А.В. Пазюк

ЗАХИСТ ПРАВ ГРОМАДЯН У ЗВ'ЯЗКУ З ОБРОБКОЮ ПЕРСОНАЛЬНИХ ДАНИХ У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ: ЄВРОПЕЙСЬКІ СТАНДАРТИ І УКРАЇНА

МГО "Прайвесі Юкрейн"

Київ 2001

УДК 342.721.:681.3.067]:006(100)
ББК 67.312.1
П 12

ISBN

Це видання присвячується проблемі захисту прав громадян на приватність персональних даних у зв'язку з діяльністю правоохоронних органів. Розглядається питання приведення чинного законодавства України у цій галузі у відповідність до загальновизнаних норм і стандартів з метою забезпечення ефективної реалізації громадянами свого конституційного права на недоторканність приватного життя (захист приватності), а також сприяння повноцінній участі нашої держави у співробітництві з європейськими країнами у справі боротьби із злочинністю.
Видання містить збірку правових стандартів, які відбивають європейські уявлення і підходи до вирішення цієї болючої як для України, так і інших молодих демократичних країн, проблеми вдосконалення роботи правоохоронних органів з урахуванням вимог захисту прав людини.
Це видання покликано вказати на можливі шляхи розв'язання існуючих проблем і буде корисним для політиків, службовців правоохоронних органів, спеціалістів у галузі міжнародного права і міжнародних відносин, адвокатів і пересічних громадян, які зітхаються з порушеннями своїх прав як державними органами України, так і установами іноземних країн відповідальними за боротьбу із злочинністю.

Подяка

Видання цієї книги стало можливим завдяки люб'язно наданій фінансовій допомозі з боку Посольства Королівства Нідерландів в Україні, яке через свої програми сприяє демократичним перетворенням в нашій державі.

This edition was published thanks to the kindly given financial support of the Royal Netherlands Embassy in Ukraine which throw its programms contributes to democratic changes in our country.

ISBN

ЗМІСТ

Вступ

В останні десятиріччя злочинність змінила своє обличчя вийшовши за рамки національних кордонів. В сучасний час міжнародна спільнота усвідомлює, що боротьба з тероризмом, наркобізнесом і відмиванням брудних грошей, торгівлею людьми і корупцією, це справа не однієї країни, а всього людства. А успіх боротьби проти міжнародної злочинності залежатиме від узгодженості правоохоронної діяльності національних структур і їх взаємної допомоги.

Відкриття залізної завіси, яка відділяла нашу державу від інших країн, політичні і суспільно-економічні перетворення всередині України і пов'язані з цим соціально-економічні проблеми спричинили значне підвищення мобільності людського і фінансового капіталу. Разом з позитивними надбаннями для економіки, які несе в собі відкритість кордонів для руху товарів, послуг і робочої сили, виникають нові проблеми, які створюють значні складності у роботі правоохоронних органів. Така суспільна хвороба наднаціонального характеру як транскордонна злочинність охопила нові незалежні країни, що виникли на теренах колишнього Радянського Союзу. Не оминула вона й Україну, яка знаходиться на шляху між Європою і Азією, а тому зазнає активної інфільтрації з боку злочинних угрупувань.

З огляду на це актуальним являється питання співробітництва нашої держави з європейськими країнами у галузі правоохоронної діяльності, що передбачає, насамперед обмін інформацією і взаємну допомогу національних підрозділів, які займаються боротьбою із злочинністю.

Прагнення України співробітничати з Європейським Союзом у цій галузі зустрічає схвалення і підтримку з боку політичних фігур, які відповідальні за визначення спільних пріоритетів зовнішньої і внутрішньої політики країн ЄС. Під час самміту Україна-Європейський Союз у Ялті, 11 вересня 2001 року така позиція пролунала у спільній заяві Президента України Л.Д. Кучми та Президента Європейської Ради Г. Вергофстадта, за участі Генерального секретаря Ради ЄС, Високого представника з питань спільної зовнішньої та безпекової політики ЄС, а також Президента Комісії Європейських Співтовариств Р. Проді:

"... Ми висловили наше спільне бажання боротися з організованою злочинністю, відмиванням грошей, нелегальним транспортуванням наркотиків та зброї, а також тісно співпрацювати у питаннях нелегальної імміграції, біженців, контрабанди та транспортування людей.

Ми домовилися просувати співробітництво у сфері юстиції та покарань для досягнення практичних результатів, які б віталися громадянами України та ЄС.

Ми будемо намагатися завершити План дій України - ЄС з юстиції та внутрішніх справ до кінця 2001 року. Цей План дій надасть можливість Україні та Європейському Союзу співпрацювати разом над реалізацією цінностей та принципів свободи, безпеки та правосуддя"[1].

Однак співробітництво між органами, які здійснюють боротьбу із злочинністю в Україні, і європейськими поліцейськими установами буде неможливим, якщо правове регулювання правоохоронної діяльності в Україні не відповідатиме встановленим в Європі стандартам і нормам захисту прав людини. Зокрема, йдеться про правові стандарти поводження з інформацією персонального характеру у галузі правоохоронної діяльності.

Отже, ставлячи перед правоохоронним органами Україні завдання досягнення у своїй діяльності відповідних європейських стандартів, слід подбати про впровадження в національне нормативно-правове регулювання цієї діяльності принципів поваги до прав людини, зокрема, права на приватність інформації персонального характеру.

Інший, не менш важливий аспект цього питання також вимагає своєї уваги і вжиття відповідних заходів не лише внутрішньополітичного, а і зовнішньополітичного характеру. Заборона збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної

[1] Інформація з офіційного серверу МЗС України; http: //www.mfa.gov.ua/information/?mfa/ua_ukr.html (веб-сторінка відвідувана 25.10.01р.)

безпеки, економічного добробуту та прав людини, проголошена в Статті 32 Конституції України, вимагає створення регулятивного механізму ефективної реалізації і захисту права на приватність від можливих порушень як з боку органів державної влади України, правоохоронних органів тощо, так і з боку відповідних установ інших держав, у тому числі країн ЄС.

Йдеться про практику збирання і опрацювання персональних даних про громадян України, які перетинають кордони Шенгенської зони, які шукають притулку або іммігрують до країн Європейського Союзу, вчинили правопорушення або злочини, стали їх свідками або жертвами на території цих країн та в інших випадках. Нерідко неточні або застарілі відомості про громадян України, що містяться в поліцейських інформаційних системах країн ЄС, недотримання громадянами України певних вимог при оформлені в'їзних документів і під час перебування на території країн Європейського Союзу, призводять до несправедливого обмеження їх прав і свобод, насамперед, права на в'їзд (виїзд) і працевлаштування, затримання, арешту і депортації тощо.

Один з таких випадків, який трапився 28 липня 2001 року на угорсько-австрійському кордоні мав наслідком відмову групі українських громадян (53 особи), які мали дійсні Шенгенські візи у в'їзді на територію Австрії. Причиною відмови у в'їзді в Австрію стало те, що під час перевірки запрошень, відомості про приймаючу сторону не підтвердилися. Тільки чотирьом громадянам України було поновлено візи, решта була вимушена повернутися в Україну[2].

Нажаль, більшість громадян неспроможна ефективно захистити свої права самотужки через незнання механізму звернення до відповідальних органів та оскарження неправомірних дій правоохоронних органів інших держав. Розв'язання цієї проблеми, яка має зовнішньополітичне забарвлення, виявляється неможливим за браком відповідних положень у вітчизняному законодавстві, а також через відсутність дієвого контролю за додержанням прав громадян щодо обробки персональних даних у діяльності правоохоронних органів України. Важливою функцією контрольного механізму у цій галузі має стати міжнародне співробітництво як на двосторонній, так і багатосторонній основах, з країнами Європейського Союзу; а однією із задач – сприяння громадянам України у реалізації і захисті їх прав стосовно обробки персональних даних на території цих країн.

Розділ перший цієї книги присвячується європейським правовим стандартам поводження з інформацією персонального характеру у правоохоронній діяльності, а також проблемам застосування принципів захисту приватності з урахуванням особливостей правоохоронної діяльності.

У другому розділі йдеться про співробітництво країн Європейського Союзу у галузі створення простору свободи, безпеки та правосуддя, а також про правове регулювання використання інформаційних систем для забезпечення такого співробітництва. Дається загальний опис функціонування поліцейських інформаційних систем, заснованих зокрема, на Шенгенській Конвенції 1990 року і Конвенції Європолу 1995 року. Крім того, аналізуються нормативно-правові положення, які регламентують операції з обробки персональних даних в цих системах, а також під час передачі інформації до третіх країн. Це безпосередньо стосується нашої держави, враховуючи необхідність все більш активної співпраці з правоохоронними структурами Європейського Союзу, зокрема, у галузі інформаційного забезпечення діяльності державних органів України, що борються із злочинністю.

Розділ третій нашого видання присвячується питанням вдосконалення і приведення законодавства України в галузі регулювання обробки персональних даних у правоохоронній діяльності у відповідність до європейських норм і стандартів.

У Додатку дається переклад основних документів (витягів), на які є посилання в описовій частині цієї книги: положень про співробітництво правоохоронних органів країн Європейського Союзу, документів Ради Європи про принципи обробки персональних даних в поліцейській діяльності. Наводяться приклади вирішення справ за цією

[2] Прес-реліз брифінгу з актуальних питань зовнішньої політики // Прес-служба МЗС України. – 31 липня 2001р.; http: //www.mfa.gov.ua/information/?press/foreign/20010731.html (веб-сторінка відвідувана 25.10.01р.)

тематикою Європейським Судом з прав людини, а також рішення Конституційного Суду Російської Федерації по справі про перевірку конституційності Федерального закону "Про оперативно-розшукову діяльність".
Це видання покликано вказати на можливі шляхи розв'язання існуючих проблем і буде корисним для політиків, службовців правоохоронних органів, спеціалістів у галузі міжнародного права і міжнародних відносин, адвокатів і пересічних громадян, які зітхаються з порушеннями своїх прав як державними органами України, так і установами іноземних країн відповідальними за боротьбу із злочинністю.

Розділ 1. Захист прав громадян у зв'язку з обробкою персональних даних у правоохоронній діяльності: європейський вимір

1.1. Правовий механізм захисту прав людини стосовно обробки інформації персонального характеру: європейська модель регулювання

Питання захисту прав людини під час обробки персональних даних у сучасній правовій доктрині європейських країн охоплюються концепцією права на приватність (right to privacy – англ.).
Це фундаментальне право, гарантоване серед інших міжнародних документів у галузі прав людини Європейською Конвенцією про захист прав людини і основних свобод 1950 року, Стаття 8 якої проголошує:

1. Кожна людина має право на повагу до її особистого і сімейного життя, житла і таємниці кореспонденції.
2. Держава не може втручатися у здійснення цього права інакше ніж згідно із законом та у випадках, необхідних у демократичному суспільстві в інтересах національної та громадської безпеки або економічного добробуту країни, з метою запобігання заворушенням і злочинам, для захисту здоров'я або моралі чи з метою захисту прав і свобод інших людей.

В текстах спеціальних міжнародно-правових актів у галузі захисту прав людини стосовно обробки інформації персонального характеру для позначення фундаментального права людини на контроль за поводженням з персональними даними також використовується термін "приватність"[3].
Право на справедливе поводження з інформацією персонального характеру визнається складовою частиною права на недоторканність приватного життя в Конституції України. Стаття 32 Конституції України проголошує:

"Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України.
Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.
Кожний громадянин має право знайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не є державною або іншою захищеною законом таємницею.
Кожному гарантується судовий захист права спростовувати недостовірну інформацію про себе і членів своєї сім'ї та права вимагати вилучення будь-якої інформації, а також право на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням такої недостовірної інформації."

Право на приватність інформації персонального характеру забезпечує правовий зв'язок між людиною і його "інформаційним портретом", відомостями про особу, які свідомо або несвідомо залишаються після кожного контакту людини з навколишнім світом. Бажання людини контролювати циркуляцію інформації персонального характеру в своєму соціальному оточенні безпосередньо пов'язано з такими категоріями як честь і репутація, недоторканність приватного життя. Розвиток інформаційної складової права на приватність був і залишається спрямованим на забезпечення контролю за цілісністю і достовірністю цього "інформаційного портрету" особи.

