

УДК 342.7

DOI <https://doi.org/10.24144/2307-3322.2025.90.1.43>

ПЕРСОНАЛЬНІ ДАНІ В УМОВАХ ВОЄННОГО СТАНУ: КОНСТИТУЦІЙНО-ПРАВОВІ ОБМЕЖЕННЯ ТА ГАРАНТІЇ

Середа І.Л.,
аспірант кафедри конституційного права України
Національного юридичного університету
імені Ярослава Мудрого
ORCID: 0009-0003-4282-1720

Середа І.Л. Персональні дані в умовах воєнного стану: конституційно-правові обмеження та гарантії.

У статті досліджується конституційно-правова природа обмежень права на захист персональних даних в умовах воєнного стану, а також гарантії, які забезпечують баланс між національною безпекою та правами людини. Доводиться, що право на захист персональних даних, закріплене у статті 32 Конституції України, є невід'ємною складовою права на приватність. Воєнний стан як особливий правовий режим, передбачає можливість тимчасового обмеження цього права з метою забезпечення обороноздатності держави та громадської безпеки. У статті проаналізовано відповідні положення Конституції України, Закону України «Про правовий режим воєнного стану» та Закону України «Про захист персональних даних».

Особливу увагу приділено практиці Конституційного Суду України, який у своїх рішеннях наголошує на необхідності дотримання принципів законності, пропорційності та необхідності при обмеженні конституційних прав. Розглянуто ключові рішення КСУ, що стосуються захисту персональних даних, зокрема в умовах надзвичайних ситуацій.

У статті визначено основні гарантії захисту персональних даних в умовах воєнного стану, серед яких: законність обробки даних, пропорційність обмежень, судовий контроль, прозорість дій держави та дотримання міжнародних стандартів. Автор робить висновок, що навіть в умовах воєнного стану держава зобов'язана забезпечувати належний рівень захисту персональних даних, а також пропонує напрями подальших досліджень у цій сфері.

Доводиться доцільність врахування міжнародного досвіду, зокрема практик країн Європейського Союзу, які регулюють захист персональних даних. У цих країнах навіть у надзвичайних ситуаціях зберігається баланс між забезпеченням безпеки та дотриманням прав людини. Україна має запозичити такі підходи, як обмеження обсягу даних, що збираються, встановлення чітких строків їхнього зберігання, а також створення незалежних органів, які здійснюють нагляд за обробкою персональних даних. Зокрема, доцільно розробити механізми, які б забезпечували прозорість дій державних органів у сфері обробки персональних даних, а також гарантували дотримання прав громадян навіть у надзвичайних умовах.

Ключові слова: інформація, персональні дані, захист персональних даних, воєнний стан, судова практика, держава, конституційні гарантії.

Sereda I.L. Personal data under martial state: constitutional and legal restrictions and guarantees.

The article examines the constitutional and legal nature of restrictions on the right to protection of personal data in martial law, as well as guarantees that ensure a balance between national security and human rights. The right to protection of personal data, enshrined in Article 32 of the Constitution of Ukraine, is an integral part of the right to privacy. Martial law, as a special legal regime, provides for the possibility of temporary restrictions on this right in order to ensure the defense capability of the state and public security. The article analyzes the relevant provisions of the Constitution of Ukraine, the Law of Ukraine “On the Legal Regime of Martial Law” and the Law of Ukraine “On the Protection of Personal Data”.

Particular attention is paid to the practice of the Constitutional Court of Ukraine, which in its decisions emphasizes the need to comply with the principles of legality, proportionality and necessity when restricting constitutional rights. Key decisions of the Constitutional Court of Ukraine concerning the protection of personal data, in particular in emergency situations, are considered.

The article identifies the main guarantees of personal data protection in martial law, including: legality of data processing, proportionality of restrictions, judicial control, transparency of state actions, and compliance with international standards. The author concludes that even in martial law, the state is obliged to ensure an adequate level of personal data protection, and also suggests directions for further research in this area.

The expediency of taking into account international experience, in particular the practices of the European Union countries that regulate the protection of personal data, is proved. In these countries, even in emergency situations, a balance is maintained between ensuring security and respecting human rights. Ukraine should adopt such approaches as limiting the volume of data collected, establishing clear periods for their storage, and creating independent bodies that oversee the processing of personal data. In particular, it is advisable to develop mechanisms that would ensure the transparency of the actions of state bodies in the field of personal data processing, as well as guaranteeing the observance of citizens' rights even in emergency conditions.

Key words: information, personal data, personal data protection, martial law, case law, state, constitutional guarantees.

