виявлення порушень безпеки персональних даних. Завчасне виявлення інцидентів дозволяє швидко вжити заходів для запобігання, а також мінімізації впливу на персональні дані.

Проблеми правозастосування, а саме фотофіксація документів, що містять персональні дані, на блокпостах.

Такі дії дозволені та є правомірними за згодою громадян, відповідно до «Порядку перевірки документів в осіб, огляду речей, транспортних засобів, багажу та вантажів, службових приміщень та житла громадян при забезпеченні заходів правового режиму воєнного стану» [9].

Аудіо- та відеофіксація особистих речей проводиться виключно за згодою громадян, також дозволена перевірка мобільних телефонів.

Проблемні питання полягають у тому, на які пристрої буде здійснюватися аудіо- та відеофіксація і чи зможуть такі особи

гарантувати безпеку збереження персональних даних. Сьогодні жодного правового регулювання з цього приводу немає.

Як підсумок, захист персональних даних повинен здійснюватися тими суб'єктами, які їх обробляють. Органи державної влади, місцевого самоврядування, а також підприємства, установи й організації всіх форм власності, фізичні особи (підприємці, особи, що впроваджують незалежну професійну діяльність), які обробляють персональні дані, зобов'язані забезпечити їх захист від випадкових втрат або знищення, незаконної обробки, зокрема незаконного знищення чи доступу до персональних даних.

Перспективи захисту персональних даних в умовах війни. Умови війни створюють багато проблем для захисту персональних даних, зокрема дуже гостро постає питання їх захисту від кібератак та інших незаконних дій. З огляду на те, що захист персональних даних є складним та комплексним завданням, варто вжити заходів для захисту своїх персональних даних як громадянам, так і державним інституціям, що здійснюють їх обробку. Тільки комплекс заходів з боку держави та приватних осіб може забезпечити належний захист персональних даних. Окреслимо зазначені перспективи.

Для державних інституцій захист персональних даних може полягати в зміні організації їх обробки й містити такі заходи:

1) Варто зазначити, що в разі загрози окупації певного населеного пункту органи державної влади, їх посадові особи повинні знищити документи та інші матеріальні носії інформації, що містять персональні дані громадян України.

Це повинно відбуватися згідно з аналогією до знищення службової інформації.

Для приватних осіб перспективними є такі заходи:

2) застосування надійного апаратного та програмного забезпечення пристроїв, на яких буде здійснюватися обробка персональних даних в умовах воєнного стану.

3) кодування даних у випадку передачі особистої інформації через мережу Інтернет.

Гарантування безпеки мереж та систем є необхідним кроком для захисту персональних даних в умовах війни. Він складається

зі встановлення надійних паролів, використання мультифакторної автентифікації, шифрування даних та регулярне оновлення програмного забезпечення для запобігання небезпекам.

Висновок. У результаті проведеного аналізу слід зазначити, що захист персональних даних є складним та комплексним завданням, яке супроводжується низкою проблем.

Більшість із них повинна бути вирішена новим законом «Про захист персональних даних», який мусить привести цю сферу до міжнародних стандартів, передбачених «Конвенцією 108» та GDPR.

Загалом, забезпечення захисту персональних даних є постійним викликом і розвиток нових технологій вимагає постійного оновлення заходів безпеки. Користувачі та організації мусять свідомо та обережно ставитися до обробки й передачі персональних даних, а законодавство і стандарти повинні постійно адаптовуватися до змін у цифровому середовищі й військово-політичній сфері.

Зазначене дослідження повністю не вичерпує проблеми захисту персональних даних в умовах воєнного стану, тому першочерговим завданням подальших досліджень є розробка пропозицій для вдосконалення чинного законодавства України у сфері захисту персональних даних.

1. *Про виконання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами членами, з іншої сторони. Постанова Кабінету Міністрів України №1106 від 25 жовтня 2017 р. URL: https://zakon.rada.gov.ua/laws/show/1106-2017-%D0%BF#Text (дата звернення: 19.11.2022 р.).*
2. *Про захист інформації в інформаційно-комунікаційних системах. Закон України від 05.07.1994 р. №80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 08.01.2023 р.).*
3. *Прозора робота з реєстрами: у системі «Трембіта» фіксуватимуть, хто і коли переглядав персональні дані українців. URL: https://thedigital.gov.ua/news/prozora-robota-z-reestrami-u-sistemi-trembita-fiksuvatimut-khto-i-koli-pereglyadav-personalni-dani-ukraintsiv (дата звернення: 02.02.2023 р.).*

4. Про правовий режим воєнного стану. Закон України від 12.05.2015 №389-VIII. URL: https://zakon.rada.gov.ua/laws/show/389-19#Text (дата звернення 08.01.2023 р.).

5. Федорончук А.В. Приводи, підстави та підсумки введення воєнного стану в Україні. Актуальні проблеми вдосконалення чинного законодавства України №49 (2019). С.23-34 URL: https://scijournals.pnu.edu.ua/index.php/apiclu/article/view/1852/2295 (дата звернення: 27.01.2023 р.).

