Захист персональних даних та конфіденційності в умовах військових конфліктів*

Думчиков М.О.[1], Бондаренко О.С.[2]

Опубліковано	Секція	УДК
18.01.2024	Право	004.056.5

DOI: http://dx.doi.org/10.5281/zenodo.10532362

Анотація. Впровадження інформаційно-телекомунікаційних технологій зумовило появу нових видів загроз, зокрема в кібернетичній безпеці. Вони спрямовані, передусім, на системи управління та підтримки прийняття рішень, проте важливу роль відіграють і небезпеки, які пов'язані з персональною інформацією, зокрема, її збиранням, зберіганням та розкриттям. Актуальність цієї проблеми постійно збільшується, оскільки нові інформаційно-телекомунікаційні технології, що впроваджуються в практику обробки відомостей, дозволяють збирати, узагальнювати та інтерпретувати дані, накопичувати їх і передавати, у тому числі по телекомунікаційним мережам, без відома громадян.

У сучасній епохі, де цінність інформації постійно зростає, особливу важливість набуває збір та захист даних під час збройних конфліктів. У статті розглядається ця проблема з двох ключових перспектив: права збройних конфліктів та міжнародного гуманітарного права, а також прав людини загалом.

Враховуючи, що інформаційні ресурси стають об'єктом стратегічних маніпуляцій, акцент робиться на важливості правового захисту інформації під час військових дій. Підкреслюється, як ця проблема впливає на сучасне міжнародне право та вимагає вдосконалення механізмів захисту прав людини та громадянина в умовах збройних конфліктів. Зокрема, наголошується на необхідності адаптації правових рамок до реалій цифрової ери та забезпечення ефективного контролю за використанням інформації військовими силами з урахуванням загальних принципів прав людини.

У статті обговорюється питання законного отримання та захисту персональних даних військовополонених у ході збройних конфліктів. Автори стверджують, що чинне право збройних конфліктів не забезпечує належного захисту персональних даних військовополонених, зокрема, не регулює порядок зберігання, збирання, використання та передачі таких даних.

* *Стаття написана в рамках проєкту Модуль Жана Моне «Досвід ЄС щодо захисту персональних даних у кіберпросторі» (2023-2026 – EUEPPDC – 101125350 – ERASMUS-JMO-2023-MODULE)*

[1] к.ю.н., доцент, ст.викладач кафедри кримінально правових дисциплін та судочинства Навчально-наукового інституту права СумДУ , https://orcid.org/0000-0002-4244-2419

[2] д.ю.н., доцент, завідувачка кафедри кримінально правових дисциплін та судочинства Навчально-наукового інституту права СумДУ , https://orcid.org/0000-0002-2288-1393

Автори пропонують застосовувати до захисту персональних даних військовополонених загальні принципи, норми та правила, які регулюють права та основоположні свободи людини та громадянина.

Ключові слова: персональні дані, конфіденційність, захист персональних даних, право збройних конфліктів, права військовополонених.

Protection of personal data and privacy in the conditions of military conflicts

Abstract. The introduction of information and telecommunication technologies led to the emergence of new types of threats, in particular in cyber security. They are aimed, first of all, at management and decision-making support systems, but the dangers associated with personal information, in particular, its collection, storage and disclosure, also play an important role. The relevance of this problem is constantly increasing, as new information and telecommunication technologies introduced into the practice of information processing allow collecting, summarizing and interpreting data, accumulating and transmitting them, including through telecommunication networks, without the knowledge of citizens.

In today's era, where the value of information is constantly increasing, the collection and protection of data during armed conflicts is of particular importance.

The article examines this problem from two key perspectives: the law of armed conflicts and international humanitarian law, as well as human rights in general.

Given that information resources become the object of strategic manipulation, emphasis is placed on the importance of legal protection of information during military operations. It is emphasized how this problem affects modern international law and requires the improvement of mechanisms for the protection of human and citizen rights in the conditions of armed conflicts. In particular, it is emphasized the need to adapt the legal framework to the realities of the digital age and ensure effective control over the use of information by military forces, taking into account the general principles of human rights.