Постановка проблеми. В умовах глобальної трансформації суспільних відносин, зумовленої як стрімким розвитком інформаційно-комунікаційних технологій, так і зростанням геополітичної напруженості, питання забезпечення права на захист персональних даних набуває особливої актуальності. Це право, будучи фундаментальною складовою права на приватність, виступає ключовим елементом правового механізму забезпечення недоторканності особистого життя, що є невід'ємною ознакою демократичної правової держави.

Водночас, у контексті збройної агресії росії проти України та запровадження воєнного стану, виникає необхідність переосмислення правових засад взаємодії між забезпеченням національної безпеки та дотриманням конституційних прав і свобод людини. Воєнний стан, як особливий правовий режим, передбачає можливість тимчасового обмеження окремих прав і свобод громадян, що зумовлює необхідність пошуку оптимального балансу між публічними інтересами та правами індивіда. У цьому стані право на захист персональних даних стає об'єктом особливої уваги, оскільки його обмеження може мати як позитивні наслідки для забезпечення обороноздатності держави, так і значні ризики для прав людини.

Актуальність дослідження зумовлена низкою факторів. По-перше, відсутність чіткого правового регулювання обмеження права на захист персональних даних в умовах воєнного стану створює правову невизначеність, що призводить до зловживань владними повноваженнями. По-друге, недостатній рівень судового контролю за обмеженням цього права ускладнює забезпечення принципу верховенства права. По-третє, недотримання міжнародних стандартів у сфері захисту персональних даних підриває довіру до державних інституцій та створює негативні наслідки для міжнародного іміджу України.

Наукова новизна дослідження полягає у комплексному аналізі правових механізмів обмеження права на захист персональних даних в умовах воєнного стану, з урахуванням як національного законодавства, так і міжнародних стандартів. Особливу увагу приділено принципам законності, пропорційності та необхідності, які мають бути основоположними у процесі обмеження конституційних прав.

Стан опрацювання цієї проблематики. Останні дослідження у сфері захисту персональних даних демонструють зростаючий інтерес науковців до проблематики конфіденційності в умовах цифровізації. Зокрема, цим питанням присвячені роботи таких авторів: В.О. Кравчук, Т.В. Попович, О.Г. Рогова, Л.В. Зінич, В.М. Брижко, А.В. Федорончук, І.І. Петровська, Даніель Солове, Пол Шварц, Гелен Ніссенбаум та інші.

Метою дослідження є розробка концептуальних підходів до правового регулювання обмеження права на захист персональних даних в умовах воєнного стану, що забезпечували б баланс між національною безпекою та дотриманням прав людини. Для досягнення цієї мети у дослідженні здійснено аналіз чинного законодавства України, практики Конституційного Суду

України, а також міжнародного досвіду у сфері захисту персональних даних в умовах надзвичайних ситуацій.

Таким чином, дослідження спрямоване на вирішення однієї з ключових проблем сучасного правознавства – забезпечення ефективного правового механізму захисту персональних даних в умовах воєнного стану, що відповідає принципам демократичної правової держави та міжнародним стандартам у сфері прав людини.

Виклад основного матеріалу дослідження. Право на захист персональних даних є однією з ключових складових права на приватність, яке, у свою чергу, належить до фундаментальних прав людини, закріплених у міжнародних та національних правових актах. Це право забезпечує юридичні гарантії недоторканності особистого життя, захисту від свавільного втручання у приватну сферу, а також контроль особи над інформацією, що стосується її ідентифікації, особистих характеристик, поведінки, комунікацій та інших аспектів приватного життя. У теоретико-правовому аспекті право на захист персональних даних розглядається як комплексне суб'єктивне право, що має міждисциплінарний характер і охоплює елементи конституційного, адміністративного, цивільного, інформаційного та міжнародного права. Його сутність полягає у встановленні правових механізмів, які забезпечують збалансоване співвідношення між інтересами особи, суспільства та держави у сфері обробки, зберігання, передачі та використання персональних даних.

Згідно з міжнародними стандартами, зокрема, Загальною декларацією прав людини (стаття 12) [1], Конвенцією про захист прав людини та основоположних свобод (стаття 8) [2], Міжнародним пактом про громадянські і політичні права (стаття 17) [3] та Конвенцією «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» [4], право на захист персональних даних є невід'ємною складовою права на повагу до приватного і сімейного життя. У цих актах закріплено основоположні принципи, які мають бути враховані при розробці національного законодавства: законність, пропорційність, цільове призначення, мінімізація даних, обмеження строків зберігання, конфіденційність та відповідальність за порушення.

