# 1 Правове забезпечення захисту інформації. Проблеми розвитку нормативної та методичної баз системи захисту інформації

**УДК 35.078:342.738**

## ПРАВОВІ АСПЕКТИ ОРГАНІЗАЦІЇ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ ВІДПОВІДНО ДО МІЖНАРОДНИХ СТАНДАРТІВ

***Олексій Мервінський, Костянтин Мельник***

*Державна служба України з питань захисту персональних даних*

*Анотація*: **На сьогоднішній день питання організації захисту персональних даних правоохоронними органами є надзвичайно важливим. З моменту ратифікації Україною базових міжнародних стандартів у сфері захисту персональних даних дане питання потребує постійного дослідження та аналізу, адже ефективне виконання владних повноважень правоохоронними органами в Україні нерозривно пов'язане із забезпеченням права на приватне життя особи та захисту її персональних даних.**

*Summary*: **Today, the issue of personal data protection by the law enforcement agencies is essential. Since the ratification by Ukraine of the basic international standards in the field of the personal data protection this issue requires the constant research and analysis, as the effective power of law enforcement in Ukraine is inseparably linked with the rights of individual on privacy and the protection of its personal data.**

*Ключові слова*: **Персональні дані, захист персональних даних, правоохоронна діяльність, правоохоронні органи, міжнародні стандарти.**

### I Вступ

Аналіз та визначення правових аспектів організації захисту персональних даних у сфері правоохоронної діяльності є вельми актуальним з огляду на складність та суттєву специфіку даного питання. Враховуючі факт нестримного зростання діяльності правоохоронних органів в житті людини, що, в свою чергу, обумовлено новими загрозами для суспільства, пов'язаними з тероризмом, торгівлею людьми, наркотиками, організованою злочинністю тощо, а також загальним зростанням злочинності, стала ще більш очевидною необхідність встановити чіткі правила для правоохоронних органів, які б визначили необхідний баланс, якого потребує наше суспільство, між правом особи на приватне життя і законними діями правоохоронних органів, коли останні обробляють персональні дані.

Зростання технологічного прогресу значною мірою полегшує роботу правоохоронних органів. В галузі, де обробка величезної кількості персональних даних необхідні у зв'язку з широкомасштабною і важливою функцією правоохоронних органів в суспільстві, переваги, які будуть отримані від використання технологій, очевидні.

Тим не менш, проблеми, які спонукали до розробки Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних 1981 року в зв'язку з більш широким використанням автоматизованих методів обробки персональних у всіх галузях, найбільш гостро відчуваються в діяльності правоохоронних органів, адже саме в цій галузі наслідки порушення основних принципів, викладених у Конвенції, можуть найбільш сильно вплинути на життя людини. З огляду на зазначене необхідно знайти баланс між задіяними інтересами людини та її правом на приватне життя та інтересами суспільства у попередженні та припиненні злочинів і підтриманні громадського порядку.

### II Основна частина

1 червня 2010 року Верховна Рада України прийняла Закон України №2297-VI «Про захист персональних даних» (далі – Закон), який створив належні правові засади забезпечення захисту персональних даних в Україні та привів законодавство України відповідно до міжнародних стандартів, зокрема, Конвенції Ради Європи № 108 про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо

органів нагляду та транскордонних потоків даних, ратифікованих 6 липня 2010 року Законом України № 2438-VI (далі – Конвенція № 108 та Додатковий протокол до неї).

Статтею 1 Закону визначається сфера його дії: Закон регулює відносини, пов'язані із захистом персональних даних під час їх обробки. Разом з цим зазначається, що дія цього Закону не поширюється на діяльність зі створення баз персональних даних та обробки персональних даних у цих базах: фізичною особою – виключно для непрофесійних особистих чи побутових потреб; журналістом – у зв'язку з виконанням ним службових чи професійних обов'язків; професійним творчим працівником – для здійснення творчої діяльності. Жодних застережень (обмежень) щодо поширення його сфери дії на діяльність правоохоронних органів зі створення баз персональних даних та обробки персональних даних Закон не містить.

