Пастернак М. С.,
кандидат юридичних наук, старший консультант-аналітик Департаменту інформаційно-аналітичного забезпечення,
Служба безпеки України
(м. Київ, Україна)

Лісов О. С.,
кандидат історичних наук, доцент кафедри управління та інформаційно-аналітичного забезпечення оперативно-службової діяльності,
Національна академія Служби безпеки України
(м. Київ, Україна)

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ПІД ЧАС ОСІНТ-ДІЯЛЬНОСТІ СУБ'ЄКТІВ РОЗВІДУВАЛЬНОГО СПІВТОВАРИСТВА УКРАЇНИ

У цифрову епоху структури розвідки і контррозвідки все більше покладаються на ОСІНТ для збору важливих відомостей з метою забезпечення національної безпеки. І хоча розвідка з відкритих джерел націлена на відкриту інформацію, вона не оминає низку етичних та правових питань, особливо щодо захисту персональних даних.

Відповідно до ЗУ «Про захист персональних даних» персональними даними є відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [6]. Набір персональних даних має забезпечувати точну ідентифікацію особи, бути унікальним і виключати варіативність отриманого результату. Тому якщо відомості містять виключно прізвище, ім'я та по батькові, які є поширеними, і стосуються декількох осіб, вони не відносяться до персональних даних. Навіть наявність дати народження разом із прізвищем, ім'ям та по батькові в певних випадках не виключає варіативності ідентифікації.

Водночас у сукупності пов'язаних відомостей про фізичну особу наявність хоча б одного елемента, який дозволяє однозначно її ідентифікувати, перетворює усю множину на персональні дані. У такому випадку будь-які додаткові відомості про ідентифіковану особу стають персональними даними.

При цьому, можливість або неможливість ідентифікації особи є суб'єктивною. Тут потрібно враховувати як фактори якості і повноти наявних до ідентифікації даних, так і сучасний стан розвитку методів, засобів ОСІНТ та спроможностей суб'єктів розвідувального співтовариства України (далі – суб'єкти ОСІНТ) у своєму максимумі. Наприклад, якщо за допомогою фото

вдалося безваріативно ідентифікувати особу, таке зображення підпадатиме під персональні дані.

Набуття відомостями ознак персональних даних породжує нові права і обов'язки, накладає додаткові вимоги до їхнього захисту. За цих обставин визначальним аспектом є об'єктивація суб'єктивної «можливості чи неможливості ідентифікації особи». Оскільки найбільш вивіреною та правдивою ідентифікація особи буде з використанням державних реєстрів, то саме з моменту отримання інформації про особу з такого джерела чи доповнення нею здобутого раніше обсягу відомостей фіксується виникнення правовідносин захисту персональних даних. Ідентифікація, що передує цьому, є попередньою і юридичних наслідків не несе.

В ОСІНТ-діяльності ідентифікація особи базується на вторинних джерелах відомостей про фізичну особу, тобто тих, які здобуті розвідувальним шляхом і правдивість яких не підтверджена безпосередньо особою зацікавленості або її документами. На відміну від вторинних джерел, первинними джерелами відомостей про фізичну особу є видані на її ім'я документи, підписані нею документи, а також відомості, які особа надає про себе (Порядок обробки та захисту персональних даних в Службі безпеки України, затверджений наказом ЦУ СБУ від 20.08.2025 № 322) [3]. Незалежно від джерела таких відомостей персональні дані, що обробляються, є інформацією з обмеженим доступом, крім випадків визначених законом [3; 6]. Обробка персональних даних в інформаційно-комунікаційних системах СБУ допускається виключно в авторизованих системах з безпеки або шляхом отримання сертифіката відповідності стандарту інформаційної безпеки, виданого органом з оцінки відповідності (ст. 8 ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах») [3; 5].

Необхідно підкреслити, що поєднання відомостей про фізичну особу і подальша остаточна ідентифікація особи за допомогою держреєстрів базується на технічних спроможностях суб'єкта ОСІНТ і не має доказової сили в досудовому розслідуванні без проведення експертизи. Наприклад, висновок аналітика про тотожність особи на зображеннях, зроблений на основні результатів їх аналізу за певною методикою або з використанням спеціалізованих програмних продуктів, для набуття ознак доказу потребуватиме висновку судового експерта.

Окремо слід зауважити, що персональні дані не стосуються юридичної особи. Проте, ОСІНТ-результат – це комплексний документ, в якому відображаються зв'язки організації або компанії із її засновниками, бенефіціарами, працівниками, контрагентами та іншими фізичними особами, встановлення яких також здійснює ОСІНТ-дослідник. Відтак у завданнях, що стосуються юридичної особи, ОСІНТ-результат здебільшого буде містити персональні дані пов'язаних фізичних осіб. У таких випадках відомості про участь ідентифікованих або можливих до ідентифікації фізичних осіб в тих чи інших організаціях, як і будь-які відомості про самі організації, пов'язані з такими особами, вважатимуться персональними даними.