На національному рівні право на захист персональних даних в Україні закріплено у статті 32 Конституції України [5], яка гарантує кожному право на невтручання в особисте і сімейне життя, а також забороняє збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, за винятком випадків, визначених законом. Базовим нормативно-правовим актом, що регулює дану сферу, є Закон України від 01.06.2010 № 2297-VI «Про захист персональних даних» [6], який визначає правові засади обробки персональних даних, права суб'єктів даних, обов'язки володільців і розпорядників даних, а також механізми контролю та відповідальності.

Теоретичний аналіз права на захист персональних даних передбачає його розгляд через призму таких ключових аспектів. По-перше, сутність і зміст права на захист персональних даних включають низку елементів, серед яких: право на інформованість щодо обробки даних, право на доступ до власних даних, право на виправлення, видалення або блокування даних, право на заперечення проти обробки даних, а також право на захист у разі порушення цих прав. Ці елементи формують змістовну основу права, яка забезпечує його реалізацію в різних правовідносинах. По-друге, особливе значення мають принципи, які визначають правові рамки обробки персональних даних. До них належать принцип законності, який передбачає, що обробка даних має здійснюватися виключно на підставі закону або згоди суб'єкта даних; принцип пропорційності, що вимагає відповідності обсягу і характеру обробки даних меті, для якої вони збираються; принцип цільового призначення, який обмежує використання персональних даних лише конкретними, чітко визначеними і законними цілями; а також принцип мінімізації даних, що передбачає обробку лише тих даних, які є необхідними для досягнення визначеної мети.

По-третє, реалізація права на захист персональних даних забезпечується через систему правових механізмів, які включають нормативно-правове регулювання, інституційний механізм та судовий захист. Законодавство встановлює чіткі правила обробки даних, права суб'єктів даних та обов'язки володільців і розпорядників.

Для забезпечення контролю за дотриманням вимог щодо захисту персональних даних передбачено спеціальну процедуру, яка регламентується Порядком здійснення контролю Уповноваженим Верховної Ради України з прав людини за виконанням законодавства у цій сфері. Цей Порядок затверджений наказом Уповноваженого від 8 січня 2014 року № 1/02-14 [7]. Основними формами контролю є проведення перевірок, які можуть бути плановими, позаплановими, виїзними або безвиїзними. У разі виявлення порушень, відповідно до Порядку, складається припис про їх усунен-

ня або протокол про адміністративне правопорушення. Суб'єкти даних мають право звертатися до суду у разі порушення їхніх прав.

По-четверте, у сучасних умовах глобалізації та цифровізації особливого значення набуває гармонізація національного законодавства із міжнародними стандартами у сфері захисту персональних даних. Зокрема, імплементація положень Загального регламенту ЄС про захист даних (GDPR) [8] є важливим кроком для забезпечення відповідності українського законодавства європейським стандартам.

Досліджуючи конституційно-правові обмеження та гарантії захисту персональних даних в умовах воєнного стану доцільно звернутися до конкретних прикладів, які ілюструють практичні виклики та проблеми, що виникають у цій сфері. Такі приклади дозволяють не лише актуалізувати досліджувану проблематику, але й продемонструвати реальні наслідки недосконалості правового регулювання та правозастосовної практики.

Одним із найбільш показових прикладів є використання мобільних додатків, які в умовах воєнного стану виконують функції моніторингу переміщень громадян, збору даних про їхню геолокацію, стан здоров'я та інші «чутливі» відомості. Зокрема, мобільний додаток «Дія», який активно використовується для надання державних послуг, у період воєнного стану став інструментом для впровадження нових функцій, пов'язаних із безпекою. Однак, відсутність чітких правових механізмів, які б регулювали обсяг, мету та строки зберігання таких даних, створює ризики їхнього неправомірного використання, що суперечить принципу мінімізації даних, закріпленому в міжнародних стандартах, таких як Загальний регламент про захист даних.

Ще однією загрозою є кібератаки на державні реєстри, які містять персональні дані громадян. У 2022–2025 роках було зафіксовано численні спроби зламу баз даних, зокрема тих, що інтегровані з додатком «Дія» або іншими державними інформаційними системами [9]. Такі атаки, здійснювані з боку агресора, мають на меті отримання доступу до чутливої інформації для її подальшого використання у дезінформаційних кампаніях, шантажі або інших злочинних діях. Недостатній рівень технічного захисту цих реєстрів, а також відсутність належного моніторингу їхньої безпеки створюють серйозні загрози як для приватності громадян, так і для національної безпеки.