The article discusses the issue of legal obtaining and protection of personal data of prisoners of war during armed conflicts. The authors claim that the current law of armed conflicts does not provide adequate protection of personal data of prisoners of war, in particular, does not regulate the procedure for storing, collecting, using and transferring such data.

The authors propose to apply the general principles, norms and rules governing the rights and fundamental freedoms of a person and a citizen to the protection of personal data of prisoners of war.

Keywords: personal data, confidentiality, protection of personal data, law of armed conflicts, rights of prisoners of war.

Вступ

Постановка проблеми. У контексті сучасних військових конфліктів дуже гостро стоїть питання захисту персональних даних та конфіденційності осіб, які опиняються під впливом воєнних подій. Зі зростанням кількості інформаційно-телекомунікаційних технологій та засобів масової комунікації у сучасному конфліктному середовищі виникає ризик неправомірного збору, обробки та розголошення персональної інформації. Основна проблема полягає в необхідності розробки ефективних стратегій та правових механізмів для захисту персональних даних військовополонених, забезпечення конфіденційності та відновлення контролю над власною інформацією в умовах кібератак, кібершпигунства та інших викликів, пов'язаних із цифровими технологіями у воєнний час.

Стан дослідження. Питанням щодо проблеми забезпечення захисту персональних даних в умовах військових конфліктів, як складової інформаційної безпеки та внесення вагомого внеску у розв'язання згаданих проблем на теоретичному рівні зробили такі науковці, як С. Єсімов, Т. Обуховська, В Головченко та Х. Ламан. Водночас, проблематика забезпечення захисту персональних даних в умовах збройної агресії Російської Федерації залишається актуальною проблемою.

Мета дослідження полягає в аналізі та визначенні ефективних стратегій та правових механізмів для забезпечення захисту персональних даних та конфіденційності осіб та військовополонених під час воєнних конфліктів. Дослідження спрямоване на розкриття викликів, які виникають у збереженні приватності в умовах військових дій, та розробку пропозицій щодо удосконалення законодавства та практичних заходів для ефективного захисту персональних даних у цих умовах.

Результати

Виклад основного матеріалу. Сьогодні наше суспільство можна вважати таким, що є повністю диджиталізованим і як результат – діяльність на основі інформаційних потоків, потоків даних. Варто наголосити, що поняття даних у цілому закладене в концепцію цифровізації, без цифровізації сьогодні важко уявити жоден процес або систему надання послуг.

Саме тому цілком очевидним є факт того, що експерти з міжнародного гуманітарного права розмірковують, як саме поводитися з інформацією у цифровій формі в межах правових рамок.

Військові конфлікти, виходячи з передумови, що військові операції, які стосуються даних можуть заподіяти набагато більше шкоди , а ніж фізичне знищення об'єктів [1, с. 562].

Кібероперації військового характеру можуть по-різному впливати та на дані громадян, в залежності від засобів проведення та цілей таких операцій. Наведемо декілька сценаріїв того, яким чином персональні дані громадян можуть впливати на розвиток військового конфлікту.

Так, наприклад під час військового конфлікту двох країн, одна з них шляхом несанкціонованого втручання у реєстри державних телекомунікаційних компаній отримує персональні дані клієнтів цієї компанії, зокрема, номера телефонів, реєстраційні данні, ПІБ та інше. Наступним етапом може виступати, ворожа дезінформаційна політика спрямована, припустимо на залучення так би мовити «пасивних» громадян до співпраці з конфліктуючою державою. Основною особливістю в даному конкретному випадку буде виступати персоналізація, тобто адресатами пропонування також «співпраці» будуть цільові громадяни, на основі відомих персональних даних про них.