Міжнародні стандарти в сфері захисту персональних даних відносять більшість персональних даних, що обробляються правоохоронними органами, з огляду на певну специфіку їх діяльності, до категорії так званих «чутливих» персональних даних, зокрема про расове або етнічне походження людини, політичні, релігійні та світоглядні переконання, членство в політичних партіях або професійних спілках тощо. Цим, зокрема, і пояснюється важливість застосування особливих та додаткових правових гарантій захисту персональних даних під час їх обробки правоохоронними органами, адже чим більша чутливість та особливість персональних даних, тим більшим стає ризик порушення прав осіб на їх приватне життя.

Відповідно до статті 6 Конвенції № 108 персональні дані, що свідчать про расову приналежність, політичні, релігійні чи інші переконання, а також дані, що стосуються здоров'я або статевого життя, не можуть піддаватись автоматизованій обробці, якщо внутрішнє законодавство не забезпечує відповідних гарантій. Це правило також застосовується до персональних даних, що стосуються засудження в кримінальному порядку. Проте, статтею 9 цієї ж Конвенції дозволяється виключення зі статті 6 тоді, коли таке відхилення передбачене законодавством Сторони та є в демократичному суспільстві необхідним заходом, спрямованим на захист державної та громадської безпеки, фінансових інтересів Держави або на боротьбу з кримінальними правопорушеннями.

Особливості обробки так званих «чутливих» персональних даних визначені і статтею 7 Закону. Виходячи з аналізу положень статті 7 можна зробити висновок, що обробка таких персональних даних можлива, якщо вона «стосується обвинувачень у вчиненні злочинів, вироків суду, здійснення державним органом повноважень, визначених законом щодо виконання завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом».

Детальне роз'яснення положень статті 9 Конвенції № 108 міститься у Рекомендації Комітету Міністрів Ради Європи № (87) 15 «Про захист персональних даних у секторі поліції» (1987 р.). Рекомендацією визначаються 8 базових принципів захисту персональних даних у секторі поліції[1].

Принципи, що містяться в цій рекомендації поширюються на збір, зберігання, використання та передачу персональних даних для поліцейських цілей, які є предметом автоматичної обробки.

В цій Рекомендації термін «персональні дані» охоплює будь-яку інформацію, що стосується ідентифікованої особи. Особа не може розглядатися як «ідентифікована», якщо ідентифікація вимагає занадто багато часу, витрат і трудових ресурсів. Термін «для поліцейських цілей» охоплює всі завдання, які поліцейські повинні виконати для попередження і припинення кримінальних злочинів і підтримки громадського порядку.

Держава – член Ради Європи, яка ратифікувала Конвенцію № 108, може застосовувати принципи, що містяться в цій рекомендації до персональних даних, що не піддаються автоматизованій обробці. Проте, ручна обробка персональних даних не дозволяється, якщо її мета полягає в тому, щоб уникнути положень цієї рекомендації.

Перший принцип стосується контролю за обробкою персональних даних. Згаданий принцип полягає в тому, що існує необхідність мати незалежний наглядовий орган за межами сектора поліції, який повинен нести відповідальність за забезпечення дотримання принципів, викладених у цій рекомендації. На цей же наглядовий орган повинна бути покладена функція реєстрації файлів (баз) персональних даних, що будуть оброблятися для поліцейських цілей. Крім цього, не повинно існувати таємних файлів (баз) персональних даних як таких, що невідомі громадськості.

[1] З урахуванням сучасних реалій в Україні згадані принципи слід застосовувати до всього спектру органів державної влади, залучених до сфери правоохоронної діяльності, а не обмежувати їх застосування лише до органів Міністерства внутрішніх справ України, оскільки питання обвинувачень у вчиненні злочинів, вироків суду, виконання завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом в Україні належать до компетенції різних правоохоронних органів.

Другий принцип визначає особливі аспекти збору персональних даних. Збір персональних даних для поліцейських цілей має бути обмежений до такої міри, яка необхідна для запобігання реальній загрозі або припиненню конкретного кримінального злочину. Будь-яке виключення з цього положення має стати предметом конкретного національного законодавства. Як тільки об'єкт діяльності поліції більше не зможе завдати шкоди, фізичну особу необхідно поінформувати (у разі збирання і зберігання даних про цю особу без її згоди) про місце зберігання інформація про неї або видалення (знищення) цих даних. Збір персональних даних про осіб, виключно на тій підставі, що вони мають расову приналежність, релігійні переконання, сексуальну поведінку або політичні переконання або належать до конкретних рухів чи організацій, не заборонених законом, має бути заборонено. Збір даних за цими позиціями може бути здійснено тільки в разі нагальної потреби для цілей персональних запитів правоохоронних органів.