Окремої уваги заслуговує розширення повноважень правоохоронних органів щодо доступу до персональних даних громадян [10]. У період воєнного стану такі повноваження часто обґрунтовуються необхідністю забезпечення національної безпеки, виявлення потенційних загроз або запобігання терористичним актам. Проте, відсутність прозорих процедур та ефективного судового контролю за діями правоохоронних органів створює ризики зловживань, що призводить до порушення права на приватність, гарантованого статтею 32 Конституції України [5].

Крім того, у період воєнного стану громадяни часто позбавлені можливості отримувати інформацію про те, як їхні персональні дані обробляються державними органами чи іншими суб'єктами. Це обмеження обґрунтовується необхідністю збереження конфіденційності операцій, пов'язаних із забезпеченням оборони, але водночас воно порушує принцип прозорості, який є ключовим у сфері захисту персональних даних. Відсутність доступу до такої інформації ускладнює реалізацію права на захист персональних даних і створює правову невизначеність.

Для порівняння, у країнах Європейського Союзу, навіть у надзвичайних ситуаціях зберігається чіткий баланс між забезпеченням безпеки та дотриманням прав людини. У випадках обробки даних для цілей національної безпеки встановлюються суворі обмеження щодо обсягу та строків зберігання даних, а також передбачаються механізми незалежного контролю за діями державних органів [8]. Такий підхід має слугувати орієнтиром для вдосконалення українського законодавства.

Тож, наведені приклади демонструють багатогранність проблематики захисту персональних даних в умовах воєнного стану. Вони підкреслюють необхідність удосконалення правового регулювання, посилення технічного захисту баз даних, забезпечення прозорості дій державних органів та підвищення рівня правової культури серед населення.

Формування теоретико-методологічних засад та практичних підходів до забезпечення захисту персональних даних є одним з напрямів сучасних наукових досліджень. Наукові напрацювання у цій сфері охоплюють широкий спектр питань, включаючи правові, технічні та організаційні аспекти, що стають предметом глибокого міждисциплінарного аналізу та дискусій. Професор права інтелектуальної власності та технологій у Школі права Університету Джорджа Вашингтона – Даніель Солове у своїй праці «Understanding Privacy» [11] наголошує на складності визначення приватності як правової категорії, що вимагає врахування технологічних, соціальних та правових

аспектів. Джоел Рейденберг у роботі «Data Privacy Law: A Study of United States Data Protection» підкреслює важливість гармонізації національного законодавства з міжнародними стандартами, що є актуальним для України в контексті адаптації до вимог GDPR [12]. Професорка Корнельського технічного університету – Гелен Ніссенбаум у своїй концепції «контекстуальної цілісності» акцентує увагу на залежності приватності від соціального контексту [13]. Наголошується на тому, що порушення приватності відбувається, коли інформація використовується або передається всупереч суспільним очікуванням, характерним для певного контексту, наприклад, у медичній, трудовій чи соціальній сфері. Цей підхід допомагає розробляти політики захисту даних, враховуючи специфіку різних ситуацій.

Цікавим видається досвід Макса Шремса, австрійського юриста та активіста, який яскраво демонструє важливість розвитку правозахисної діяльності у сфері захисту персональних даних, особливо в умовах глобалізації та стрімкого розвитку цифрових технологій. Його боротьба з порушеннями приватності, зокрема у справі проти Facebook, стала знаковою подією, яка привернула увагу до проблеми незаконного використання персональних даних транснаціональними корпораціями. Завдяки його зусиллям Європейський суд справедливості у 2015 році скасував угоду «Safe Harbor» [14], яка дозволяла передачу даних європейських користувачів до США без належного рівня захисту. Цей прецедент підкреслив необхідність посилення правового регулювання у сфері обробки даних, а також важливість активної участі громадянського суспільства у відстоюванні права на приватність. Досвід Шремса доводить, що індивідуальні ініціативи можуть мати глобальний вплив, стимулюючи вдосконалення законодавства, підвищення прозорості діяльності компаній та зміцнення механізмів захисту персональних даних.

Українська наукова спільнота також активно досліджує проблематику захисту персональних даних та приватності. В.О. Кравчук [15] наголошує, що держава, як найбільший володілець персональних даних, несе відповідальність за їх збереження, обробку та використання, особливо в умовах сучасних викликів, таких як кібератаки. Він підкреслює, що кібератаки є небезпечним інструментом ведення війни, який потребує мінімальних ресурсів, проте, завдає значної шкоди. У відповідь на ці виклики Україна активно залучає IT-фахівців для захисту національної безпеки, що є позитивним кроком у забезпеченні захисту персональних даних, особливо в умовах воєнного стану. Окрему увагу Кравчук В.О. приділяє питанням інформаційного обігу на тимчасово окупованих територіях, де захист персональних даних має критичне значення як для інтересів окремих осіб, так і для національної безпеки.