Ще одним прикладом використання персональних даних під час військового конфлікту можна навести використання шкідливого програмного забезпечення «вимагача». Під час військового конфлікту, одна з держав проводить умисне зараження шкідливим програмним забезпечення здатним криптувати та шифрувати відповідні типи даних, мережу столичних лікарень державного типу власності. Підкреслимо, що таке зараження відбулося через корпоративну мережу, зокрема, шляхом передачі шкідливого програмного коду через імейл. Позиція, сторони конфлікту, яка «заразила» корпоративну мережу полягає у виведенні військ протилежної сторони конфлікту з певної території. До того часу всі файли, які були вражені шкідливим програмним забезпечення будуть знаходитися у режимі криптування, з їх подальшим блокуванням або знищенням. В наведеному прикладі, ні один із пацієнтів лікарні не страждає від

фізичної шкоди, водночас, велика кількість операцій та надання інших медичних послуг є неможливою.

Для розуміння впливу конфіденційності та незахищеності персональних даних в рамках військових конфліктів, пропонуємо розглянути саме поняття «персональних даних».

Відповідно до Закону України «Про захист персональних даних» персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [2].

С. Єсімов зазначає, що захист персональних даних має конституційну природу, є елементом права громадян на повагу до особистого життя, а також правові норми, які регламентують питання захисту персональних даних, охоплюють більшість галузей права [3].

На думку Т. Обуховської, персональні дані – це юридичний термін спеціального призначення. Він означає не просто конфіденційну інформацію, а її конкретний тип, різновид [4].

Аналізуючи сутність права на повагу до особистого та сімейного життя, можна зробити висновок, що терміни «інформація, яка містить персональні дані» та «інформація про приватне життя» мають схожу змістову наповненість і взаємозв'язок, схожий на "ціле та частина". Відповідно до цієї концепції існують два основних підходи до її розуміння: 1) персональні дані включаються до інформації про приватне життя, пояснюючи це тим, що міжнародна практика вважає будь-яку інформацію, яку можна пов'язати з конкретною особою, частиною приватного життя; 2) інформація про приватне життя включається до персональних даних, оскільки не всі відомості можуть містити інформацію про особисте життя (наприклад, стандартні анкетні дані про дату народження або місце проживання).

На наш погляд, доцільним є застосування підходу, в якому інформація про приватне життя та персональні дані розглядаються як "ціле та частина" відповідно. Це можна обґрунтувати наступним чином:
1) за допомогою анкетних даних можна отримати різноманітну інформацію; наприклад, з відомостей про місце проживання можна визначити, у яких відносинах перебувають особи, якщо відомі дані про декілька осіб. Це особливо актуально при спробі встановити родинні зв’язки;
2) за допомогою особистих ідентифікаційних даних, таких як ПІБ та дата народження, за використанням інтернет-ресурсів та телефонних довідників, також можна встановити родинні зв’язки між особами або визначити їх місце проживання.

З урахуванням досягнень правової доктрини та законодавчого забезпечення можна зробити висновок, що поняття та значення персональних даних необхідно постійно досліджувати та удосконалювати, зокрема з огляду на розвиток новітніх технологій. Це є важливим для забезпечення ефективного захисту цих даних.

Міжнародне право щодо захисту конфіденційності інформації розвивається в рамках різних національних, регіональних та міжнародних ініціатив. Загальний регламент захисту персональних даних (далі GDPR) [5], а також Конвенція про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних Ради Європи ґрунтуються на положеннях договорів про права людини, які захищають недоторканність приватного життя, що передували цифровізації суспільства. Так, наприклад Європейська конвенція «Про захист прав людини і громадянина» 1950 р [6]. передбачає захист приватного життя у ст. 8.