Сучасний правовий механізм регулювання відносин з обробки, тобто збирання, зберігання, використання, передачі або знищення персональних даних включає такі складові елементи як: принципи правомірності обробки, права суб'єкта даних (особи, якої стосується інформація персонального характеру), принципи легітимного обмеження прав суб'єктів даних, обов'язки інших суб'єктів цих відносин, система нагляду за додержанням законності обробки і захисту прав суб'єктів даних.
Стаття 5 Конвенції Ради Європи "Про захист осіб стосовно автоматизованої обробки персональних даних" 1981 року № 108 вказує на такі принципи правомірності обробки, "якості" персональних даних з точки зору законності:

- отримуються та обробляються правомірно та законно;
- зберігаються для визначених і законних цілей та не використовуються у спосіб несумісний з цими цілями;
- мають бути адекватними, відповідними не надмірними з точки зору цілей, заради яких вони зберігаються;
- мають бути точними та у разі необхідності мають поновлюватися;
- зберігаються у формі, що дозволяє ідентифікувати суб'єктів даних не довше, ніж це необхідно для цілі, заради якої такі дані зберігаються.

[3] Про поширення концепції права на приватність на відносини з обробки персональних даних зазначається у частині третій преамбули Конвенції Ради Європи № 108 "Про захист осіб стосовно автоматизованої обробки персональних даних" (м. Страсбург, 28 січня 1981 року), а також у пункті десятому преамбули до Директиви № 95/46 СЕ Європейського Парламенту і Ради "Про захист фізичних осіб стосовно автоматизованої обробки персональних даних та безперешкодного руху цих даних" (м. Люксембург, 24 жовтня 1995 року).
В текстах міжнародних документів, а також національних законодавчих актів країн Європейського Союзу для позначення правового механізму захисту прав осіб щодо обробки персональних даних часто використовується більш лаконічний термін "data protection", який буквально перекладається як "захист даних" (англ.). Хоча під цим розуміється саме захист прав громадян у зв'язку з обробкою персональних даних. Тобто йдеться, насправді про захист інформаційних прав і свобод, а не про захист інформації.

Стаття 6 Конвенції передбачає особливий режим певних категорій даних, зокрема, тих, що свідчать про расову приналежність, політичні погляди або релігійні чи інші переконання, а також персональні дані, що стосуються здоров'я або статевого життя, кримінальних вчинків, з огляду на загрозу їх використання для дискримінації індивідів за тією чи іншою ознакою.
Стаття 8 Конвенції передбачає гарантії для суб'єкта даних для ефективної реалізації права на приватність інформації персонального характеру, які включають такі правові можливості:

- бути ознайомленим про існування файлів персональних даних, умови їх обробки, у тому числі про особу, яка визначає цілі обробки і є відповідальною за додержання правил обробки, так званого "контролера файлу";
- одержувати підтвердження обробки і ознайомлюватися з самою інформацією, що обробляється;
- вимагати виправлення або знищення персональних даних, які обробляються з порушенням вказаних принципів; і нарешті,
- звертатися за правовим захистом у разі порушення відповідних прав контролером файлу.

Підвищення рівня захисту приватності у порівнянні з існуючими стандартами, зокрема, Конвенцією Ради Європи № 108, - таку мету не приховують розробники Директиви 95/46 СЕ Європейського Парламенту і Ради "Про захист фізичних осіб стосовно автоматизованої обробки персональних даних та безперешкодного руху цих даних" 1995 року.
У вступній частині Директиви вказується: "… принципи захисту прав і свобод, зокрема, права на приватність, що містяться в цій Директиві, уточнюють і розширюють принципи Конвенції Ради Європи від 28 січня 1981 року "Про захист осіб стосовно автоматичної обробки персональних даних". У додаток до запроваджених Конвенцією Ради Європи № 108 принципів, Директива передбачає наступні положення.
Так, стаття 11 Директиви встановлює, що у разі отримання персональних даних не від самого суб'єкта даних, а з інших джерел, суб'єкт даних має бути сповіщеним про цілі збору і обробки, її одержувачів, наявність права доступу та виправлення даних. Стаття 12 Директиви передбачає право суб'єкта даних вимагати сповіщення третім особам про зміну, знищення чи блокування інформації, що її було сповіщено раніше. А стаття 14 Директиви надає особі право заперечувати обробці персональних даних за певних обставин та заборонити використання даних у цілях рекламної діяльності чи прямого маркетингу.
Крім того, Директива ЄС встановлює нові правила, які до цього не містилися у Конвенції Ради Європи 1981 року. Ідеться про рішення, що їх приймають автоматизовані системи під час оцінки якостей людини на основі аналізу інформації, що стосується цієї людини. Директива надає особам право ознайомитися з логічною формулою, що її використовує така система (стаття 12), і право оскаржити таке рішення (стаття 15). Ці положення були запозичені з законодавства про захист персональних даних Франції, яке відображає ідею захисту людини перед "бездушною" машиною.
Директивою ЄС запроваджується процедура попереднього сповіщення контролером (особою, яка визначає цілі обробки і є відповідальною за додержання правил обробки) про заплановану обробку наглядовій інстанцій. Відповідні відомості вносяться до реєстру, який веде наглядовий орган. Така процедура має на меті забезпечити гласність цілей обробок і основних умов її здійснення для перевірки їх відповідності положенням національного законодавства і запобігання можливим порушенням.
Встановлена також процедура попереднього контролю, за якою держави мають встановлювати, обробка яких персональних даних може становити підвищений ризик для безпеки осіб, та проводити їх перевірки до початку обробки даних (стаття 20). До того ж, запроваджується механізм внутрішнього контролю за обробкою. З цією метою, контролер

(особа, яка визначає цілі обробки і є відповідальною за додержання правил обробки) зобов'язаний призначити службовця, який буде контролювати додержання правил обробки. Це нововведення прийшло до тексту Директиви з відповідних положень законодавства Німеччини.
Окремі вимоги встановлені щодо "вразливих даних". Дані, які за своє природою несуть підвищений ризик їх використання не на користь людині, тобто здатні завдати шкоди її основним свободам і безпеці, за загальним правилом не повинні піддаватися обробці. Стаття 8 Директиви ЄС містить загальну заборону на обробку даних, що розкривають расове або етнічне походження, політичні погляди, релігійні або філософські переконання, членство у профспілках, а також даних стосовно стану здоров'я або статевого життя суб'єкта даних.
Іншим не менш принциповим є положення Директиви ЄС про заборону передачі даних до третіх країн, що не забезпечують адекватного рівня захисту. Цим, зокрема, встановлюється, що для транскордонних потоків даних з країн Європейського Союзу, від одержувача даних у третій країні вимагається надання достатніх гарантій щодо дотримання ним вимог Директиви ЄС.
Хоча Директива ЄС, в силу того, що прийнята в рамках "першої колони" права Європейського Союзу, на сьогоднішній день не застосовується до обробки персональних даних в цілях боротьби із злочинністю, її вплив відчувається й на "третю колону", якою охоплюються питання національної безпеки і підтримання правопорядку. Принцип заборони передачі даних до третіх країн, що не забезпечують адекватного рівня захисту, застосовується до передачі персональних даних під час правоохоронної діяльності поліцейських установ країн Європейського Союзу. Зокрема, відповідні вимоги щодо надання адекватного рівня захисту прав суб'єктів даних не нижчого за рівень захисту, передбачений Конвенцією Ради Європи "Про захист осіб стосовно автоматизованої обробки персональних даних" 1981 року № 108, містяться в "третій колоні" права Європейського Союзу, у тому числі Шенгенській Конвенції, Конвенції Європол тощо.
Отже, співробітництво правоохоронних органів України з поліцейськими установами і органами юстиції країн Європейського Союзу, зокрема, взаємний інформаційний обмін неможливий доки законодавство України в цій частині не буде приведено у відповідність до вимог Конвенції Ради Європи 1981 року і Директиви Європейського Союзу 1995 року.

1.2. Обмеження права на приватність інформації персонального характеру в цілях боротьби із злочинністю

Інтерес людини відчувати свою автономію в суспільстві, яка захищається правом на приватність (недоторканність приватного життя), знаходиться у діалектичному протиріччі

з певними інтересами інших осіб і суспільства, зокрема у забезпеченні безпеки і добробуту, захисті прав і свобод інших осіб. Заради цих інтересів здійснюється боротьба із злочинністю під час якої не рідко відбувається втручання у приватне життя. Однак це діалектичне протиріччя не може бути вирішено відкиданням одних інтересів на користь іншим. Для його розв'язання вимагається оцінка задіяних інтересів і їх узгодження.

Цей безперечний постулат явно відображається в конструкції деяких статей Європейської Конвенції про захист прав людини і основних свобод. Як і Статті 9, 10 та 11 Конвенції, Стаття 8 складається з двох частин. Перша частина вказує на права, які підлягають захисту, а друга – зазначає на можливі обмеження чи виключення з проголошених прав.

Зокрема, Стаття 8 Європейської Конвенції про захист прав людини і основних свобод вказує на такі інтереси, що конкурують з правом особи на приватність:

- інтереси національної та громадської безпеки;
- економічного добробуту країни;
- запобігання заворушенням і злочинам;
- захисту здоров'я або моралі;
- захисту прав і свобод інших людей.

Стаття 32 Конституції України вказує на інтереси національної безпеки, економічного добробуту та прав людини як можливу підставу для обмеження права на приватність інформації персонального характеру, що є цілком виправданим, оскільки право на повагу до приватного життя як ширше за правовим змістом може зазнавати більших обмежень, ніж право на приватність інформації персонального характеру, яке є його складовою частиною.

Це підтверджується, зокрема, положеннями спеціальних міжнародно-правових документів, присвячених захисту права на приватність інформації персонального характеру. Стаття 9 вищевказаної Конвенції Ради Європи "Про захист осіб стосовно автоматизованої обробки персональних даних" 1981 року № 108 передбачає, що відступ від положень, що гарантують права суб'єкта даних, дозволяється в інтересах державної безпеки та громадського спокою, грошових інтересів держави або для боротьби із кримінальними злочинами та для захисту прав і свобод інших осіб. А стаття 13 Директиви 95/46 СЕ Європейського Парламенту і Ради "Про захист фізичних осіб стосовно автоматизованої обробки персональних даних та безперешкодного руху цих даних" 1995 року гласить, що обмеження можуть застосовуватися, якщо це є необхідним заходом для забезпечення: державної безпеки, оборони, громадського порядку, в інтересах слідства, важливого економічного або фінансового інтересу, захисту суб'єкта даних або прав і свобод інших осіб. Як вбачається, цьому переліку обмежень майже тотожні відповідні положення статті 32 Конституції України.

Отже, правове регулювання питань обробки персональних даних в діяльності правоохоронних органів покликано визначити рамки реалізації права на приватність з урахуванням інтересів суспільства у приборканні злочинності.

Правова конкуренція задіяних інтересів, особи - у захисті приватності інформації персонального характеру, з однієї сторони, і суспільства – у здійснені обробки персональних даних (у тому числі в цілях боротьби із злочинністю), з другої сторони, покладає на державу зобов'язання щодо визначення, встановлення і підтримання балансу цих інтересів. Європейський Суд з прав людини, даючи тлумачення Статті 8 Європейської Конвенції про захист прав людини і основних свобод, так окреслив це зобов'язання держави у рішенні по справі "*Рііс проти Сполученого Королівства* " [4]:

"З'ясовуючи, чи існує позитивне зобов'язання, слід враховувати, що між загальним інтересом суспільства і інтересами окремої особи *повинна бути встановлена справедлива рівновага*, пошук якої – характерна риса усієї Конвенції.

[4] Rees vs. the United Kingdom. - Judgment of 17 October 1986 // Judgments and decisions. - Series A no. 106

Розглядаючи справи про порушення права на повагу до приватного життя, Європейський Суд з прав людини здійснює оцінку відповідності застосованих обмежень цього права зазначеним у частині другій Статті 8 Європейської Конвенції про захист прав людини і основних свобод вимогам. Ці обмеження повинні:

- *запроваджуватися на підставі закону (“in accordance with the law”);*
- *мати легітимну ціль (“legitimate aim”);*
- *бути необхідними у демократичному суспільстві (“necessary in a democratic society”).*

Загальним критерієм для встановлення балансу між конкуруючими інтересами є дотримання принципу пропорційності при впроваджені обмежень. Цей принцип був сформульований Європейським Судом з прав людини під час розгляду справи “*Сільвер та інші проти Сполученого Королівства*” у 1983 році[5]:
“… фраза “бути необхідним у демократичному суспільстві” означає, щоб бути сумісним з Конвенцією, втручання повинно, серед іншого, відповідати “нагальній соціальній потребі” і бути “пропорційним до законної мети, що переслідується”; і далі
“Закон, що надає свободу вибору під час здійснення повноважень повинен передбачати їх обсяги.”