Разом із цим, варто погодитися з думкою Т.П. Попович [16], яка визначає право на захист персональних даних, як втілення впевненості особи у збереженні та охороні відомостей про неї. Вона підкреслює, що правові обов'язки у цій сфері покладаються передусім на державу, яка повинна забезпечити збереженість персональних даних на законодавчому, інституційному, організаційно-технічному рівнях. Держава має гарантувати конфіденційність даних, передбачити чіткий режим їх обробки, а також створити механізми отримання згоди від особи на обробку інформації про неї.

Проаналізувавши викладені позиції, ми схиляємося до думки Т.П. Попович, оскільки її підхід до визначення права на захист персональних даних як втілення впевненості особи у збереженні інформації про неї є концептуально обґрунтованим і системним. Її акцент на необхідності створення чітких правових, інституційних та технічних механізмів забезпечує комплексний підхід до вирішення проблеми. Водночас позиція Кравчука В.О. є важливою у контексті сучасних викликів, таких як кібератаки та в умовах воєнного стану, однак вона більше зосереджена на оперативних аспектах, тобто зі здатністю реагування в короткостроковій перспективі.

З наведеного вище можемо зробити проміжний висновок, що інтеграція міжнародного досвіду та наукових підходів, запропонованих як зарубіжними, так і українськими вченими, дозволяє сформувати комплексну систему захисту персональних даних, яка відповідатиме сучасним викликам цифрової епохи.

Розглянуті теоретичні підходи до захисту персональних даних дозволяють перейти до аналізу практики Конституційного Суду України, яка конкретизує правові механізми реалізації цього права. Конституційний Суд України, як гарант конституційного ладу, неодноразово наголошував на важливості дотримання прав і свобод людини і громадянина, навіть у надзвичайних умовах, таких як воєнний стан. Його рішення є важливим джерелом для розуміння правових стандартів у сфері захисту персональних даних.

Зокрема, у своїх рішеннях Конституційний Суд України неодноразово підкреслював, що право на приватність, включно із захистом персональних даних, є невід'ємною складовою правового статусу особи. У рішенні № 2-рп/2012 [17] Суд зазначив, що обробка персональних даних повинна здійснюватися виключно на підставі закону, а будь-яке втручання у приватне життя особи має бути обґрунтованим, пропорційним і відповідати легітимній меті. Вважаємо, що дане положення є особливо актуальним в умовах воєнного стану, коли держава може вдаватися до обмеження певних прав і свобод.

Крім того, Конституційний Суд України у своїй практиці наголошує на необхідності забезпечення балансу між інтересами національної безпеки та правами людини. Рішення Конституційного Суду України у справі щодо Міністерства фінансів України № 7-р/2018 [18] стало важливим орієнтиром у сфері захисту персональних даних. Суть справи полягала у перевірці конституційності положень законодавства, які надавали Міністерству фінансів України широкі повноваження щодо доступу до персональних даних громадян у рамках адміністрування державних реєстрів, зокрема Єдиного реєстру отримувачів соціальної допомоги. Заявники стверджували, що такі положення порушують право на приватність, гарантоване статтею 32 Конституції України, оскільки передбачають можливість обробки даних без належного обґрунтування, чітких меж та гарантій захисту.

На думку Конституційного Суду України, Міністерство може бути наділене повноваженнями щодо отримання та обробки інформації, що містить персональні дані, лише для досягнення легітимної мети. Проте, через відсутність будь-яких меж дискреції, встановленої законом, щодо подальших дій з інформацією, яка містить персональні дані, унеможливується навіть мінімальний захист суб'єкта персональних даних, не забезпечується передбачуваність застосування окремих положень абзацу першого пункту 40 розділу VI «Прикінцеві та перехідні положення» Кодексу. Конституційний Суд України зазначив, що оспорюваними положеннями Кодексу не передбачено критеріїв визначення змісту та обсягу інформації, що містить персональні дані, категорій осіб як суб'єктів персональних даних, проміжків часу, яких мають стосуватися персональні дані, строків, порядку та умов їх зберігання.

Таким чином, чітко не встановлено меж повноважень Міністерства як центрального органу виконавчої влади при здійсненні ним повноважень з контролю за дотриманням бюджетного законодавства в частині моніторингу пенсій, допомог, пільг, субсидій, інших соціальних виплат, що унеможливує настання відповідальності держави за можливі зловживання.