6. Про основні засади забезпечення кібербезпеки України. Закон України від 05.10.2017 р. №2163-VII URL: https://zakon.rada.gov.ua/laws/show/2163-19#top (дата звернення: 16.01.2023 р.).

7. Петровська І.І. Правові засади публічного контролю за інформаційною безпекою в Україні. Актуальні проблеми вдосконалення чинного законодавства України №49 (2019). С.13-23 URL: https://scijournals.pnu.edu.ua/index.php/apiclu/article/view/1851/2294 (дата звернення: 27.01.2023 р.).

8. Зінич Л.В. Інформаційна безпека Естонії: досвід для України. Актуальні проблеми вдосконалення чинного законодавства України. Збірник наукових статей. Випуск 50. 2019. С.26-38. http://lib.pnu.edu.ua:8080/bitstream/123456789/8674/1/2088-Article%20Text-4373-1-10-20200219.pdf (дата звернення: 27.01.2023).

9. Про затвердження порядку перевірки документів у осіб, огляду речей, транспортних засобів, багажу та вантажів службових приміщень і житла громадян під час забезпечення заходів правового режиму воєнного стану. Постанова Кабінету Міністрів України від 29 грудня 2021 р. №1456. URL: https://zakon.rada.gov.ua/laws/show/1456-2021-%D0%BF#Text (дата звернення: 27.01.2023 р.).

Zinych L.V Current status and perspectives of personal data protection under the conditions of marital state

The aggression of russia has created numerous problems in terms of legal and organizational protection of personal data. Therefore, this article analyzes the current state and prospects of personal data protection during a state of war. The author examines the changes to legislation in this field caused by russia's full-scale invasion and analyzes the state of cybersecurity legislation in Ukraine as part of personal data protection.

Emphasis is placed on the fact that effective protection of personal data is impossible without ensuring cybersecurity. The experience of Estonia as a leading European country in this field is highlighted. The main directions of Estonia's data protection policy are indicated.

The analysis of legislation and law enforcement practices highlights a number of issues, such as the absence of a plan for cyber attacks and the vulnerability of devices

used for photo and video documentation at checkpoints. It is expressed that these shortcomings need to be addressed through the adoption of a new law on personal data protection.

Regarding the prospects of personal data protection in a state of war, the article argues that measures for safeguarding personal data should be taken by both private individuals and state institutions. Private individuals should employ measures such as using reliable software and data encryption. State institutions should implement the following measures: in the event of a threat of occupation of a specific locality, the authorities and their officials should destroy documents and other physical media containing personal data of Ukrainian citizens.

The overall conclusion is that the protection of personal data is a constant challenge, and the development of new technologies requires continual updating of security measures. Users and organizations must be knowledgeable and cautious in the processing and transmission of personal data, while legislation and standards need to constantly adapt to changes in the digital environment and the military-political sphere.

Keywords: aggression, personal data, cyber protection, information security, privacy.

Зінич Л. В. Сучасний стан та перспективи захисту персональних даних в умовах воєнного стану

Агресія росії зумовила численні правові та організаційні проблеми у сфері захисту персональних даних. Саме тому ця стаття присвячена аналізу сучасного стану й перспектив їх захисту в умовах воєнного стану. Автор склав характеристику змін законодавства в цій сфері, що відбулися внаслідок повномасштабного вторгнення росії, і проаналізував стан законодавства України в галузі кібербезпеки як складової захисту персональних даних.

Акцент зроблено на тому, що ефективний захист персональних даних неможливий без гарантування кібербезпеки. Звернено увагу на досвід Естонії, як провідної європейської держави, в зазначеній сфері. Вказано основні напрямки політики Естонії в цій галузі.

На основі аналізу законодавства та практики правозастосування виділено низку проблемних питань, зокрема відсутність плану заходів у разі кібератак, незахищеність пристроїв, на які здійснюється фото- або відеофіксація документів на блокпостах. Висловлюється думка, що зазначені недоліки повинні бути усунені шляхом прийняття нового закону про захист персональних даних.

Щодо перспектив їх захисту в умовах воєнного стану, у статті обґрунтовується, що заходи із захисту персональних даних повинні бути вжиті як приватними особами, так і державними інституціями. Приватні особи повинні вжити таких заходів, як використання надійного програмного забезпечення, кодування даних. Державні інституції повинні вжити інших заходів: у разі загрози окупації певного населеного пункту органи державної влади, їх посадові особи повинні знищити документи й інші матеріальні носії інформації, що містять персональні дані громадян України.

Як підсумок, відзначається, що забезпечення захисту персональних даних є постійним викликом і розвиток нових технологій вимагає постійного оновлення заходів безпеки. Користувачі та організації повинні обережно й свідомо ставитися до обробки й передачі персональних даних, а законодавство та стандарти — постійно адаптуватися до змін у цифровому середовищі й військово-політичній сфері.

Ключові слова: агресія, персональні дані, кіберзахист, інформаційна безпека, конфіденційність.