Аргумент, який часто наводять представники правоохоронних структур під час обговорення питань впровадження принципів захисту приватності інформації персонального характеру в регулювання правоохоронної діяльності, що для успішної боротьби із злочинністю необхідно збирати і опрацьовувати якомога більше відомостей про осіб і бажано у негласний спосіб – не витримує критики. Це так само неправомірно як суцільне стеження, тотальний обшук житла чи огляд усіх транспортних засобів громадян з метою знаходження доказів вчинення злочину, що суперечило б презумпції невинуватості. Правовий зв’язок між особою і її персональними даними, який захищається правом на приватність, не може розриватися свавільно на розсуд державних службовців, у тому числі тих, на які за законом покладаються повноваження здійснювати правоохоронні заходи.
Зрозуміло, що ризик порушення прав людини, і зокрема, права на приватність інформації персонального характеру під час здійснення негласних оперативно-розшукових заходів існує навіть за наявності чітких правових гарантій захисту прав людини, - через недодержання процесуальних норм внаслідок службової недбалості або ж навмисного перевищення повноважень посадовими особами. У випадку ж відсутності детального регулювання питань збирання, використання і знищення інформації персонального характеру, а також відсутності законних гарантій відновлення обмежених під час правоохоронної діяльності прав громадян - такий ризик підвищується значною мірою.
Питання “якості закону”, який покликаний регулювати відносини з обробки персональних даних у правоохоронній діяльності неодноразово розглядалося під час вирішення Європейським Судом з прав людини справ про порушення права на повагу до приватного життя під час здійснення правоохоронними органами оперативно-розшукових заходів, зокрема, прослуховування телефонних розмов.
У справі *“Мелоуні проти Сполученого Королівства”* Суд, знайшовши втручання у права заявника, гарантовані статтею 8 Європейської Конвенції про захист прав людини і основних свобод, дав оцінку, чи було таке втручання у відповідності до вимог, що їх містить частина друга статті 8. Суд постановив наступне[6]:

“Суд знову наголошує, що фраза “у відповідності до закону” відсилає не лише до національного законодавства, але також стосується **якості закону**, яке вимагає його відповідності принципу верховенства права, яке чітко сформульовано у преамбулі до Конвенції... Застосована тут фраза – і це випливає з об’єкту і цілі статті 8 – означає, що

[5] Silver and Others vs. the United Kingdom. - Judgment of 25 March 1983 // Judgments and decisions. - Series A no. 61
[6] Malone vs. the United Kingdom. - Judgment of 2 August 1984 // Judgments and decisions. - Series A no. 82

повинні бути заходи правового захисту у національному законодавстві проти свавільного втручання публічної влади у вказані в частині першій права людини... Особливо, коли повноваження виконавців здійснюються секретно, ризик свавілля не потребує доказування... [Тому] закон повинен бути **достатньо конкретним** у поняттях, щоб надати громадянам адекватну картину щодо обставин в яких і умов за яких, публічна влада уповноважена звернутися до цих секретних и потенційно небезпечних втручань у право на повагу до приватного життя і кореспонденції."

Конкретність закону, серед іншого, означає і передбачуваність щодо його наслідків. Цю вимогу Суд розтлумачив в одному з недавніх рішень, яке має безпосереднє відношення до предмету нашої уваги.
Розглядаючи справу "Аманн проти Швейцарії", Європейський Суд з прав людини встановив, що 12 жовтня 1981 року до заявника, який займався продажем косметичних засобів, зателефонувала жінка з колишнього посольства СРСР у Берні для замовлення одного з таких засобів[7]. Телефонна розмова була підслухана Федеральною прокуратурою, яка за наслідками розслідування проведеного поліцією, завела на заявника секретну картку, що містила інформацію з результатами перевірки у вигляді шифру.
У 1990 році заявнику стало відомо про існування картки. На запит йому була надіслана копія картки, однак певна інформація в ній була викреслена. Заявник звертався до національних органів з метою дізнатися про зміст невідомих для нього даних, однак повною мірою його вимоги задоволені не були, через що він звернувся до Європейського Суду із заявою про порушення права на повагу до приватного життя, гарантованого статтею 8 Європейської Конвенції про захист прав людини і основних свобод.
У цій справі Суд сформулював, якими мають бути правові гарантії під час застосування прослуховування телефонної розмови:

"56. Відповідно до виробленої Судом практики, правило є передбачуваним, якщо воно сформульовано достатньо конкретно для надання будь-якому індивіду за необхідністю відповідної поради для регулювання його поведінки...
Оскільки застосування на практиці заходів негласного стеження за кореспонденцією не є відкритим для ознайомлення зацікавленою особою або громадського загалу, надана законодавством виконавцям свобода дій у необмеженому об'ємі може суперечити принципу верховенства права. Отже, закон повинен визначати межі розсуду компетентних органів і способи їх застосування з достатньою ясністю, з урахуванням легітимної мети їх застосування у конкретному випадку, для надання індивідам адекватного захисту проти свавільного втручання...
61. ... Закон не регулює детально випадки щодо осіб, які підпадають під моніторинг випадково як необхідні учасники в телефонній розмові, яка записується органами влади згідно з цими положеннями. Зокрема, Закон не конкретизує запобігливі засоби, які повинні бути вжиті щодо цих осіб. "

Розглядаючи питання правомірності заведення на заявника картки і її зберігання в картотеці Конфедерації, Європейський Суд з прав людини також знайшов порушення вимог щодо "якості" закону:

"76. ... Директиви Федеральної Ради від 16 березня 1981 року, які мають застосовуватися до обробки персональних даних Федеральною Адміністрацією, встановлюють деякі загальні принципи..., однак не містять жодних відповідних посилань на рамки і умови здійснення владних повноважень наданих прокуратурі щодо збору, запису і зберігання інформації; тим самим вони не визначають умови, за яких картки можуть створюватися, процедуру яка має додержуватися, інформацію, що може збиратися чи коментарі, які забороняються".

[7] Див.: Додаток № __.

Європейський Суд з прав людини дійшов висновку, що право заявника на повагу до приватного життя було порушено внаслідок того, що положення національного законодавства були написані у поняттях дуже загальних щоб задовольнити вимоги передбачуваності щодо телефонного прослуховування і заведення картки на заявника.

Показовими для розуміння питання захисту права людини на приватність інформації персонального характеру, яка збирається і використовується в діяльності правоохоронних органів, є справа розглянута Конституційний Судом Російської Федерації, що стосується перевірки конституційності окремих положень Федерального закону "Про оперативно-розшукову діяльність". Ця справа має звернуту на себе окрему увагу вітчизняних правознавців, оскільки правові традиції регулювання правоохоронної діяльності в Україні і Росії беруть свої коріння в недалекому спільному минулому і навіть через десяток років після відокремлення правових систем формулювання правових приписів в законодавчих актах у цій галузі є досить схожими.

Громадянка Російської Федерації І.Г. Чернова звернулась до Конституційного Суду РФ із скаргою на порушення її конституційних прав положеннями вказаного закону[8]. В червні 1995 року у зв'язку з підготовкою критичних публікацій про роботу волгоградської міліції, журналістка І.Г. Чернова була піддана шантажу з боку посадових осіб УВС Волгоградської області, які погрожували публічно поширити відомості про її приватне життя здобуті оперативним шляхом. Згідно зі статтею 5 Закону РФ "Про оперативно-розшукову діяльність" вона звернулась із скаргою для захисту своїх прав до органів прокуратури і суду. В цей час їй стало відомо, що на підставі "агентурного повідомлення" (частина перша ст. 7 федерального закону) про незаконну підприємницьку діяльність на неї було заведено справу оперативного обліку (ст. 10 федерального закону), здійснювалось спостереження (ст. 6 Федерального закону) з використанням технічних засобів, з ініціативи правоохоронних органів було одержано судове рішення на прослуховування квартирного телефону "для встановлення і документування злочинних зв'язків" (ст.9 Федерального закону).

Після втручання Генеральної прокуратури Російської Федерації їй було повідомлено, що оперативно-розшукові заходи щодо неї були припинені в січні 1996 року, при цьому жодних порушень закону встановлено не було, однак при цьому не було встановлено і самого факту правопорушення з боку І.Г. Чернової або інших осіб. Незважаючи на вимоги заявниці, щодо неї не було прийнято жодних процесуальних рішень ні про порушення, ні про відмову в порушені кримінальної справи, що стало причиною відмови в наданні їй для ознайомлення зібраної про неї інформації (ч.3 статті 5 Федерального закону). Після тривалих і неодноразових вимог судді певна оперативна інформація була направлена у секретному порядку до Волгоградського обласного суду, де розглядалась скарга заявниці. Однак Управління внутрішніх справ віднесло цю інформацію до відомостей, що містять "державну таємницю" (стаття 12 Федерального закону), і з цих підстав заявниці було відмовлено в ознайомлені з ними. Після чого, за "непотребом" оперативні матеріали були повернуті до УВС і знищені у вересні 1997 року на підставі "відомчих інструкцій", що стало причиною припинення розгляду справи за скаргою заявниці.

Конституційний Суд Російської Федерації не розглядав справу по суті, а визнав її неприйнятною, мотивуючи це тим, що права заявниці були порушені невірним застосуванням положень Федерального закону "Про оперативно-розшукову діяльність", а не його невідповідністю Конституції.

Разом з тим, чотири судді із 15, що становили склад суду, не погодились з прийнятою ухвалою і висловили окремі думки. Найбільш ґрунтовною, на нашу думку, є позиція судді А.Л. Кононова, який піддав справедливій критиці висновки Конституційного Суду Російської Федерації по цій справі, а також відповідні положення Федерального закону "Про оперативно-розшукову діяльність".

Зокрема, позиція судді А.Л. Кононова щодо невідповідності положень Федерального закону "Про оперативно-розшукову діяльність" Конституції Російської Федерації була обґрунтована посиланнями на принципи, які виробив Європейський Суд під час розгляду

[8] Див.: Додаток № ___

численних справ щодо правомірності застосування обмежень певних прав людини. Вказані принципи суддя Конституційного Суду Російської Федерації застосував до обставин конкретної справи, йдеться про підстави, а також межі для втручання в права людини під час оперативно-розшукової діяльності. Серед підстав правомірного застосування обмежень він зазначив такі:

- запроваджуватися на підставі закону:

“Подібні обмеження можуть встановлені тільки в федеральному законі (стаття 55, ч. 3 Конституції Російської Федерації). Це означає, що нормативні акти іншого рівня, включаючи відомчі, а тим більше не оприлюднені або закриті, не тільки не можуть встановлювати будь-яких обмежень прав і свобод людини, але і регулювати порядок і підстави їх застосування, умови, межі, строки та інші суттєві ознаки цих обмежень”

- мати легітимну (законну) ціль:

“... обмеження прав і свобод людини в оперативно-розшуковій діяльності можуть бути виправданими і допустимими, якщо вони встановлені в цілях захисту не від будь-якого правопорушення, а лише від найбільш небезпечних злочинних порушень закону, принаймні тих, які вимагають попереднього слідства

- бути необхідними в демократичному суспільстві:

“Оперативно-розшукові заходи можуть здійснюватися лише тоді, коли в інший спосіб досягнути поставленої мети неможливо”.

Рамки правомірного обмеження права на приватність інформації персонального характеру під час оперативно-розшукової діяльності повинні, на думку судді Конституційного Суду Російської федерації А.Л. Кононова, встановлюватися зважаючи на характер, суб’єктний склад, часовий період можливих обмежень і повинні гарантувати їх підконтрольність:

“Ці обмеження повинні враховувати необхідний баланс інтересів людини, суспільства і держави...
Будь-яке втручання тут повинно бути строго вибірковим, а не загально пошуковим...
Такі обмеження, включаючи і таємний характер можливих оперативно-розшукових заходів, не можуть зберігатися невизначено тривалий строк...
Таке втручання повинно бути достатньо обґрунтованим як за даних конкретних обставин, так і по відношенню до конкретного індивіду, за умови обмеження свободи розсуду посадової особи і за наявності реального позавідомчого, у тому числі судового, контролю за обґрунтованістю цих заходів”.

Щодо початку оперативно-розшукових заходів, зважаючи на ці визначальні принципи, суддя дійшов висновку, що положення частини другої ст. 10 Федерального закону, які у якості підстав заведення справи оперативного обліку називають “відомості, які стали відомі правоохоронним органам, про осіб, які готують, вчиняють або вчинили протиправні діяння, за відсутності достатніх підстав для вирішення питання про порушення кримінальної справи”, - не “вписуються” в рамки дозволених обмежень прав людини:

“Таке формулювання закону фактично надає оперативній службі необмежену свободу розсуду під час вирішення питання про початок оперативно-розшукового провадження. Вона не вимагає обґрунтування цього рішення з точки зору ступеня достовірності наявних відомостей, їх важливості, доведеності, реальності в конкретній ситуації і по відношенню до конкретної особи. Вона не зобов’язує враховувати і відображати можливість інших способів досягнення мети. Нарешті, це формулювання допускає заведення справи і у випадках адміністративних чи інших не небезпечних чи незлочинних порушень закону”.