Тож, Конституційний Суд України сформулював низку ключових правових позицій на основі даного рішення. По-перше, Суд наголосив на принципі законності обробки персональних даних: будь-яке втручання у право на приватність має бути чітко врегульоване законом, який повинен бути передбачуваним і відповідати принципу правової визначеності. По-друге, Суд підкреслив принцип пропорційності, зазначивши, що втручання у право на приватність має бути мінімально необхідним для досягнення легітимної мети. Законодавство, яке надає Міністерству фінансів необмежений доступ до персональних даних, було визнано таким, що порушує цей принцип, оскільки не встановлює чітких меж втручання.

Крім того, Суд звернув увагу на необхідність дотримання принципу мінімізації даних, тобто обробка має здійснюватися лише у тому обсязі, який є необхідним для досягнення конкретної мети. Відсутність чітких критеріїв для визначення обсягу даних створює ризики надмірного втручання у приватне життя громадян. Також Суд наголосив на обов'язку держави забезпечувати належний рівень захисту персональних даних, зокрема через впровадження ефективних організаційно-технічних заходів та механізмів контролю за їх обробкою.

Рішення Суду стало важливим прецедентом, який зобов'язав законодавця внести зміни до нормативно-правових актів з метою усунення виявлених недоліків. Воно також визначило основні підходи до регулювання обробки персональних даних, зокрема дотримання принципів законності, пропорційності та мінімізації даних.

Питання захисту персональних даних у сучасному світі є одним із ключових аспектів забезпечення прав людини, особливо в умовах цифровізації та зростання обсягів інформації, що обробляється державними органами.

Конституційні суди різних країн формують власні підходи до вирішення цієї проблематики, які, попри національні особливості, мають спільні риси, зокрема акцент на принципах законності, пропорційності та мінімізації втручання у приватне життя. У даному випадку доцільно

провести паралель між практикою Конституційного Суду України та досвідом Федерального Конституційного Суду Німеччини (Bundesverfassungsgericht) і Конституційної Ради Франції.

Федеральний Конституційний Суд Німеччини у своєму знаковому рішенні у справі про «Цифрову приватність» (Census Act Case, 1983 p.) [19] закріпив фундаментальні принципи захисту персональних даних, які стали орієнтиром не лише для Німеччини, але й для багатьох інших країн. У цій справі Суд розглядав конституційність закону, який регулював проведення перепису населення та передбачав збір великого обсягу персональних даних. Суд визнав, що право на інформаційне самовизначення є невід'ємною складовою права на людську гідність (стаття 1 Основного закону Німеччини) та права на вільний розвиток особистості (стаття 2). Він наголосив, що будь-яке втручання у приватність має бути чітко врегульоване законом, а обробка даних повинна відповідати принципу пропорційності, тобто бути обмеженою лише тими даними, які є необхідними для досягнення конкретної легітимної мети. Це рішення стало основою для формування концепції «інформаційного самовизначення», яка передбачає, що кожна особа має право самостійно вирішувати, які її персональні дані можуть бути зібрані, збережені, використані чи передані. Суд також підкреслив, що масовий збір даних без належних гарантій захисту створює ризик «тотального спостереження», що несумісно з демократичними принципами.

Конституційна Рада Франції у своєму рішенні від 23 липня 2015 року [20] також висловила критичну позицію щодо необмеженого втручання держави у приватне життя громадян. Рада розглядала законодавчі положення, які дозволяли масове зберігання даних без чітких обмежень щодо їх обсягу, строків зберігання та мети використання. У своєму рішенні Рада визнала, що такі положення порушують право на приватність, оскільки вони не забезпечують належного балансу між інтересами національної безпеки та правами громадян. Конституційна Рада наголосила, що масове зберігання даних без чітких критеріїв і гарантій створює ризик зловживань і може призвести до непропорційного втручання у приватне життя. Вона підкреслила, що законодавство має передбачати чіткі межі щодо обсягу даних, які можуть бути зібрані, а також встановлювати прозорі процедури контролю за їх використанням. Це рішення стало важливим кроком у формуванні європейських стандартів захисту персональних даних, які пізніше були закріплені у Загальному регламенті про захист даних (GDPR).