Третій принцип стосується зберігання персональних даних. В міру можливості зберігання персональних даних для поліцейських цілей має бути обмежене точністю даних і відноситись до таких даних, які необхідні органам поліції для виконання своїх законних завдань у рамках національного законодавства і своїх зобов'язань, що випливають з міжнародного права. Різні категорії персональних даних, що зберігаються, повинні розрізнятися відповідно за їх ступенем точності і надійності і, зокрема, дані, засновані на фактах, слід відрізняти від даних на основі думки або особистої оцінки. Персональні дані, які були зібрані для адміністративних цілей, і які повинні зберігатися постійно, повинні бути збережені в окремий файл. Ці дані повинні зберігатися окремо від даних, зібраних для адміністративних цілей, у тому числі і про адміністративні правопорушення.

Четвертий принцип визначає, що персональні дані, які збираються і зберігаються поліцією для поліцейських цілей, повинні використовуватися виключно для цих цілей, тобто для запобігання або припинення злочинів або підтримки суспільного порядку. Це, в свою чергу, не означає, що дані з поліцейських баз не можуть передаватися іншим органам, оскільки зазначену функцію можуть виконувати і інші органи державної влади.

П’ятий принцип визначає особливості передачі персональних даних поліцейськими органами: у поліційному секторі (передача даних між поліцейськими органами, які будуть використовуватися для поліцейських цілей, допустиме, якщо існують законні підстави для такої передачі і вона не виходить за рамки правових повноважень цих органів), державним органам, приватним особам, іноземним суб’єктам, пов’язаним з персональними даними. Правовою підставою для передачі таких персональних даних є наявність двох або багатосторонніх домовленостей між державами. Також принципом врегульовані питання умов та гарантій передачі таких даних.

Принцип шостий регламентує право суб’єкта персональних даних на ознайомлення і виправлення помилкових даних. Наглядовий орган повинен вжити заходів, аби упевнитися в тому, що громадськість було поінформовано про існування файлів, які є предметом подання відповідного повідомлення, а також про свої права відносно до цих файлів. Реалізація цього принципу має враховувати специфіку спеціальних файлів: необхідність запобігти серйозній шкоді продуктивності вирішення завдань, що належать до компетенції органів поліції. Права на доступ, виправлення і знищення персональних даних мають бути обмежені тільки тією мірою, якою обмеження є необхідною передумовою для виконання безпосередніх завдань поліції, або якщо це необхідно для захисту суб'єкта даних або прав і свобод інших осіб. Варто зазначити, що національним правовим механізмом має бути знайдений баланс між таємним характером обробки персональних даних з метою боротьби зі злочинністю та принципом доступу до персональних даних.

Сьомий принцип стосується тривалості зберігання персональних даних. Відповідно до цього принципу персональні дані, що збирались з визначеною метою, після досягнення визначеної мети повинні знищуватись. З цією метою, зокрема, слід приділити увагу наступним критеріям: необхідність зберігання даних у світлі висновків розслідування конкретної справи; остаточного судового рішення, зокрема, звільнення від покарання; реабілітації; засуджень, що проводились; амністій; вік суб'єкта даних, окремих категорій даних.

Восьмий принцип стосується забезпечення захисту персональних даних від незаконної обробки та незаконного доступу до них. Відповідальний орган повинен вжити всіх необхідних заходів для забезпечення відповідної фізичної та логічної безпеки даних і запобігання несанкціонованого доступу, передачі або зміни.

## III Висновки

Підсумовуючи вищезазначене варто зауважити, що згадані рекомендації в цілому належним чином імплементовані в національне законодавство України. Проте, подальшого вирішення потребують наступні питання:

- забезпечення реєстрації всіх баз персональних даних правоохоронних органів у Державному реєстрі баз персональних даних, не повинно існувати таємних баз персональних даних;

- створення механізмів нагляду (контролю) з боку уповноваженого органу з питань захисту персональних даних (Державної служби України з питань захисту персональних даних) за дотриманням правоохоронними органами встановлених законом вимог щодо обробки персональних даних;

- запровадження механізмів контролю з боку громадськості за обробкою персональних даних через уповноважений орган з питань захисту персональних даних.