Проаналізувавши визначення підстав закриття (припинення) справи оперативного обліку в положеннях частини четвертої статті 10 Федерального закону, які передбачають, що справа оперативного обліку припиняється у випадку "вирішення конкретних завдань оперативно-розшукової діяльності, а також "встановлення обставин, що свідчать про об'єктивну неможливість вирішення цих завдань", суддя також знайшов перевищення меж і неправомірність підстав втручання у права людини:

"Наведені формулювання не визначають ясно і точно, якими є конкретні підстави (факти), з якими закон пов'язує обов'язок оперативного органу припинити справу...
... норми цього Закону не передбачають обов'язок винесення при цьому процесуального рішення навіть у тих випадках, коли метою оперативно-розшукових заходів була перевірка повідомлень по відношенню до конкретних осіб, підозрюваних у підготовці або вчиненні злочинів.
Таким чином, особи, по відношенню до яких збиралась інформація про їх причетність до вчинення злочинів, але не знайшла свого підтвердження, або оперативний орган з тих чи інших міркувань не вважав доцільним передачу матеріалів для винесення процесуального рішення, - ці особи позбавляються можливості захисту своїх прав і інтересів, зостаючись у підозрі невизначено тривалий час".

Значну частину окремої думки судді Конституційного Суду Російської федерації А.Л. Кононова по цій справі присвячено питанню доступу громадян до інформації, яка була зібрана про них під час оперативно-розшукових заходів, оскільки таке право громадянина є суттєвою гарантією ефективної реалізації права на оскарження неправомірних дій, а отже, є гарантією законності негласного збору, зберігання і використання інформації персонального характеру.
Суддя, аналізуючи положення статті 5 Федерального закону "Про оперативно-розшукову діяльність", знайшов порушення визначальних принципів правомірного обмеження права людини на доступ до інформації про себе. Так частина друга статті 5 Федерального закону надає право доступу лише вузькому колу зацікавлених осіб, а саме: особам, винуватість яких у вчиненні злочину не доведена, тобто як пояснено у цьому законі, щодо яких у порушені кримінальної справи відмовлено, або кримінальна справа припинена за відсутністю події злочину або за відсутністю складу злочину. Під цю категорію, до речі, не попала заявниці по справі І.Г. Чернова, щодо якої оперативні заходи здійснювались, але жодних процесуальних рішень не приймалось.
Частина третя і четверта статті 5 Федерального закону також невиправдано обмежують право на доступ до інформації за її змістом, надаючи громадянину право витребувати "відомості про одержану про нього інформацію" і "в межах допустимих вимогами конспірації, які виключають можливість розголошення державної таємниці". До того ж, розпливчасті положення частини першої статті 12 цього закону, що визначають відомості віднесені до державної таємниці, і серед них "відомості про результати оперативно-розшукової діяльності", дозволяють працівникам оперативних органів відмовляти зацікавленим особам у наданні практично будь-якої інформації.
На думку судді, "вона не може бути засекречена від тієї особи, з якою ідентифікується. В противному випадку це буде повним відкиданням його права". А отже,

"... у органа оперативно-розшукової діяльності повинен виникати обов'язок повідомити зацікавленій особі про наявність щодо нього документованої чи іншої інформації і надати таку інформацію на її вимогу. У тих спірних питаннях, коли певна інформація, на думку органів, може містити відомості, що здатні спричинити розкриття осіб, які проникли в організовані злочинні групи, штатних негласних співробітників оперативних органів і осіб, які сприяють їх діяльності на конфіденційній основі, питання повинно вирішуватися у судовому порядку."

Суддя також проаналізував положення статті 9 Федерального закону, присвячені питанню контролю за здійсненням оперативно-розшукової діяльності з боку судової гілки влади. Зокрема, він вказав на такий недолік Закону, як відсутність регламентації процедури перевірки доказів і оцінки доводів оперативних органів для вирішення судом загальної юрисдикції питання про проведення оперативно-розшукових заходів, які обмежують конституційні права громадян.

Підсумовуючи вищезазначене, можна висунути такі вимоги до нормативно-правового регулювання обмежень прав громадян у зв'язку із обробкою персональних даних в правоохоронній діяльності: на усіх етапах від збирання до знищення інформації персонального характеру мають бути встановлені правові рамки для дій службовців через детальну регламентацію службових прав і обов'язків, мають бути запроваджені дієві гарантії додержання законності і відновлення обмежених прав громадян.

Здійснений вище аналіз загальних вимог до застосування легітимних обмежень права на повагу до приватного життя дозволяє перейти до розгляду специфічних питань обмеження права на приватність інформації персонального характеру в цілях правоохоронної діяльності.

1.3. Вимоги до обробки інформації персонального характеру у правоохоронній діяльності

Спеціальні міжнародно-правові документи у галузі захисту приватності інформації персонального характеру відносять "поліцейські файли" до категорії відомостей, обробка яких несе підвищений ризик правам суб'єктів даних. Зокрема, Стаття 6 Конвенції Ради Європи "Про захист осіб стосовно автоматизованої обробки персональних даних" 1981 року № 108, а також Стаття 8 Директиви 95/46 СЕ Європейського Парламенту і Ради "Про захист фізичних осіб стосовно автоматизованої обробки персональних даних та безперешкодного руху цих даних" 1995 року відносять ці дані до розряду вразливих.

Категорія "вразливості" даних показує націленість правового регулювання обробки на захист інтересів людини. Чим більше вразливість даних, тим більше ризик порушення прав осіб під час обробки персональних даних, а значить тим сильнішими повинні бути правові гарантії захисту від порушень. Оцінка вразливості даних, а отже і всіх обставин їх обробки, повинна передувати самій обробці. Цей принцип є визначальним для побудови всієї правової конструкції відносин з обробки персональних даних у правоохоронній діяльності, оскільки напряму пов'язаний з принципом пропорційності, - пропорційності обмеження прав громадян відповідно до рівня суспільної небезпечності злочину.

Стаття 9 Конвенції Ради Європи 1981 року зазначає, що національними положеннями можуть запроваджуватися виключення з загальних принципів приватності інформації персонального характеру, якщо це запроваджується на підставі закону і є необхідним у демократичному суспільстві для боротьби із злочинністю і захисту громадського порядку.

Ці вимоги деталізуються у Рекомендації № R (87)15 Комітету Міністрів Ради Європи державам-членам, що регулює використання персональних даних у секторі поліції. Схвалена у 1987 року на 410-й зустрічі заступників міністрів, вона не втратила своє актуальності на сьогоднішній день.

Сам текст Рекомендації містить всього вісім принципів, розгорнуте тлумачення яких додається у пояснювальній записці. Не випадково, що **першим принципом** є принцип контролю за обробкою персональних даних. Йдеться про запровадження механізму нагляду за додержанням поліцією встановлених законом вимог до обробки інформації персонального характеру. Такий нагляд повинен здійснюватися незалежним органом державної влади, діяльність якого не пов'язана з діяльністю поліції. На цей же наглядовий орган може бути покладено функцію реєстрації файлів (масивів) персональних даних, які оброблятимуться поліцією.

Процедура повідомлення покликана, по-перше, запровадити попередній контроль за законністю обробки тієї чи іншої категорії персональних даних, а по-друге, спростити процедуру і підвищити ефективність нагляду за допомогою одержаних при цьому

відомостей про орган і його посадових осіб, відповідальних за обробку і наступну передачу даних.

Враховуючи все більше впровадження новітніх інформаційних технологій у діяльність поліції, незалежний наглядовий орган повинен виконувати важливу роль попередньої перевірки нових засобів чи пристроїв, які використовуються для обробки персональних даних, а отже можуть нести великий ризик для прав людини. Зокрема, може йтися про технології негласного стеження чи збирання інформації за допомогою співставлення інформації з різних баз даних, що є потенційно небезпечним.

Принцип 2 Рекомендації присвячується питанням збирання інформації про особу правоохоронними органами і адаптує вимоги статті 5 Конвенції Ради Європи 1981 року до умов діяльності поліції. Зокрема, окреслюються межі збирання персональних даних. Вони можуть збиратися для запобігання реальній небезпеці або припинення особливого кримінального злочину. Для негласного збирання персональних даних, у тому числі з використанням технічних засобів, в національному законодавстві повинні бути запроваджені детальні правила і гарантії від зловживань.

Окрема увага приділяється збиранню, так званих, "вразливих даних", які розкривають расову або етнічну належність, релігійні переконання, політичні погляди або філософські переконання, сексуальну поведінку тощо. Їх збирання дозволяється лише у разі "виключної потреби для цілей особливого запиту", тобто коли існують серйозні підстави вважати, що злочин скоєний чи може бути скоєним особою, яка може бути ідентифікована за допомогою таких вразливих даних. При цьому, роз'яснюється, що відомості про сексуальну поведінку можуть збиратися лише для розслідування вже скоєних злочинів.

До процедури зберігання даних також пред'являються вимоги, які надають гарантії не порушення прав осіб під час їх подальшого використання. Ці ж вимоги сприятимуть ефективності правоохоронної діяльності. **Принцип 3** Рекомендації передбачає необхідність запровадження системи класифікації даних, розрізняючи підтверджені дані від непідтверджених, дані одержані з надійних джерел від ненадійних[9].

Крім того, рекомендується щоб за можливістю дані про скоєні злочини або про підготовку до вчинення злочинів зберігалися окремо від даних, зібраних для адміністративних цілей, у тому числі про адміністративні правопорушення. Тим самим, буде забезпечуватися, по перше, принцип додержання цілі збирання під час зберігання, по друге, унеможливиться помилкове їх використання внаслідок змішування.

Четвертий принцип закріплює вимогу використання даних зібраних в поліцейських цілях, тобто для запобігання чи припинення злочинів або підтримання громадського порядку, лише в цих цілях. Це не означає, що дані з поліцейських файлів не можуть передаватися іншим органам, оскільки вказану функцію певним чином виконують також

---

[9] Для прикладу, система класифікації поліцейських рапортів запроваджена у Великій Британії, так звана система "5x5x5", передбачає процедуру попередньої оцінки (до внесення відомостей до бази даних) відповідальним офіцером поліції джерела інформації, змісту і наслідків поширення даних, на підставі чого рапорту надається код в залежності від цих критеріїв.

Джерелам інформації присвоюється літери A, B, C, D або E у залежності від рівня довіри до них. Джерело, яке до цього завжди надавало достовірні відомості, позначається літером "A", а будь-яке нове неперевірене джерело – літером "E". Інформація класифікується за її достовірністю від 1 до 5. Ті відомості, що є достовірно відомі без жодних застережень позначаються категорією "1"; а ті, що вважаються недостовірними або повідомленими із злими намірами – категорією "5". Наслідки від поширення даних оцінюється на потенційний ризик і вигоди за цим класифікатором від 1 до 5. Категорія "1" дозволяє поширення іншим правоохоронним і судовим органам, а категорія "5" – відкидає таку можливість. Після закінчення оцінки, поліцейському рапорту присвоюється код, який складається з трьох символів. Наприклад, код поліцейського рапорту "E-5-1" означає, що джерело інформації нове і неперевірене, відомості не відповідають дійсності і рапорт не може бути переданий іншим правоохоронним і судовим органам.

Джерело: David Wolstenholme. Police Requirements and Practices in the Information Society 'The case in the United Kingdom' // ADACS/DGI (2000) 3 Sem.: Data protection in Police Sector. Council of Europe Regional Seminar under the activities for the development and consolidation of democratic stability. – Strasbourg. - Council of Europe. - 2000.

інші державні органи і установи. Ці випадки, які становлять не правило, а виняток з нього, конкретизуються у **Принципі 5**.

Однією з вимог для легітимної передачі даних поліцейською установою іншим органам і установам є наявність санкції; тобто передачі даних передує розгляд її доцільності і законності уповноваженим органом, наприклад, судом або незалежним наглядовим органом.

За відсутності такої санкції, передача дозволяється коли це необхідно для виконання державним органом покладених на нього за законом обов'язків, в інтересах особи, якої стосується інформація (суб'єкта даних), а також коли це необхідно для відвернення серйозної реальної небезпеки ("навислої загрози").

Міжнародна передача поліцейських даних дозволяється лише між органами поліції. Правовою підставою для таких передач є наявність дво або багатосторонніх домовленостей між державами. Це питання більш детально розглядається в наступному розділі нашої книги. Однак слід звернути увагу на дуже важливе питання, яке безпосередньо зачіпає Україну.

