

DOI <https://doi.org/10.30525/978-9934-26-409-2-76>

**PERSONAL DATA PROTECTION IN THE FIELD OF LIFE
SAFETY: LEGAL REGULATION AND EUROPEAN STANDARDS**

**ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ ЗАБЕЗПЕЧЕННЯ
БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ: ПРАВОВЕ РЕГУЛЮВАННЯ
ТА ЄВРОПЕЙСЬКІ СТАНДАРТИ**

Bondar D. V.

*Candidate of Science in Public
Administration, Rector
Lviv State University of Life Safety
ORCID: 0009-0004-9571-7828
Lviv, Ukraine*

Бондар Д. В.

*кандидат наук з державного
управління, ректор
Львівський державний університет
безпеки життєдіяльності
ORCID: 0009-0004-9571-7828
м. Львів, Україна*

В сучасному світі інформаційні технології проникли майже у всі сфери суспільного життя. Фактично кожна людина має смартфон та є активним користувачем Інтернет. Все більшої популярності набувають соціальні мережі та месенджери, яким людина часто довіряє свої персональні данні, починаючи від анкетних даних та особистих фотографій і закінчуючи службовою інформацією, яка пересилається між співробітниками органів публічної адміністрації.

Водночас цифровий формат даних, які розміщуються в соціальних мережах, пересилаються засобами електронної пошти та через мобільні застосунки (месенджери), робить їх відкритими для інших користувачів, які часто переслідують протиправні цілі. Крім того, люди часто добровільно надають персональну інформацію різноманітним інформаційним ресурсам комерційних компаній, банків, державних установ та організацій, і така інформація також часто стає загальнодоступною.

Незахищеність персональних даних значною мірою впливає на безпеку життєдіяльності, адже заволодіння персональними даними сторонніми особами із протиправною метою може призвести до вкрай негативних наслідків, включаючи отримання зловмисниками доступу до банківських рахунків особи, використання фото та відеоматеріалів для шантажу (з погрозами поширити конфіденційну, інтимну інформацію), створення клонів сторінок певної особи у соціальних мережах та здійснення від її імені певної діяльності (збирання коштів на

нібито лікування та інші потреби; здійснення психологічного тиску на родичів та знайомих з метою схилити їх до певних дій; поширення матеріалів, які дискредитують особу тощо).

Не поодинокими є випадки здійснення від імені особи, персональні дані якої викрадено, терористичної діяльності, вчинення інших злочинів проти національної безпеки.

Таким чином, захист персональних даних у сфері забезпечення безпеки життєдіяльності є одним із завдань національних органів публічної адміністрації. Правовою основою виконання даного завдання є Закон України «Про захист персональних даних». Вказаний закон регулює правові відносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних. Він поширюється, у тому числі, на діяльність з обробки персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів [1].

Мета обробки персональних даних має бути сформульована в законах, інших нормативно-правових актах, положеннях, установчих чи інших документах, які регулюють діяльність володільця персональних даних, та відповідати законодавству про захист персональних даних. Обробка персональних даних здійснюється для конкретних і законних цілей, визначених за згодою суб'єкта персональних даних, або у випадках, передбачених законами України, у порядку, встановленому законодавством (ст. 6 Закону України «Про захист персональних даних») [1].

Враховуючи євроінтеграційні прагнення України, важливим є дотримання європейських стандартів у сфері захисту персональних даних.

В Європейському Союзі у 2016 році прийнято Загальний регламент про захист даних (General Data Protection Regulation, GDPR). Цей загальноєвропейський акт розширює повноваження держав у сфері соціальних мереж – дозволяє видаляти незаконний контент і змушує платформи докладати більше зусиль для боротьби з небезпечними матеріалами [2].

Загальний регламент захисту даних (GDPR) є найсуворішим законом про конфіденційність і безпеку в світі. Незважаючи на те, що він був розроблений і прийнятий в Європейському Союзі, він накладає зобов'язання на підприємства, установи та організації незалежно від місця їх знаходження, якщо вони націлені або збирають дані, пов'язані із громадянами держав-членів ЄС.

