УДК 342.9

Онищенко В.В., аспірант кафедри цивільного, господарського та екологічного права;
Потіп М.М., д.ю.н., професор, професор кафедри цивільного, господарського та екологічного права
(Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна)

ОБРОБКА ПЕРСОНАЛЬНИХ ДАНИХ В УМОВАХ ВОЄННОГО СТАНУ

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, наголошують Я.Г. Худолєй та Н.А. Загребельна [1].

В умовах введеного в Україні воєнного стану захист персональних даних від випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних, захист державних інформаційних ресурсів, ІТ-систем об'єктів критичної інфраструктури, державних реєстрів, які містять персональні дані є вкрай важливими. Обробка персональних даних має бути пропорційною та здійснюватися для конкретних і законних цілей, наголошує Уповноважений Верховної Ради з прав людини [2].

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 [2]. Основними моментами, зауважують Я.Г. Худолєй та Н.А. Загребельна 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: 1) право на обробку здійснюється органами, які визначені у Законі України «Про правовий режим воєнного стану»; 2) не повинен бути перевищений строк, форма та порядок обробки даних; 3) має діяти тільки щодо певного набору даних та в межах повноважень [1].

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 [3].

Проєкт Закону про захист персональних даних № 8153 от 25.10.2022 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 [4]. Я.Г. Худолєй та Н.А. Загребельна зазначають, що проект закону зазначає про неможливість 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 [1].

У контексті воєнних дій, зазначають Я.Г. Худолєй та Н.А. Загребельна, 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 [1].

На сьогодні інститут захисту персональних даних знаходиться на етапі становлення та адаптації до норм Європейського Союзу та до реалій правового режиму воєнного стану в Україні.

Список використаних джерел:

1. Худолєй Я.Г., Загребельна Н.А. Захист персональних даних у період дії в Україні правового режиму воєнного стану: загальнотеоретичні аспекти. URL: https://doi.org/10.31732/2708-339X-2023-08-75-82

2. Уповноважений Верховної Ради з прав людини. Щодо захисту персональних даних в умовах воєнного стану. URL: https://ombudsman.gov.ua/storage/app/media83.pdf

3. Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану. Постанову КМУ від 12 березня 2022 р. № 263. URL: https://zakon.rada.gov.ua/laws/show/263-2022-%D0%BF#Text

4. Проект Закону України «Про захист персональних даних» № 8153 от 25.10.2022. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/40707