В цьому принципі закріплюється вимога, що міститься в статті 12 Конвенції Ради Європи № 108. Також вона включена до текстів європейських угод у галузі співробітництва між органами поліції. Йдеться про відповідність національного законодавства країни одержувача даних вимогам щодо захисту права на приватність персональних даних, викладеним у Рекомендаціях.

Забезпечення цієї вимоги покладається на поліцейську установу, яка передає дані до країни, в якій рівень правового захисту не є адекватним. При цьому, передбачається можливість застосування застережень з боку передаючої сторони щодо процедури обробки і використання персональних даних одержувачем для задоволення інформаційного запиту.

Важливою гарантією законності обробки персональних даних в поліцейський цілях, відновлення обмежених і захисту порушених прав громадян під час правоохоронної діяльності є, по-перше, право на ознайомлення з поліцейськими файлами зацікавлених осіб, по-друге, право на виправлення неточних даних, по-третє, право на оскарження неправомірних дій. Ці питання регламентується в **шостому принципі**.

Не вимагає додаткових пояснень твердження, що збирання, систематизація і аналіз відомостей про осіб, які готують або вчинили злочини, так само як й про осіб, життя, здоров'я або майно яких стали об'єктом посягань, є ключовими елементами правоохоронної діяльності. В той же час, в цілях правоохоронної діяльності – не повідомляти осіб про негласне збирання інформації персонального характеру, тримати одержані відомості про особу недоступними для громадськості, оскільки розголошення може зашкодити слідству, унеможливити досягнення результату оперативно-розшукових заходів і слідчих дій взагалі.

Таємний характер обробки інформації про особу в цілях боротьби із злочинністю входить у протиріччя з принципом прозорості, який є суттєвим для ефективної реалізації права людини на приватність інформації персонального характеру. Назнаючи про збирання персональних даних, зацікавлена особа не може захистити свої права.

Отже, потребується вироблення правового механізму, який дозволить врахувати інтереси особи, чиї права обмежуються. Зокрема, у принципі 6 йдеться про контроль з боку громадськості (суспільства) через орган нагляду за обробкою персональних даних, яка здійснюється правоохоронними органами. Тобто не повинно існувати таємних файлів або баз даних, які невідомі громадськості. Усі вони повинні бути легалізованими і їх використання врегульовано у законодавстві, доступному для громадськості.

Право на доступ до персональних даних, що містяться у поліцейських файлах, повинно гарантуватися. Однак межі здійснення цього права залежатимуть від наслідків, які буде мати розголошення відповідної інформації. Якщо розголошення тієї чи іншої інформації, одержаної як гласними, так і не гласними засобам може зашкодити слідству – вона не повинна повідомлятися. В інших випадках, як в інтересах громадян, так і в інтересах правоохоронних органів надати зацікавленій особі доступ до відомостей з правом їх

виправлення або додавання додаткових достовірних даних. При цьому, персональні дані, які були зібрані з порушенням закону, повинні бути знищені на вимогу суб'єкта даних.
Національне законодавство повинно передбачати процедуру контролю за додержанням законності у випадку відмови у доступі до поліцейських файлів. Цю функцію може виконувати незалежний орган держави, будь-то наглядова інстанція чи суд.
Принцип 7 Рекомендацій передбачає, що персональні дані, які збиралися з певною метою, після досягнення цієї мети або неможливості чи недоцільності її досягнення, повинні знищуватись. Такими підставами можуть бути відмова у порушені кримінальної справи, засудження особи, реабілітація, амністія чи інші аналогічні випадки. Національне законодавство повинно визначати терміни зберігання тих чи інших даних у залежності від мети їх збирання чи характеру самих даних.
Кінцевий **восьмий принцип** покликаний забезпечити цілісність даних шляхом адекватних технічних й організаційних заходів для унеможливлення, запобігання чи припинення несанкціонованого доступу, передачі, перетворення або знищення персональних даних і від будь-якої іншої незаконної обробки як внаслідок необережності, так і навмисних дій третіх осіб.
Рекомендовані принципи тією чи іншою мірою впроваджені в тексти міжнародних і, зокрема, європейських документів, що регулюють співробітництво поліцейських установ. Більше того, прямі посилання на Рекомендацію № R (87)15 міститься у статті 115 Шенгенської Конвенції, яка інкорпорована в європейське право Амстердамським Договором, а також в статті 14 Конвенції Європол.
Як вже зазначалось, однією з основних вимог для можливого включення третіх держав в ці європейські домовленості як партнерів і учасників є відповідність національного законодавства, що регулює обробку персональних даних в цілях запобігання і боротьби із злочинністю, вищевказаним принципам.
З огляду на це, одним з першочергових кроків на шляху розвитку співробітництва України з Європейським Союзом у галузі правоохоронної діяльності має бути приведення національного законодавства і практики використання персональних даних у відповідність до європейських норм і стандартів.

Розділ 2. Співробітництво країн Європейського Союзу у галузі правоохоронної діяльності і використання персональних даних

2.1 Створення простору свободи, безпеки і правосуддя в Європі і обробка персональних даних

Важко визначити конкретну дату, з якої слід відраховувати початок співробітництва європейських країн з питань забезпечення свободи, безпеки і правосуддя в Європі. Однак інституційну форму цей процес почав набувати із створенням Європейського Співтовариства після підписання Договору 1957 року, однією з цілей якого було вільне пересування робітників по Співтовариству. Питання перетинання кордонів, імміграції чи візової політики ним не зачіпалися, оскільки першорядними були економічні пріоритети.
Серед іншого, "завдячуючи" зростанню рівня злочинності, її транс – націоналізації, європейські країни почали більш активно опікуватися питаннями співробітництва у галузі правосуддя і внутрішніх справ. А реалізація ідеї свободи пересування незважаючи на кордони для усіх, як громадян, так і не громадян вимагала адекватного удосконалення співробітництва поліцейських установ у галузі контролю за перетинанням кордонів.
Амстердамський Договір змінив підхід до співробітництва європейських країн у галузі правосуддя і внутрішніх справ, визначивши простір свободи, безпеки і правосуддя більш програмно і чітко. Зокрема, встановивши мету забезпечити вільне пересування по Європейському Союзу як громадян, так і негромадян, було наголошено на необхідності

гарантування безпеки через боротьбу із усіма формами організованої злочинності і тероризмом.

Питання захисту приватності персональних даних певним чином торкається цих трьох складових взаємопов'язаних "елементів" простору. А в планах Європейського Союзу, об'єднати ці складові в "третій колоні" Європейського права з поширенням на неї вимог захисту приватності персональних даних[10]. Про це свідчить, зокрема, Рішення Ради Європейського Союзу від 17 жовтня 2000 року, яким запроваджується об'єднаний секретаріат спільних органів нагляду за додержанням законності під час обробки персональних даних, створених Конвенцією Європол, Конвенцією про використання інформаційних технологій для митних цілей та Шенгенською Конвенцією[11]. Так званий "секретаріат з захисту даних" буде виконувати ті функції, які розрізнено виконували відповідні секретаріати спільних наглядових органів цих Конвенцій Європейського Союзу. Крім того, нова Стаття 286 Договору про Європейські Співтовариства застосовує нормативні акти ЄС у галузі захисту приватності персональних даних до інституцій і органів Європейського Союзу.

На розвиток такого напрямку співробітництва країн ЄС як створення простору свободи, безпеки і співробітництва Європейський Парламент и Рада ухвалили Хартію основних прав громадян Європейського Союзу. Захисту права на повагу до приватного життя і захисту персональних даних, як фундаментальним правам людини відводиться дві статті цієї Хартії. Стаття 7 за назвою "Повага до приватного і сімейного життя", яка є другою по порядку у Розділі 2 Хартії "Свободи", майже тотожна за змістом частині першій статті 8 Європейської Конвенції про захист прав людини і основних свобод. А наступна стаття 8 Хартії містить квінтесенцію принципів захисту приватності персональних даних. Зокрема, в ній проголошується[12]:

Стаття 8

Захист персональних даних

1. Кожний (а) має право на захист персональних даних, що стосуються його чи її.
2. Такі дані повинні оброблятися правомірно для визначених цілей і базуватися на згоді зацікавленої особи чи інших легітимних підставах, передбачених законом. Кожний (а) має право на доступ до зібраних даних, що стосуються його чи її, і право на їх виправлення.
3. Додержання цих правил повинно контролюватися незалежним органом влади.

Тим самим, у галузі створення свободи, безпеки і правосуддя в Європі підкріплюються існуючі в праві Європейського Союзу ("перша колона") гарантії, запроваджені Директивою № 95/46 СЕ Європейського Парламенту і Ради "Про захист фізичних осіб стосовно автоматизованої обробки персональних даних та безперешкодного руху цих даних" (м. Люксембург, 24 жовтня 1995 року).

Повага до прав людини є важливою елементом концепції створення простору свободи в Європі. Стаття 6 (1) Договору про створення Європейського Союзу передбачає, що "Союз ґрунтується на принципах свободи, демократії, поваги до прав людини і фундаментальних свобод, верховенстві (правлінні) права".

Захист прав громадян у зв'язку з обробкою інформації персонального характеру в діяльності органів правосуддя також знаходиться в порядку денному інституцій Європейського Союзу. Зокрема, нещодавно прийнята Конвенція про взаємну допомогу у

---

[10] Директива № 95/46 СЕ Європейського Парламенту і Ради "Про захист фізичних осіб стосовно автоматизованої обробки персональних даних та безперешкодного руху цих даних" не поширюється на "третю колону" права ЄС.

[11] Council Decision of 17 October 2000 establishing a secretariat for the joint supervisory data protection bodies set up by the Convention on the Establishment of a European Police Office (Europol Convention), the Convention on the Use of Information Technology for Customs Purposes and the Convention implementing the Schengen Agreement on the gradual abolition of checks at the common borders (Schengen Convention) // Official Journal of the European Communities. – 2000. - L 271. – P. 0001-0003.

[12] Chapter of Fundamental Rights of the European Union // Official Journal of the European Communities. – 2000. – C 364 - P. 10.

кримінальних справах країн-членів Європейського Союзу передбачає обмін інформацією персонального характеру в рамках такого співробітництва[13]. Для цього створюється інформаційна мережа, управління якою здійснюватиме спеціальний підрозділу з питань судового співробітництва Євроджаст (Eurojust)[14]. У грудні 2000 року тимчасовий склад Євроджаст був призначений із судів, прокурорів і магістратів з країн-членів ЄС, які координують правові питання проведення транскордонних розслідувань, включаючи тероризм, комп'ютерну злочинність, відмивання грошей і екологічні правопорушення[15].

Між тим питання впровадження принципів захисту приватності персональних даних в механізм здійснення правосуддя є недостатньо розробленим на сьогоднішній день в теорії, і практично не застосовуються на практиці. Про це свідчать результати дослідження проведеного Європейською Комісією в рамках реалізації проекту "Фальконе"[16]. Можливим шляхом розвитку цього питання є розробка спеціальних правил захисту приватності персональних даних, які були б адаптовані до вимог кримінального і цивільного процесуального права, враховували б особливий статус учасників процесу, а також незалежний статус суддів[17]:

"... вже більше не достатньо встановлювати процесуальні правила – які також стосуються реалізації права на захист – щодо діяльності державних і приватних установ відповідальних за поліцейську і судову діяльність. Існує зростаюча потреба конкретизації для громадян як персональна інформація збирається, обробляється і передається, хто має право доступу до такої інформації і з якою метою, які заходи з технічного захисту наявні для запобігання їх неправомірного використання чи розповсюдження та інше."

Відсутність гарантій поваги до приватного життя під час здійснення судочинства або їх недодержання нерідко призводить до порушення прав учасників судових процесів, а також інших причетних до цього осіб. Один з таких випадків був предметом розгляду Європейського Суду з прав людини.

У рішенні по справі "Z проти Фінляндії", датованому 25 лютого 1997 року, Європейський Суд з прав людини встановив порушення гарантованого статтею 8 Європейської Конвенції про захист прав людини і основних свобод права на повагу до приватного життя через обмеження строку зберігання вироку суду, яке містить медичні дані про зараження заявниці ВІЛ-інфекцією, 10-ма роками, а також розкриття особи заявниці та факту зараження у тексті вироку апеляційного суду, що став доступним для преси. Європейський Суд наголосив на необхідності ретельної оцінки судами можливих наслідків втручання у приватне життя і встановлення справедливого балансу між інтересами окремої людини і всього суспільства[18]:

"97. ... Суд визнає, що інтереси пацієнта і суспільства в цілому у захисті конфіденційності медичних даних можуть переважати інтереси дослідження і розкриття злочину та гласності судових процесів...