Загальний регламент захисту даних (GDPR) набув чинності 25 травня 2018 року. GDPR передбачає стягнення значних за розміром штрафів за порушення стандартів конфіденційності та безпеки, причому штрафи можуть сягати десятків мільйонів євро. За допомогою вказаного акту Європейський Союз демонструє свою тверду позицію щодо необхідності захисту конфіденційності та безпеки даних у той час, коли все більше людей довіряють свої особисті дані хмарним сервісам (службам), а порушення у цій сфері є щоденним явищем [3].

Особливу увагу необхідно приділити питанню захисту персональних даних в процесі використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності.

Так, в Україні наразі відбувається тестування Системи оповіщення та реагування «Я – Доброволець».

Вказана система являє собою інноваційну платформу, яка включає в себе базу даних, операційну систему та мобільний застосунок. Її ідея полягає в тому, щоб кожен бажачий зміг завантажити на свій смартфон або комп'ютер мобільний застосунок «Я – доброволець», надати свої анкетні дані та згоду на залучення до ліквідації надзвичайних ситуацій та їх наслідків. Адміністрування Системи оповіщення та реагування «Я – Доброволець» будуть здійснювати фахівці Державної служби України з надзвичайних ситуацій. В подальшому, у разі виникнення надзвичайної ситуації всі зареєстровані в базі даних Системи добровольці будуть отримувати сповіщення про місце, час виникнення та характеристики надзвичайної ситуації. Оповіщення буде здійснюватися з урахуванням місцезнаходження (геолокації) добровольців, що дозволить сповістити та залучити в першу чергу тих осіб, які проживають або знаходяться поблизу місця події або місця локалізації наслідків надзвичайної ситуації. Таким чином буде забезпечена швидка мобілізація людських ресурсів для ліквідації надзвичайної ситуації та її наслідків. Завдяки сучасним інформаційним технологіям, зокрема, мобільним месенджером з функцією відеозв'язку, спеціалісти ДСНС України зможуть в режимі онлайн координувати дії добровольців на місці події, давати поради та застерігати від небезпечних дій до приїзду основних підрозділів рятувальників.

Реалізація такого проєкту дозволить проявити соціальну активність всім бажачим громадянам, долучитися до рятувальної справи та набутти вмінь та навичок ліквідації надзвичайних ситуацій та їх наслідків. Натомість органи ДСНС України отримають додаткові сили та засоби цивільного захисту у вигляді бази даних добровольців та

реальну допомогу в процесі ліквідації кожної конкретної надзвичайної ситуації.

Отже, враховуючи функціонування загальнодержавної системи цивільного захисту в умовах правового режиму воєнного стану, необхідно забезпечити належний рівень захисту персональних даних добровольців, які вносять відомості про себе в інформаційну базу Системи оповіщення та реагування «Я – доброволець».

На рівні спільного наказу МВС України та Міністерства цифрової трансформації України доцільно затвердити порядок функціонування Системи оповіщення та реагування «Я – доброволець» та заходи щодо криптографічного захисту персональних даних добровольців, які внесені до бази даних вказаної Системи.

Література:

1. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. Дата оновлення: 27.10.2022. URL: <https://zakon.rada.gov.ua/laws/show/2297-17/ed20221027#Text> (дата звернення: 07.02.2024).
2. Снопко О. Як Верховний суд США поступово стає регулятором у сфері соціальних мереж. Опора. Tech. 10.03.2023. URL: https://www.oporaua.org/polit_ad/iak-verkhovnii-sud-ssha-postupovo-staie-reguliatorom-u-sferi-sotsialnikh-merezh-24609 (дата звернення: 07.02.2024).
3. What is GDPR, the EU's new data protection law? GDPR.EU. URL: <https://gdpr.eu/what-is-gdpr/> (дата звернення: 07.02.2024).