Важливим аспектом також залишається приведення законодавства, яке регламентує діяльність правоохоронних органів України, у відповідність до Закону України «Про захист персональних даних».

Відповідно до статті 2 Закону володілець бази персональних даних – фізична або юридична особа, якій законом або за згодою суб'єкта персональних даних надано право на обробку цих даних, яка затверджує мету обробки персональних даних у цій базі даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом. Загальні та особливі вимоги щодо обробки персональних даних визначені в статтях 6 та 7 Закону. Відповідно до вимог Закону персональні дані, отримані в ході роботи правоохоронних органів, повинні бути точними, достовірними і в разі необхідності – оновлюватися. Склад та зміст персональних даних мають бути відповідними та не надмірними стосовно визначеної мети їх обробки. Також відповідно до статті 6 Закону мета обробки персональних даних має бути сформульована в законах, інших нормативно-правових актах, положеннях, установчих чи інших документах, які регулюють діяльність володільця бази персональних даних. Обробка персональних даних має здійснюватися для конкретних і законних цілей, визначених за згодою суб'єкта персональних даних, або у випадках, передбачених законами України, в порядку, встановленому законодавством. Захист персональних даних покладається на володільця бази персональних даних. На дії володільця бази персональних даних поширюються усі вимоги щодо захисту персональних даних від незаконної обробки, а також від незаконного доступу до них.

Отже, законодавство, що регламентує діяльність правоохоронних органів, обов'язково повинно враховувати:

- чітку мету обробки персональних даних у базі персональних даних (наприклад, з метою забезпечення особистої безпеки громадян, захист їх прав і свобод, законних інтересів тощо);

- склад персональних даних (наприклад, прізвище, ім'я, по батькові (інші імена, псевдоніми, прізвиська), дата і місце народження, національність, стать, обставини здійснення або підготовки до вчинення злочинів, засоби здійснення злочинів, підозрюване членство у злочинній групі тощо);

- процедури обробки персональних даних у базах персональних даних з урахуванням специфіки обробки персональних даних у сфері правоохоронної діяльності.

*Література:* ***1.*** *Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних //* www.rada.gov.ua ***2.*** *Закон України «Про захист персональних даних» //* www.rada.gov.ua ***3.*** *Порівняльно-правове дослідження відповідності законодавства України законодавству ЄС у сфері персональних даних / В. М. Брижко, А. І. Радянська, М. Я. Швець. – К.: Тріумф, 2006. – 256 с.*

**УДК 351.745.7:343.9:007**

# ІНФОРМАЦІЙНИЙ ДЕТЕРМІНІЗМ В НАУКАХ КРИМІНАЛЬНОГО ЦИКЛУ У СВІТЛІ БУТСТРАП-КОНЦЕПЦІЇ

***Дарія Прокоф'єва-Янчиленко***
*Служба безпеки України*

*Анотація*: **Стаття присвячена питанням інформаційного детермінізму в науках кримінального циклу (кримінальному праві, кримінології, криміналістиці тощо), які пропонується розглядати з точки зору концепції бутстрапу, застосованої до феномену злочинності.**

*Summary*: **The article is devoted to the problem of doctrine ofinformational necessity in the sciences of criminal cycle (criminallaw, criminology, criminalistics etc.), which is offered forconsideration in a context of the bootstrap-concept, applied to thephenomenon of criminality.**

*Ключові слова*: **Детермінізм, причинність, інформація, інформаційний зв'язок, інформаційна безпека, кримінологічна безпека, злочинність, бутстрап, система, суспільство.**

## І Вступ

«Після військової глобальної небезпеки над людством висять дві інші: екологічна і кримінальна» – так наприкінці 90-х років минулого століття писав відомий російський кримінолог В. Лунєєв [1]. За останні 15 років мало що змінилось, і відповідна тенденція не лише збереглась, але й набула загрозливих обрисів, що