99. В питаннях стосовно доступу громадськості до персональних даних Суд визнає, що вони повинні розглядатися компетентними національними органами влади з суворим дотриманням справедливого збалансування інтересів гласності судових справ, з одного боку, та інтересів якоїсь сторони чи третьої особи у збереженні конфіденційності таких даних, з другого боку. Означення лінії розрізнення залежить від таких факторів, як характер і серйозність цих інтересів та міра втручання..."

---

[13] Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty of European Union the Convention on Mutual Assistance in Criminal Matters between the member States of the European Union // Official Journal of the European Communities. – 2000. – C 197.

[14] Council Decision of 14 December 2000 setting up a Provisional Judicial Cooperation Unit // Official Journal of the European Communities. – 2000. – L 324.

[15] EU agrees principles for Eurojust // EUobserver.com. – 2001. – September 28.

[16] Fight Against Organized Crime and Control of Personal Data // European Commission Falcone Programme Project. - Rome: 2000. - P. 223-241.

[17] Ibid. 7. - P. 256.

[18] Z vs. Finland. - Judgment of 25 February 1997 // Reports of Judgments and Decisions. – 1997. – I. – P. 347-348.

Вироблені і застосовані в практиці Європейського Суду з прав людини критерії для узгодження інтересів окремої людини і суспільства служать орієнтиром для розробки законодавства Європейського Союзу про захист приватності персональних даних у галузі правосуддя. Такий позитивний приклад варто запозичити і вітчизняним законодавцям.
Повертаючись безпосередньо до питання захисту приватності персональних даних у зв'язку з їх обробкою поліцейськими установами, слід зауважити, що це питання стало надзвичайно актуальним для Європейського Союзу після того як були ліквідовані митні кордони між країнами членами Шенгенської Конвенції

2.2 Захист приватності персональних даних в контексті регулювання співробітництва Європейський поліцейських установ

Шенгенська Конвенція

Повертаючись безпосередньо до питання захисту приватності персональних даних у зв'язку з їх обробкою поліцейськими установами, слід зауважити, що це питання стало надзвичайно актуальним для Європейського Союзу після того як були ліквідовані митні кордони між країнами членами Шенгенської Конвенції
Дозволимо собі зробити короткий екскурс в історію створення і розвитку цієї структури. Перша домовленість "Про поступове скасування перевірок на спільних кордонах" об'єднала групу з п'яти Європейських країн (Францію, Німеччину, Бельгію, Люксембург і Нідерланди). Підписана 14 червня 1985 року, вона заклала фундамент для подальшого співробітництва європейських країн у галузі створення територію без внутрішніх кордонів. Ця домовленість одержала назву Шенгенська Угода від назви міста у Великому Герцогстві Люксембург, де відбулося її підписання.
Процес ліквідації внутрішніх кордонів і створення спільних правил паспортного контролю був продовжений підписанням у тому ж місті Конвенції 19 червня 1990 року "Про застосування Шенгенської Угоди від 14 червня 1985 року про поступове скасування перевірок на спільних кордонах", яка вступила в силу лише у 1995 році.
Шенгенський простір поширив на майже усі країни члени Європейського Союзу і вже у 1997 році включала 13 країн ЄС, за виключенням Великої Британії та Ірландської Республіки. А з 25 березня 2001 року Шенгенський простір поширюється й на дві країни Північного (Скандинавського) Паспортного Союзу, які не є членами ЄС, - Ісландію і Норвегію. Цей факт однак не заважає Європейським інституціям вживати заходів для поступового включення Шенгенської структури до складу "третьої колони", на якій "тримається" Європейський Союз, а саме регулювання співробітництва між національними правоохоронними і судовими органами країн ЄС.
Запроваджений Амстердамським Договором простір свободи, безпеки і правосуддя дозволив включити Шенгенську Угоду до структури Європейського Союзу. Цим же Договором, що набув чинності 1 травня 1999 року, повноваження Виконавчого Комітету Шенгенської Конвенції були передані Раді Європейського Союзу.
З метою сприяння діяльності правоохоронних органів особливо з огляду на труднощі, які виникають в їх діяльності через надання громадянам європейських і неєвропейських країн свободи вільного пересування в Шенгенському просторі, була створена комплексна інформаційна система (SIS) для обміну відомостями про осіб, а також про вкрадені або загублені предмети. Інформаційна система складається з мережі, до якої підключені національні підрозділи, інформаційного центру, а також операційної системи задоволення запитів національних підрозділів за назвою "SIRENE" (Supplément d'Information Requis a l'Entrée Nationale).
Ця операційна система з вересня 2001 року замінена на нову систему "SISNET", в якій додатково оброблятимуться відомості про імміграцію. Функції технічної підтримки цієї системи забезпечує Французька Республіка; служби технічного забезпечення розташовуються в Страсбурзі.

Ліквідація контролю під час перетинання внутрішніх кордонів всередині Шенгенської зони компенсується спільним контролем за перетинанням її зовнішніх кордонів, який здійснюється національними підрозділами за загальним порядком визначеним Шенгенської Конвенцією. Під час такого контролю перевіряються як громадяни країн Шенгенського простору, так і громадяни інших країн. Це включає в себе перевірку документів ідентифікуючих особу, а для громадян інших країн додатково – наявність офіційного дозволу на в'їзд та відсутність підстав для затримання цієї особи у будь-якій Шенгенській країні. Інформація необхідна для проведення контролю надається вищевказаною інформаційною системою (SIS), в якій містяться відомості про усі ордери на затримання, видані в Шенгенських країнах, а також відмови на в'їзд негромадянам. Інформація в системі тримається у стані постійного оновлення в режимі реального часу.
У разі відсутності дозволу на в'їзд, негромадянин позбавляється доступу на територію Шенгенського простору. При наявності підстав для затримання, передбачених Шенгенською Конвенцією, особа підлягає затриманню на кордоні. Такими підставами можуть бути:

- судовий ордер на арешт або на екстрадицію цієї особи під юрисдикцію іншої Шенгенської країни (стаття 95);
- відомості про зникнення особи або про необхідність надання їй спеціального захисту (стаття 97);
- відомості про необхідність дачі цією особою свідчень у суді або відбуття покарання у вигляді позбавлення волі (стаття 98).

Шенгенська інформаційна система містить такі вхідні дані, що стосуються осіб (стаття 94):

- прізвище, ім'я, а також інші імена (псевдоніми, прізвиська), якими користується особа і які можуть бути зареєстровані;
- особливості зовнішнього вигляду, його сталі характеристики;
- першу літеру імені по батькові;
- дату і місце народження;
- стать;
- національність;
- наявність зброї;
- агресивність (готовність до вчинення насильства);
- підстави для внесення відомостей до системи;
- заходи, які повинні бути вжиті до особи у випадку її ідентифікації під час контролю.

До інформаційної системи заносяться відомості про іноземців, щодо яких зроблено інформаційних запит з метою не допуску. Шенгенські країни вирішують питання щодо запиту на підставі своїх національних положень з додержанням відповідних процесуальних норм. Стаття 96 Конвенції доволі розпливчасто визначає підстави для прийняття таких рішень, залишаючи країнам майже необмежену свободу розсуду. Зокрема, це такі:

- загроза громадському порядку чи національній безпеці та спокою, що може спричинитися через перебування іноземця на території країни;
- іноземець є об'єктом депортації, примусового повернення чи вислання, дія яких не відмінена і не зупинена, внаслідок недодержання національних правил про в'їзд і перебування іноземців.

Введена інформація використовується для здійснення негласного стеження чи спеціального контролю, коли на це є наступні підстави:

- наявна об'єктивна інформація про підготовку до вчинення або вчинення злочину цією особою;
- загальна оцінка цієї особи здійснена на підставі її попередніх злочинів свідчить про вірогідність повторення особливо небезпечних злочинів;

- одержання відомостей необхідно для відвернення серйозної загрози внутрішній і зовнішній безпеці держави.

В рамках негласного стеження для органу, що надіслав інформаційний запит, може збиратися і передаватися інформація, зібрана національними правоохоронними органами під час вжиття профілактичних і запобіжних заходів всередині країни. Негласно одержана інформація може включати наступні відомості як персонального, так і не персонального характеру про:

- факт виявлення особи або транспортного засобу щодо яких направлено інформаційний запит;
- місце, час і підстави вжитих заходів;
- маршрут та місце призначення поїздки;
- супроводжуючих осіб або пасажирів транспортного засобу;
- транспортний засіб, що використовується;
- предмети, що перевозяться;
- обставини, за яких було виявлено особу чи транспортний засіб.

За процедурою спеціального контролю, особи, транспортні засоби та предмети, що перевозяться, можуть бути піддані обшуку у відповідності з національними процесуальними нормами для одержання вищевказаної інформації.

Питанням контролю за безпекою персональних даних і додержанню прав осіб, щодо яких здійснюється їх обробка в Шенгенській інформаційній системі, присвячується третя глава в Розділі IV Конвенції (статті 102-118), а також окремий Розділ VI за назвою "Захист персональних даних" (статті 126-130).

Принципи правомірності обробки персональних даних проголошені вказаною Конвенцією Ради Європи, а також конкретизовані у Рекомендаціях № R (87)15 Комітету Міністрів Ради Європи інкорпоровані до Шенгенської Конвенції.

Стаття 126 Шенгенської Конвенції вимагає від кожної з країн-членів прийняття національних положень з захисту персональних даних, які повинні гарантувати рівень правового захисту не нижчий за стандарти впроваджені Конвенцією Ради Європи "Про захист осіб стосовно автоматизованої обробки персональних даних" 1981 року № 108. Ця ж стаття забороняє будь-яку передачу персональних даних до країн, рівень захисту в яких не відповідає вимогам Конвенції Ради Європи №108.

Крім того, на сторону, яка одержує дані, покладається зобов'язання використовувати їх лише у цілях, передбачених Конвенцією. При цьому такі дані можуть використовуватися лише судовими органами. Перед передачею даних повинна бути здійснена перевірка їх точності. Неточні дані підлягають уточненню або знищенню, про що повідомляються усі їх одержувачі.

Особи, яких стосується інформація введена до інформаційної системи, можуть здійснювати своє право на доступ до таких відомостей у кожній Шенгенській країні відповідно до положень національного законодавства за місцем звернення. У разі оскарження внесення інформації персонального характеру до вказаної системи або звернення щодо внесення уточнення чи знищення персональних даних, рішення приймається національним наглядовим органом після одержання пояснення від компетентного органу держави відповідальної за внесення даних. Таке рішення має обов'язковий характер на території усіх Шенгенських країн.

Якщо повідомленням недостовірних або частково неточних даних було порушено права суб'єктів даних, завдано збитки тощо, компенсація заподіяної зацікавленим особам шкоди у повному обсязі здійснюється згідно з національними положеннями країн-членів. Кінцеву відповідальність у порядку регресу несе сторона, яка повідомила недостовірні дані, що призвело до заподіяння шкоди особам.

З метою здійснення внутрішнього контролю, будь-яке направлення або одержання персональних даних підлягає реєстрації в базі даних (національній складовій інформаційної системи). Такі ж самі правила поширюються на неавтоматизовану (ручну) обробку і передачу персональних даних.

Гарантувати додержання правил поводження з персональними даними і відповідно додержання прав суб'єктів даних повинні національні органи, які уповноважені здійснювати незалежний нагляд. У разі відсутності такої гарантії, передача даних до такої країни забороняється.
Персональні дані внесені до Шенгенської інформаційної системи використовуються не лише в цілях контролю під час перетинання кордонів Шенгенського простору, але й у правоохоронній діяльності поліцейських установ і судових органів Європейських країн.

Конвенція Європол

Співпраця поліцейських установ Європейського Союзу набула певних інституційних форм із створенням Європейської Поліцейської Установи, скорочена назва якої Європол. Перше офіційне згадування Європолу міститься в Маастрихтському Договорі 1992 року, в статті К.1.9 якої країни-члени ЄС зобов'язуються "вважати наступні сфери об'єктом спільного інтересу: співпрацю поліції з метою запобігання і приборкання тероризму, незаконного обігу наркотиків та інших серйозних форм міжнародної злочинності, включаючи за необхідністю аспекти співпраці митних установ, з огляду на організацію всесоюзної системи обміну інформацією через Європейську Поліцейську Установу (Європол)".
Після підписання Конвенції Європолу у липні 1995 року знадобилось ще три роки для того, щоб парламенти усіх країн-членів ЄС її ратифікували. Вступивши в силу 1 жовтня 1998 року, Конвенція дозволила Європолу розпочати свою діяльність з 1 липня 1999 року.
Сферами, на які поширюється компетенція Європолу (стаття 2 Конвенції), і які постійно розширюються, є запобігання і приборкання:

- тероризму,
- незаконного обігу наркотиків,
- торгівлі людьми (включаючи виробництво і поширення дитячої порнографії),
- злочинів, пов'язаних з нелегальною імміграцією,
- протизаконного обігу радіоактивних і ядерних речовин,
- протизаконної торгівлі викраденими автомобілями,
- підробки грошей і засобі платежу, зокрема, у євро,
- відмивання грошей, здобутих злочинним шляхом, які пов'язані з міжнародною злочинністю.