Практика Конституційного Суду України у сфері захисту персональних даних, зокрема у справі щодо повноважень Міністерства фінансів, демонструє схожість із підходами, сформульованими конституційними судами Німеччини та Франції. Як і Федеральний Конституційний Суд Німеччини, Конституційний Суд України наголошує на необхідності дотримання принципу пропорційності при обробці персональних даних. У своєму рішенні Суд підкреслив, що втручання у право на приватність має бути мінімально необхідним для досягнення легітимної мети, а законодавство повинно чітко визначати межі такого втручання. Подібно до Конституційної Ради Франції, Конституційний Суд України звернув увагу на ризики, пов'язані з відсутністю чітких критеріїв і гарантій при обробці персональних даних. Суд зазначив, що законодавство, яке надає державним органам необмежені повноваження щодо доступу до персональних даних, створює загрозу зловживань і порушує принцип правової визначеності. Як і у випадку з Францією, український Суд наголосив на необхідності встановлення чітких меж щодо обсягу даних, строків їх зберігання та процедур контролю.

Порівняльний аналіз практики конституційних судів України, Німеччини та Франції свідчить про спільне прагнення забезпечити ефективний захист персональних даних в умовах сьогодення. Усі три суди наголошують на важливості дотримання принципів законності, пропорційності та мінімізації втручання у приватне життя. Водночас кожна країна має свої особливості правового регулювання, які відображають національні пріоритети та контекст. Досвід Німеччини та Франції може бути корисним для України у вдосконаленні національного законодавства та правозастосовної практики у сфері захисту персональних даних. Зокрема, концепція «інформаційного самовизначення», сформульована Федеральним Конституційним Судом Німеччини, та акцент на прозорості й чітких критеріях, зроблений Конституційною Радою Франції, є важливими орієнтирами для подальшого розвитку української правової системи.

Висновки. У сучасних умовах воєнного стану, який є особливим правовим режимом, питання захисту персональних даних набуває особливої актуальності, оскільки воно перебуває на перетині забезпечення національної безпеки та дотримання фундаментальних прав і свобод людини. Конституційно-правові обмеження, що запроваджуються в умовах воєнного стану, мають відпові-

дати принципам законності, пропорційності, необхідності та тимчасовості, які є основоположними у правовій державі. Водночас гарантії захисту персональних даних повинні залишатися дієвими навіть у надзвичайних умовах, що вимагає вдосконалення правового регулювання, технічних механізмів захисту та правозастосовної практики.

Аналіз чинного законодавства України та практики його застосування виявив низку проблем, які потребують системного вирішення. Найперше це, відсутність спеціального нормативно-правового акта, який би регламентував особливості обробки персональних даних у період воєнного стану, що створює правову невизначеність. Законодавство України не містить чітких положень щодо обсягу, мети, строків зберігання та порядку доступу до персональних даних у надзвичайних умовах. Що призводить до ризиків зловживань з боку державних органів та інших суб'єктів, які здійснюють обробку даних, а також до порушення права на приватність, гарантованого статтею 32 Конституції України. У зв'язку з цим доцільно розробити та ухвалити спеціальний закон, який би визначав правові рамки обробки персональних даних у період воєнного стану, зокрема встановлював обмеження щодо обсягу даних, що збираються, та строки їхнього зберігання, а також передбачав ефективні механізми захисту прав громадян.

Технічний захист баз даних, які містять персональні дані, залишається недостатнім, що створює значні ризики неправомірного доступу, витоку або знищення. Особливо це стосується державних реєстрів, які стають об'єктами кібератак з боку агресора. У цьому контексті необхідно посилити технічні заходи безпеки, зокрема шляхом впровадження сучасних технологій шифрування, багаторівневого доступу, регулярного аудиту інформаційних систем та моніторингу їхньої безпеки. Крім того, слід створити спеціалізовані підрозділи з кіберзахисту, які б забезпечували оперативне реагування на загрози, пов'язані з обробкою персональних даних, та здійснювали постійний моніторинг стану інформаційної безпеки.

Розширення повноважень правоохоронних органів щодо доступу до персональних даних у період воєнного стану потребує ефективного судового контролю. Відсутність прозорих процедур та незалежного нагляду за діями правоохоронних органів створює ризики порушення прав громадян. У зв'язку з цим необхідно запровадити механізми судового та громадського контролю за доступом до персональних даних, а також забезпечити прозорість процедур, пов'язаних із їхньою обробкою. Це може включати обов'язкове інформування громадян про факти доступу до їхніх даних, якщо це не суперечить інтересам національної безпеки, а також створення незалежного органу, який би здійснював нагляд за дотриманням законодавства у сфері захисту персональних даних.

Ще одним важливим аспектом є підвищення рівня правової культури серед населення. Громадяни повинні бути обізнані про свої права у сфері захисту персональних даних, а також про механізми їхнього захисту. Для цього доцільно проводити інформаційно-просвітницькі кампанії, спрямовані на підвищення обізнаності населення щодо правових аспектів обробки персональних даних, особливо в умовах воєнного стану. Це сприятиме формуванню правосвідомості громадян та підвищенню рівня довіри до державних органів.