GDPR містить низку положень та винятків, які обмежують застосування цього правового акту в умовах національних надзвичайних ситуацій, включаючи можливі озброєні конфлікти. Так, зокрема, стаття 2 GDPR встановлює обмеження на застосування

цього регулюючого акта до обробки персональних даних, які є складовою частиною системи даних. Відзначається, що GDPR не поширюється, ані на питання, пов'язані із захистом основних прав і свобод, які виникають в контексті діяльності, що виходить за рамки права Європейського Союзу, такої як діяльність, пов'язана з національною безпекою, ані на обробку персональних даних державами-членами в ході проведення діяльності щодо спільної зовнішньої та безпекової політики Союзу.

Багато важливих «наборів» особистих даних громадян, які можуть бути потенційно вражені ворожими кібероперaціями під час збройного конфлікту з метою порушення соціальних функцій на території супротивника, вважаються персональними даними (наприклад, акти громадянського стану, страхові дані, медичні інформації, дані про соціальне забезпечення, податкові записи та банківські рахунки). Отже, на перший погляд, ці дані можуть підпадати під дію системи захисту особистих даних, такої як GDPR.

Питання щодо застосування заходів конфіденційності даних в умовах збройного конфлікту залежить від принципів міжнародного права, а не від положень національного чи регіонального законодавства. Навіть у відношенні національних чи регіональних законів, таких як, наприклад, GDPR, виключення на підставі забезпечення національної безпеки не можна допускати.

По-перше, держави можуть посилатися на такі виключення лише у разі наявності реальних, обґрунтованих інтересів у контексті національної безпеки. По-друге, національне законодавство, яке встановлює стандарти захисту прав людини та громадянина, застосовується до держав в інтересах людей, які знаходяться під юрисдикцією цих держав. Для, прикладу, GDPR спрямований на обмеження держав ЄС у порушенні прав на непорушність приватного життя громадян ЄС та інших осіб, які знаходяться під юрисдикцією ЄС. GDPR та його виключення не поширюються за межі території ЄС.

Для міжнародних принципів захисту прав людини, які стосуються конфіденційності даних, не існує виключень у сфері національної безпеки. Таким чином, у випадку збройного конфлікту, навіть якщо держава-член ЄС посилається на виключення GDPR, вони будуть застосовуватися лише до тих, хто перебуває під її юрисдикцією. Громадяни країни-противника не втрачають захисту через виключення, засновані на інтересах національної безпеки. Цей критичний момент, здається, в основному упускається з уваги при обговоренні винятків з GDPR [7].

Зауважимо, що у всіх вище перелічених випадках нормами закону, які регулюють роботу шкідливого програмного коду, будуть вважатися національне кримінальне законодавство, місце вчинення суспільно небезпечного діяння, та місце заподіяння шкоди завданої цим діянням. Водночас, спостерігається відсутність прямого зв’язку з кінетичними діями військового конфлікту, а отже і норми міжнародного гуманітарного права застосовуватися не будуть.

Згідно із статтею 51 Статуту ООН, право на застосування сили (фізичної) можливе в результаті військового нападу. Водночас, порушення кордонів однією державою іншої не призведе до права на самозахист. За аналогією, атака без кінетичного спрямування – несанкціоноване втручання в інформаційно-телекомунікаційну мережу наслідками якої стало «зараження» корпоративної мережі шкідливим програмним кодом «вірус вимагач» підпадає під статтю 51 Статуту ООН не більше ніж введення економічних санкцій, які лише опосередковано можуть призвести до смерті людей. На нашу думку кібернаслідки так як і економічні, не можуть бути оцінені як «військовий напад» [8].

Враховуючи той факт, що сьогодні наша держава знаходиться в стані військового конфлікту з Російською Федерацією, питання законного отримання персональних даних про військовополонених, які можуть бути зібрані утримувачою стороною, постає

особливо гостро. Отримання персональних даних про осіб, які були затримані в розрізі військового конфлікту має першочергове значення. На самому базовому рівні для органу, який здійснює затримання, дуже важливо знати країну походження військовополоненого та іншу ідентифікуючу інформацію для своїх власних записів. Відповідно до женевської конвенції, сторони конфлікту повинні повідомляти інформації про військовополоненого – державі його громадянства, його сім'ї або заінтересованій стороні, наприклад, Міжнародний комітет Червоного Хреста [9].