Європол має наступні основні завдання:

- покращити обмін інформацією між поліцейськими установами країн-членів Європейського Союзу;
- одержувати, сортирувати і аналізувати інформацію і відомості;
- повідомляти компетентним установам країн-членів ЄС без затримки про інформацію, що їх стосується, а також про будь-які зв'язки встановлені між кримінальними вчинками;
- надання допомоги у розслідуваннях, які здійснюються національними поліцейськими підрозділами;
- підтримання комп'ютеризованої системи зібраної інформації.

Однією з унікальних характеристик Європолу є те, що в рамках цієї установи постійно підтримується зв'язок з національними підрозділами через офіцерів зв'язку, призначеними країнами-членами для роботи у складі центрального апарату Європолу. Крім того, досягається певна централізація правоохоронної діяльності на Європейському рівні, завдяки організації підрозділів-представництв Європолу, які слугують проміжними ланками для обміну інформацією з національними поліцейськими органами.
Для виконання своїх завдань Європол утримує інформаційну систему, в якій збираються, сортируються і аналізуються відомості, що можуть бути використані для розслідування злочинів. Основна перевага існування спільної інформаційної системи полягає у тому, що

одержані від національних підрозділів розрізнені дані після їх опрацювання в системі дозволяють на ранніх стадіях розслідування виявити зв'язки, які не могли бути встановлені під час їх первинного аналізу національними підрозділами.

Інформаційна система Європолу містить наступні види персональних даних (стаття 9):

- прізвище, дівоче прізвище, а також інші імена (псевдоніми, прізвиська);
- дату і місце народження;
- національність;
- стать;
- особливості зовнішнього вигляду, його сталі характеристики.

Крім того, інформаційна система Європолу використовується для обробки додаткової інформації щодо:

- обставин вчинення чи підготовки до вчинення злочинів;
- засобів вчинення злочинів;
- підрозділів, що здійснювали розслідування, а також матеріалів розслідування;
- підозрюване членство в злочинній групі;
- пред'явленні звинувачення.

Введені дані повинні стосуватися лише осіб, які готуються вчинити злочин, підозрюються у вчиненні або причетності до злочину, на який поширюється компетенція Європолу, а також звинувачених у такому злочині (стаття 8).

Персональні дані, які збираються і накопичуються в інформаційній системі, передаються до неї національними підрозділами держав-членів Конвенції, третіми державами чи міжнародними організаціями і органами як за власною ініціативою, так і на запит Європолу.

Розділ IV Конвенції Європол містить положення, які регулюють обробку персональних даних, у тому числі принципи захисту приватності. Стаття 14 покладає на держави-члени зобов'язання узгодити національне законодавство з стандартами захисту приватності персональних даних у галузі правоохоронної діяльності, зокрема, тими, що запроваджуються в Конвенції Ради Європи № 108, а також Рекомендації № R (87)15 Комітету Міністрів Ради Європи. Невиконання цієї умови матиме наслідком заборону на передачу персональних даних.

Відповідальність за додержання правил поводження з персональними даними покладається на державу-члена Конвенції, яка уводить або передає дані; а також на Європол, якщо дані одержані від третіх сторін заносяться до інформаційної системи безпосередньо офіцерами Європолу чи одержані в результаті проведеного офіцерами Європолу аналізу. Оскільки передбачається розмежування відповідальності між суб'єктами-обробки, інформаційна система повинна забезпечувати можливість їх розпізнавання.

Стаття 16 Конвенції Європол передбачає механізм внутрішнього контролю за додержанням законності під час обробки персональних даних в інформаційній системі Європол. Один з десяти випадків використання персональних даних, а також кожне їх виправлення підлягають перевірці на предмет їх відповідності вимогам Конвенції, про що складається звіт.

Загальним правилом поводження з даними, одержаними з інформаційної системи Європол, є обмеження їх використання уповноваженими органами держав-членів Конвенції випадками, що підпадають під компетенцію Європол. Однак вони також можуть бути ними використані для боротьби з іншими серйозними видами злочинів, що виходять за межі компетенції Європолу. При цьому будь-яка повідомляючи держава-член Конвенції або третя сторона (держава чи міжнародний орган) вправі обумовити застереження щодо подальшого використання персональних даних. У цих випадках користувач даних (Європол чи держава-член Конвенції) повинен узгодити з передаючою стороною умови використання даних у кожному конкретному випадку.

Стаття 18 Конвенції Європол закладає основи для співробітництва Європолу з третіми державами та організаціями, передбачаючи правила передачі персональних даних, що містяться в інформаційній системі Європолу, сторонам, які не є членами Конвенції. Це

питання є важливим для нашої держави, з огляду на прагнення співробітничати з Європейським Союзом у галузі правоохоронної діяльності.
Передача персональних даних третім державам та організаціям дозволяється, коли це необхідно в окремих випадках в цілях запобігання чи боротьби із злочинами, які входять до компетенції Європолу. При цьому третя держава чи організація повинні забезпечувати адекватний рівень захисту (приватності) персональних даних.
Це положення запозичене зі статті 25 Директиви № 95/46 СЕ Європейського Парламенту і Ради "Про захист фізичних осіб стосовно автоматизованої обробки персональних даних та безперешкодного руху цих даних" (м. Люксембург, 24 жовтня 1995 року). Для оцінки адекватності рівня захисту до уваги братимуться такі умови як характер даних, ціль запропонованої обробки, її тривалість, а також які положення законодавства застосовуються до передачі персональних даних. Необхідною умовою для передачі даних на вказаних вище підставах є наявність у третій державі чи організації механізму нагляду за додержанням законності використання персональних даних, який здійснюється відповідальним за це органом.
Питання передачі персональних даних до третіх держав чи організацій деталізуються у Акті Ради Європейського Союзу від 12 березня 1999 року. Загальною підставою для передачі персональних даних є відповідна угода між Європолом та третьою державою чи організацією. Рішення про укладення угоди з третьою державою чи організацією приймається одноголосно Радою Європейського Союзу на підставі оцінки можливості додержання правил обробки персональних даних третьою державою чи організацією.
В угоді між Європолом і третьою державою чи організацією зазначаються одержувачі даних (відповідальний орган держави чи організації), характер даних, цілі передачі і використання. Кожний запит на передачу даних також повинен містити вказівку на вказані умови одержання і використання даних.
Передачі даних третій державі або організації передує одержання згоди тієї держави-члена Конвенції Європол, яка занесла дані до інформаційної системи. Про передачу персональних даних, які уведені до інформаційної системи безпосередньо Європолом, рішення приймає Європол. Від одержувача даних (третьої держави чи організації) вимагається запевнення, що заявлена ціль використання персональних даних буде дотримуватися.
За відсутності угоди між Європолом і третьою державою чи організацією, як виняток, дозволяється передача санкціонована директором Європолу, якщо це необхідно для захисту важливих інтересів держав-членів Конвенції або для відвернення навислої небезпеки, пов'язаної зі злочином. Про таку передачу негайно повідомляються правління та спільний наглядовий орган Європолу.
Виключно під санкцію директора Європолу можуть передаватися, так звані, "вразливі дані", які розкривають расове походження, політичні погляди, релігійні чи інші переконання, дані про здоров'я, сексуальне життя. Цим, зокрема, забезпечується вимога статті 6 Конвенції Ради Європи № 108 "Про захист осіб стосовно автоматизованої обробки персональних даних" (м. Страсбург, 28 січня 1981 року) щодо надання додаткових гарантій стосовно обробки персональних даних, що можуть з огляду на їх характер несуть підвищений ризик для безпеки прав і свобод особи.
Як вже зазначалося вище, право зацікавлених осіб на доступ до своїх персональних даних є важливою гарантією законності, оскільки при цьому особа здатна оскаржити можливі неправомірні дії з персональними даними. Стаття 19 Конвенції Європол регламентує порядок доступу осіб до персональних даних, що знаходяться в інформаційній системі Європолу. Звернення громадян повинні адресуватися національним компетентним органам відповідно до вимог національного права. У доступі до даних може бути відмовлено, якщо це необхідно для забезпечення належного виконання Європолом своїх функцій, для захисту безпеки та громадського порядку чи запобігання злочину, а також для захисту прав і свобод інших осіб.
Враховуючи міжнародний характер діяльності Європолу і наявність різних джерел інформації, що потрапляє до інформаційної системи, в цій статті передбачається процедура узгодження позицій різних суб'єктів щодо вирішення питання про надання

доступу. Зокрема, враховується думка держав-членів Конвенції, третіх держав і організацій, які надали персональні дані чи зацікавлені у надані чи ненадані їх для ознайомлення. При цьому, достатньо лише одного заперечення будь-якої з зацікавлених сторін, щоб персональні дані не були повідомлені.

Зацікавлена особа, яка не буде задоволена відповіддю на прохання про доступ чи перевірку даних вправі звернутися з апеляцією до спільного наглядового органу. Своє рішення цей орган приймає після одержання висновку національного наглядового органу, який повинен здійснити перевірку додержання національного законодавства під час розгляду звернення національним підрозділом поліції. Якщо дані уведені до інформаційної системи безпосередньо офіцерами Європолу, необхідні перевірки здійснюються також Європолом.

У випадку, коли персональні дані є неточними або уведені до інформаційної системи чи обробляються з порушенням вимог правил обробки, передбачених Конвенцією Європол чи національним правом, вони виправляються чи знищуються. Про це повідомляються усі одержувачі даних, а також держави чи організації, які їх утримують; а також суб'єкт даних, який звернувся з проханням про виправлення своїх персональних даних. Стаття 22 Конвенції Європол містить важливу гарантію запобігання приховування порушення прав суб'єктів даних під час процедури знищення персональних даних, а також запобігання зашкодженою реалізації ним своїх законних інтересів. Якщо існують підстави вважати, що законні інтереси суб'єкта даних можуть бути незбереженнями у разі знищення неточних даних, файли не знищуються, а спеціально позначаються, щоб їх не могли використати. Це ж саме правило застосовується також у випадках можливого знищення даних за перебігом терміну зберігання.

Стаття 21 Конвенції Європол регламентує строк зберігання і знищення персональних даних. За загальним правилом, дані зберігаються стільки, скільки це потрібно для виконання Європолом своїх завдань. Перший строк обмежується трьома роками, після чого дані переглядаються на предмет можливості їх тривалішого зберігання. Держави-члени повідомляються за три місяці про наближення терміну перегляду даних. Дані, щодо яких рішення про продовження строку зберігання не прийнято, автоматично знищуються. Держава-член повідомляє Європол про знищення даних, які були раніше уведені нею до інформаційної системи. У разі необхідності Європол може не знищувати такі дані, якщо він має інтерес у їх подальшому зберіганні. Про таке рішення повідомляється зацікавлена держава-член.

Національні наглядові органи контролюють усі операції, що здійснюються національними поліцейськими підрозділами з персональними даними, а також розглядають звернення зацікавлених осіб щодо перевірки правомірності дій з персональними даними, а також відмови зацікавленим особам у наданні доступу до персональних даних. Стаття 23 Конвенції передбачає, що такий наглядовий орган має діяти цілком незалежно.

Положення стаття 25 Конвенції Європол, що стосуються технічного і організаційного захисту (безпеки) даних, майже тотожні за своїм змістом до відповідних положень статті 118 Шенгенської Конвенції. Зокрема, в обох документах передбачаються такі заходи як: контроль за доступом до обладнання, контроль за носіями і змістом даних, контроль за доступом до інформаційної системи, контроль за використанням, контроль за передачею, контроль за введенням, контроль за транспортуванням. Однак у додаток до передбачених в Шенгенській Конвенції заходів з безпеки, Конвенція Європол також вказує на необхідність забезпечення негайного налагодження систем, які вийшли з ладу, а також негайного повідомлення про помилкові операції. Вимагається також гарантування цілісності персональних даних у разі неправильного функціонування систем автоматизованої обробки.