Нарешті, доцільним є врахування міжнародного досвіду, зокрема практик країн Європейського Союзу, які регулюють захист персональних даних. У цих країнах навіть у надзвичайних ситуаціях зберігається баланс між забезпеченням безпеки та дотриманням прав людини. Україна має запозичити такі підходи, як обмеження обсягу даних, що збираються, встановлення чітких строків їхнього зберігання, а також створення незалежних органів, які здійснюють нагляд за обробкою персональних даних. Зокрема, доцільно розробити механізми, які б забезпечували прозорість дій державних органів у сфері обробки персональних даних, а також гарантували дотримання прав громадян навіть у надзвичайних умовах.

Таким чином, захист персональних даних в умовах воєнного стану є складною та багатогранною проблемою, яка потребує комплексного підходу до її вирішення. Вдосконалення законодавства, посилення технічного захисту баз даних, забезпечення прозорості дій державних органів, впровадження ефективного судового контролю, підвищення рівня правової культури серед населення та врахування міжнародного досвіду є ключовими напрямками, які дозволять забезпечити баланс між національною безпекою та дотриманням прав людини. Лише системний підхід до вирішення цих питань сприятиме формуванню правової держави, яка здатна ефективно реагувати на виклики сучасності, зберігаючи при цьому фундаментальні права і свободи громадян.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Загальна декларація прав людини. *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text.
2. Конвенція про захист прав людини і основоположних свобод (з протоколами) (Європейська конвенція з прав людини). *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text.
3. Міжнародний пакт про громадянські і політичні права. *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/995_043#Text.
4. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних. *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text.
5. Конституція України. *Офіційний вебпортал парламенту України*. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text>.
6. Закон України «Про захист персональних даних». *Офіційний вебпортал парламенту України*. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>.
7. Про затвердження документів у сфері захисту персональних даних. *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text.
8. Загальний регламент про захист даних (GDPR) – GDPR-Text.com. *GDPR-Text.com - GDPR Text, Translation and Commentary*. URL: <https://gdpr-text.com/uk>.
9. Реєстри відновили. Які наслідки кібератаки для України - BBC News Україна. *BBC News Україна*. URL: <https://www.bbc.com/ukrainian/articles/c5ye75y8415o>.
10. Омбудсман України. Захист персональних даних в діяльності суб'єктів владних повноважень. URL: <https://ombudsman.gov.ua/storage/app/media/27012023/37676120-9a08-47d9-a376-b498dd07ede5.pdf>.
11. Solove D.J. Understanding Privacy. Harvard University Press, 2010. 272 p. URL: <https://www.hup.harvard.edu/books/9780674035072>.
12. Reidenberg J. Data privacy law: A study of United States data protection. URL: https://www.academia.edu/27046308/Data_privacy_law_A_study_of_United_States_data_protection.
13. Nissenbaum H. Privacy in Context. Technology, Policy, and the Integrity of Social Life. Stanford Law Books, 2009. 304 p.
14. Max Schrems v. Data Protection Commissioner (CJEU – “Safe Harbor”). URL: <https://epic.org/max-schrems-v-data-protection-commissioner-cjeu-safe-harbor>.
15. Кравчук В. Захист персональних даних в умовах воєнного стану. *Юридичний науковий електронний журнал*. 2022. № 9. С. 319-321. URL: http://lsej.org.ua/9_2022/77.pdf.
16. Попович Т.П. Право особи на захист персональних даних в Інтернеті: теоретико-правові аспекти. *Аналітично-порівняльне правознавство*. 2021. № 2. С. 51–54.
17. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України № 2-рп/2012. *Офіційний вебпортал парламенту України*. URL: <https://zakon.rada.gov.ua/laws/show/v002p710-12#Text>.
18. Рішення Конституційного Суду України у справі за конституційним поданням Уповноваженого Верховної Ради України з прав людини щодо відповідності Конституції України (конституційності) окремих положень абзацу першого пункту 40 розділу VI «Прикінцеві та перехідні положення» Бюджетного кодексу України. *Офіційний вебпортал парламенту України*. URL: <https://zakon.rada.gov.ua/laws/show/v007p710-18#Text>.
19. CensusActCase, 1983p. *Bundesverfassungsgericht*. URL: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html.
20. Décision n° 2015-713 DC du 23 juillet 2015. URL: <https://www.conseil-constitutionnel.fr/decision/2015/2015713DC.htm>.