Захист персональних даних забезпечується процедурою обмеження доступу до конфіденційної інформації. При цьому, персональні дані можуть бути віднесені до конфіденційної інформації про особу законом або відповідною особою (ч. 2 ст. 5 ЗУ «Про захист персональних даних») [6]. Законодавець відносить до конфіденційної інформації про особу, зокрема, дані щодо її національності, освіти, сімейного стану, релігійних переконань, стану здоров'я, а також адреси, дати та місця народження (ч. 2 ст. 11 ЗУ «Про інформацію») [7]. Водночас, він не обмежує зазначений перелік. Тобто, за замовчуванням усі персональні дані особи є конфіденційною інформацією за винятком тих, які особа добровільно оприлюднює і жодним чином не обмежує до них доступу. Своєю чергою, дії щодо збереження персональних даних, навіть об'єктивно недостатні, свідчать, що особа воліла б їх обмежити в доступі.

Деякі персональні дані законодавчо заборонено відносити до конфіденційної інформації. Це зокрема:

- прізвища, імена, по батькові фізичних осіб, які отримали бюджетні кошти, отримали у володіння, користування чи розпорядження державне та/або комунальне майно (ч. 5 ст. 6 ЗУ «Про доступ до публічної інформації») [1];
- персональні дані, що стосуються здійснення особою, яка займає посаду, пов'язану з виконанням функцій держави або органів місцевого самоврядування, посадових або службових повноважень (ч. 2 ст. 5 ЗУ «Про захист персональних даних») [6];
- персональні дані, зазначені у декларації особи, уповноваженої на виконання функцій держави або місцевого самоврядування (ч. 6 ст. 6 ЗУ «Про запобігання корупції») [2] і т.д.

Тобто персональні дані не можна обмежувати в доступі у випадках, коли їхній суб'єкт залучений до публічно-правових відносин і суспільний інтерес доступу до них переважає ймовірну шкоду від їхнього поширення. Але в цьому випадку персональні дані не позбавлені певного ступеня узагальнення і, ймовірно, не включатимуть РНОКПП, адреси реєстрації і проживання, але можуть містити дані біографії (освіта, кваліфікація, досвід державної служби тощо).

Ч. 1 ст. 11 ЗУ «Про інформацію» ототожнює персональні дані та інформацію про фізичну особу [7]. Проте, більш спеціалізований ЗУ «Про захист персональних даних» у ст. 2 такого ототожнення не притримується [6]. Враховуючи принцип переваги спеціальної норми над загальною до конфіденційної інформації про фізичну особу за межами персональних даних відносимо будь-яку інформацію про особу, що обмежена нею у доступі і не дозволяє ідентифікувати таку особу методами ОСІНТ. Отже, персональні дані, які є конфіденційною інформацією, і конфіденційна інформація про особу, яка не є персональними даними, однаково захищаються шляхом дотримання процедури обмеження доступу до конфіденційної інформації.

Таким чином, обробка персональних даних, зокрема в межах наданих законодавцем повноважень зі спеціального оброблення інформації з відкритих джерел, інформаційних систем, обліків, реєстрів, баз даних (п. 14 ч. 1 ст. 12

ЗУ «Про розвідку»), має здійснюватися із суворим дотриманням прав на приватне життя, належним дотриманням законів про захист персональних даних і етичних зобов'язань структур розвідки і контррозвідки [8]. Балансуючи між інтересами національної безпеки і правом на недоторканність приватного життя, суб'єкти ОСІНТ повинні розробляти політики і найкращі практики, які б забезпечували дотримання вимог законодавства про захист персональних даних, зберігаючи при цьому оперативну ефективність.

Список використаних джерел:

1. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI : станом на 08.08.2025. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 14.10.2025).
2. Про запобігання корупції : Закон України від 14.10.2014 № 1700-VII : станом на 12.09.2025. URL: https://zakon.rada.gov.ua/laws/show/1700-18#Text (дата звернення: 14.10.2025).
3. Про затвердження Порядку обробки та захисту персональних даних в Службі безпеки України : Наказ Центрального управління Служби безпеки України від 20.08.2025 № 322 : станом на 20.08.2025. URL: https://ips.ligazakon.net/document/RE44740?an=1 (дата звернення: 14.10.2025).
4. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : Постанова Каб. Міністрів України від 29.03.2006 № 373 : станом на 18.04.2025. URL: https://zakon.rada.gov.ua/laws/show/373-2006-п#Text (дата звернення: 14.10.2025).
5. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР : станом на 20.04.2025. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення: 14.10.2025).
6. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI : станом на 14.06.2025. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 14.10.2025).
7. Про інформацію : Закон України від 02.10.1992 № 2657-XII : станом на 14.06.2025. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 14.10.2025).
8. Про розвідку : Закон України від 17.09.2020 № 912-IX : станом на 30.10.2024. URL: https://zakon.rada.gov.ua/laws/show/912-20#Text (дата звернення: 14.10.2025).