Інформація про особисті речі, які перебували у військовополонених, їх фізичне та психічне – усе це становить значний обсяг інформації, яку можна зібрати щодо військових які опинилися у полоні. Водночас, варто наголосити, що такі дані мають виключно персональний характер, а отже можуть бути неправильно використані державою, яка утримує військовополоненого, проти нього самого або членів його сім'ї. При цьому, а ні Женевська Конвенція, а ні право збройних конфліктів не містить правил, щодо зберігання, збирання та використання таких персональних даних їх передача зацікавленій у конфлікті стороні. Зокрема не врегульована процедура передачі отриманих персональних даних військовополонених, які є громадянами іншої не конфліктуючої держави, однак було у складі ворожої армії, іншій державі, громадянином, якої є така особа під час її переведення.

Аналогічна ситуація існує по відношенню приватного життя військовополонених, сьогодні все на чому акцентується увага у праві військових конфліктів виступають норми, які захищають військовополонених від «образ». Враховуючи, що правила та норми права військових конфліктів фактично не регулюють захист персональних даних військовополонених в зазначених ситуаціях. Вбачаємо за необхідність застосування загальних принципів, норм та правил, щодо регулювання прав та основоположних свобод людини та громадянина задля усунення цих прогалин.

Режими захисту даних, зокрема GDPR, надають гарантії того, що персональні дані підпадають під суворі правила обробки. Зокрема, ці правила включають в себе заборону на обробку персональних даних, які розкривають расове чи етнічне походження, політичні погляди, релігійні чи філософські переконання, або членство у профспілках. Також забороняється обробка генетичних даних, біометричних даних з метою однозначної ідентифікації фізичної особи, даних про здоров'я, або даних щодо сексуального життя чи сексуальної орієнтації фізичної особи [6].

Згідно з GDPR, також встановлені заходи захисту, які надають особам право, зокрема, на видалення їхніх даних. Це свідчить про суворий контроль над передачею персональної інформації третім особам. Ці правила, ймовірно, здатні усунути ряд прогалин, що існують у правових каркасах щодо збору та захисту даних. Водночас, ці норми можуть бути відповідними як у мирний, так і у воєнний час, забезпечуючи ефективний контроль над обробкою особистих даних та забезпечуючи їхню конфіденційність.

Список використаних джерел

1. Geiß R., Lahmann H. Protection of data in armed conflict. *International law studies.* 2022. Vol. 97. P. 555–572.
2. Закон України: Про захист персональних даних від 01.06.2010 № 2297-VI (редакція від 27.10.2022). URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
3. Єсімов С. С. Захист персональних даних у контексті розвитку динамічних інформаційних систем. URL: http://www2.lvduvs.edu.ua/documents_pdf/visnyky/nvsy/03_2013/13yessdis.pdf

4. Обуховська Т. І. Захист персональних даних в умовах розвитку інформаційного суспільства: передумови, принципи та міжнародне законодавство. URL: http://visnyk.academy.gov.ua/wpcontent/uploads/2014/05/2014-1-17.pdf
5. Головченко В. Правові основи захисту персональних даних. URL: http://yur-gazeta.com/publications/practice/inshe/pravovi-osnovi-zahistu-personalnihdanih.html
6. Regulation (eu) 2016/679 of the European Parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation). URL: https://gdpr-info.eu/
7. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text
8. O'Connell M.E. Data privacy rights : the same in war and peace. The rights to privacy and data protection in times of armed conflict / ed. by R. Buchan and A. Lubin. – Tallinn, 2022. – P. 12–29.
9. United Nations Charter. URL: https://www.un.org/en/about-us/un-charter/full-text
10. Женевська Конвенція «Про поводження з військовополоненими». URL: https://zakon.rada.gov.ua/laws/show/995_153#Text