Положення про технічний і організаційний захист (безпеки) персональних даних далі по тексту Конвенції Європол доповнюються в статтях 31 і 32. Крім того, Актом Ради Європейського Союзу від 3 листопада 1998 року затверджені правила про конфіденційність інформації Європолу. Передбачається, що рівень технічного і організаційного захисту (безпеки) персональних даних на території держав-членів Конвенції, був не нижчий за рівень захисту запроваджений Конвенцією Європол,

зазначеними правилами про конфіденційність інформації Європолу, а також у "Керівних принципах з безпеки".
Для інформації, що знаходиться у розпорядженні Європолу, крім тієї, що явно відноситься до відкритої для громадськості, за загальним правилом встановлюється основний рівень захисту. Інформації, що за своїм характером вимагає додаткових заходів з безпеки, надається умовне позначення за одним з трьох запроваджених рівнів безпеки:
"Європол 1" – рівень захисту інформації, несанкціоновані дії з якою можуть заподіяти *серйозну шкоду* для основних інтересів Європолу чи одній або більше держав-членів Європейського Союзу;
"Європол 2" – рівень захисту, несанкціоновані дії з якою можуть заподіяти *дуже серйозну шкоду* для основних інтересів Європолу чи одній або більше держав-членів Європейського Союзу;
"Європол 3" - рівень захисту, несанкціоновані дії з якою можуть заподіяти *екстремально-серйозну шкоду* для основних інтересів Європолу чи одній або більше держав-членів Європейського Союзу.
Запровадження такої системи маркування інформації не означає, що громадськість буде позбавлена можливості контролювати діяльність Європолу. Будь-яка зацікавлена особа також має право на доступ не лише до своїх персональних даних, але й до інформації про діяльність Європолу як і будь-якої іншої інституції Європейського Союзу. Це право закріплюється в Акті Ради ЄС від 20 грудня 1993 року "По доступ громадськості до документів Ради" , який прийнятий для забезпечення прозорості у роботі органів ЄС. Виключними легітимними підставами для відмови у наданні інформації для ознайомлення є захист:

- суспільних інтересів (державна безпека, міжнародні відносини, монетарна стабільність, розслідування злочинів, перевірки та дослідження);
- осіб, їх права на приватність;
- комерційної та виробничої таємниці;
- фінансових інтересів Європейських Співтовариств;
- конфіденційності, про що просить фізична чи юридична особа, що надала інформацію;
- конфіденційності роботи Ради ЄС тощо.

Отже, у громадян ЄС, а також громадян третіх держав є можливість скористатися своїм правом на доступ до інформації, що стосується діяльності Європолу, якщо це не за шкодитиме законним інтересам суспільства, інших осіб тощо.
Безперечно, що укладення як Шенгенської Конвенція, так і Конвенція Європол позитивно вплинуло на урегулювання питань обробки персональних даних у правоохоронній діяльності на Європейському рівні. Однак відсутність міжнародних стандартів присвячених захисту приватності персональних даних в контексті правоохоронної діяльності, які б мали обов'язків характер для держав-учасниць відповідного міжнародного договору, залишає багато не вирішених питань, що негативно відбивається на правах і свободах людини.
Положення про захист (приватності) персональних даних, які містяться в Шенгенській Конвенції і Конвенції Європол, справедливо критикуються за їх фрагментарність і наявність прогалин. Зокрема, в Шенгенській Конвенції підстави для внесення даних до інформаційної системи сформульовані дуже широко і дозволяють використовувати її, серед іншого, в політичних цілях для заборони в'їзду небажаних для влади осіб[19].
В цих же цілях інформаційна система може використовуватися для стеження за профспілковими активістами, правозахисниками, екологічними активістами. Саме через використання Шенгенської інформаційної системи були здійснені масові арешти

[19] Один з таких випадків трапився у 1998 році, коли активістці "Грінпісу" з Нової Зеландії було відмовлено у в'їзді до Нідерландів, оскільки її прізвище було внесено Францією до Шенгенської інформаційної системи як небажану особу з огляду на інтереси національної безпеки. Її "злочин" полягав у тому, що вона брала участь у демонстрації проти випробувань ядерної зброї, які проводила Франція.

учасників демонстрацій в Амстердамі під час підписання Амстердамського Договору у 1997 році[20].

Також підлягає удосконаленню механізм контролю за доступом до персональних даних, що містяться в Шенгенській інформаційній системі. Станом на 2000 рік налічується близько 48000 комп'ютерів підключених до Шенгенської мережі. Про порушення режиму конфіденційності в системі свідчить кримінальна справа, порушена у 1997 році проти двох офіцерів з Бельгії, які підозрювалися у наданні інформації з Шенгенської інформаційної системи для осіб, задіяних в організованому злочинному угрупуванні[21].

Конвенція Європол також не достатньо конкретно визначила питання додержання правил обробки персональних даних одержувачами даних. Принцип додержання заявленої цілі використання персональних даних чітко не приписаний в тексті Конвенції.

Ці та інші недоліки існуючого на Європейському рівні правового регулювання питань обробки персональних даних у правоохоронній діяльності були предметом уваги міжнародного семінару, проведеного у грудні 1999 року Радою Європи. За результатами семінару, були запропоновані рекомендації для покращення правового регулювання як на національному, так і міжнародному рівнях[22].

Зокрема, на національному рівні рекомендовано, щоб законодавство з питань захисту приватності персональних даних у правоохоронній діяльності ґрунтувалося як на загальному законі про захист (приватності) персональних даних, так і на спеціальних нормативно-правових актах з питань обробки персональних даних різними ланками правоохоронних (поліцейських) установ.

З огляду на зростаючий обсяг транскордонної передачі персональних даних під час співробітництва у галузі правоохоронної діяльності, рекомендується щоб перед початком передачі якість даних ретельно оцінювалася; здійснювався ефективний нагляд за законністю обробки; суб'єкти даних одержували ефективну допомогу навіть за межами національних кордонів.

На міжнародному рівні рекомендується вдосконалити регулювання передачі даних до країн, які не забезпечують адекватного захисту (приватності) персональних даних, посиливши відповідні вимоги до одержувачів.

Підсумовуючи вищевказане, слід відзначити, що питання регулювання обробки персональних даних у правоохоронній діяльності на Європейському рівні залишається відкритим. А його вирішення великою мірою залежатиме від успіху процесу подальшої співпраці країн ЄС у галузі створення простору свободи, безпеки і правосуддя на території Європейського Союзу.

Нашій державі слід вивчати досвід Європейських країн, однак орієнтуватися не лише на існуючі норми і стандарти у цій галузі. Щоб не відставати, треба прагнути бути на передніх позиція, намагаючись рухатися на крок попереду від стандартів сьогодення.

Розділ 3. Захист прав громадян у зв'язку з обробкою персональних даних в діяльності правоохоронних органів України

Конституційною основою, на якій будується законодавство України у галузі обробки персональних даних, є стаття 32 Конституції України, яка проголошує:

"Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України.

[20] Див.: Stephen Kabera Karanja. The Schengen Co-operation: Consequences for the right of EU Citizens. – 2000.

[21] Там само.

[22] Data protection in Police Sector. Council of Europe Regional Seminar under the activities for the development and consolidation of democratic stability // ADACS/DGI (2000) 3 Sem. – Strasbourg: 2000.

Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.
Кожний громадянин має право знайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не є державною або іншою захищеною законом таємницею.
Кожному гарантується судовий захист права спростовувати недостовірну інформацію про себе і членів своєї сім'ї та права вимагати вилучення будь-якої інформації, а також право на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням такої недостовірної інформації."

Як видно з тексту статті, право особи на контроль за збиранням, використанням та поширенням персоніфікованої інформації, як складової частини права на приватність персональних даних, може обмежуватися в інтересах національної безпеки, економічного добробуту та прав людини.
Боротьба із злочинністю має на меті саме захист цих цінностей, а тому обмеження права на приватність під час правоохоронної діяльності є виправданим. Однак, з іншого боку, будь-яке обмеження права може перетворитися на його порушення, якщо законодавством детально не регламентуються умови і порядок застосування таких обмежень, не передбачаються механізм контролю і гарантії відновлення обмежених прав. Саме такі недоліки властиві чинному законодавству України у галузі регулювання обробки персональних даних правоохоронними органами.
Частина 3 статті 32 Конституції України надає громадянам право на доступ до відомостей, що стосуються їх особисто, які не є державною або іншою захищеною законом таємницею. Цим фактично визнається, що інформація персонального характеру може бути віднесена до державної або іншої захищеної законом таємниці, що позбавляє громадян права на доступ до неї.
Заплутаність в питанні визначення режиму інформації персонального характеру за чинним законодавством України, віднесення її чи до відкритої, чи до конфіденційної або таємної, стала однією з причин розгляду Конституційним Судом України справи щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України "Про інформацію" та статті 12 Закону України "Про прокуратуру" (справа К.Г. Устименка).
Заявник по справі К.Г. Устименко за клопотанням адміністрації спеціального навчального закладу у 1998 році був поставлений на консультативний психіатричний облік за місцем проживання, а дізнався про це лише два роки потому. Він звернувся до головного лікаря психоневрологічного диспансеру з вимогою надання відомостей з питань постановки і зняття його з обліку, про можливі випадки повідомлення про це іншим особам, а також про застосовані до нього обмеження щодо працевлаштування за висновками психіатрів.
Посилаючись на лікарську таємницю, головний лікар диспансеру відмовив заявнику у надані такої інформації. Звернення до прокуратури не дали бажаного результату, посадові особи органів прокуратури, посилаючись на статтю 37 закону України "Про інформацію", відмовляли заявнику у наданні наявної інформації про стан його здоров'я. Суди загальної юрисдикції різних ланок неодноразово і неоднозначно розглядали скарги заявника, задовольнивши його вимоги частково. Заявник одержав копію диспансерної картки і деяку іншу інформація, що не задовольнило його в повній мірі.
Отже, в цій ситуації посадові особи державних органів, використовуючи хибні положення законодавства, зокрема, Законів України "Про інформацію" і "Основи законодавства України про охорону здоров'я" неправомірно відмовляли громадянину в доступі до інформації персонального характеру, посилаючись на лікарську таємницю.
Конституційний Суд України, констатуючи "наявність у нормативно-правовій базі в частині інформаційних правовідносин нечітко визначених, колізійних положень і прогалин, що негативно впливає на забезпечення конституційних прав і свобод людини і громадянина", конкретизував це таким чином:
"...вітчизняним законодавством не повністю визначено режим збирання, зберігання, використання та поширення інформації, зокрема, щодо психічного стану людини, її

примусового огляду та лікування, не створено процедуру захисту прав особи від протизаконного втручання в її особисте життя психіатричних служб. Закон України "Про інформацію" закріплює лише загальні принципи доступу громадян до інформації, що стосується їх особисто. Механізм реалізації зазначеного права належним чином не визначений. Відсутнє й регулювання використання конфіденційних даних у сфері психіатрії."

Конституційний Суд України дав офіційне тлумачення лише частинам четвертій і п'ятій статті 23 та статті 48 Закону України "Про інформацію", не знайшовши невизначеності в статтях 3, 31 , 47, як і в частині першій, другій, третій і шостій статті 23 Закону України "Про інформацію", які вимагали б офіційного тлумачення у контексті справи заявника.

Так, Конституційний Суд України розтлумачив, що забороняється не лише збирання, а й зберігання, використання та поширення конфіденційної інформації про особу без її попередньої згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту, прав та свобод людини. Тим самим, Суд повторив відповідні положення статті 32 Конституції України. При цьому, Конституційний Суд не надав відповіді на питання, яке становило суть справи, - якими є правомірні підстави для обмеження права громадян на доступ до своїх персональних даних, у тому числі тих, що знаходяться у розпорядженні правоохоронних органів (органів прокуратури).

Право на доступ до персональних даних є складовою частиною права на приватність, що підтверджується прецедентами Європейського Суду з прав людини[23]. З огляду на це, право на доступ до персональних даних повинно зазнавати обмежень у тих самих випадках, як і право на контроль за збиранням, зберіганням і використанням персональних даних, яке також становить складову права на приватність.

На нашу думку, частину третю статті 32 Конституції України, слід розуміти у такому значенні, що право на ознайомлення з відомостями про себе може обмежуватися лише тоді, якщо це необхідно в інтересах національної безпеки, економічного добробуту та прав людини. Саме в цих рамках слід тлумачити вираз, "*які не є державною або іншою захищеною законом таємницею*".

Ось чому, відмова державними установами і органами прокуратури в ознайомлені гр. Устименка з його медичними даними з посиланням на лікарську таємницю (яка є "*іншою захищеною законом таємницею"*) є порушенням його конституційного права, оскільки така відмова не мала на меті захист інтересів національної безпеки, економічного добробуту та прав людини.

Крім того, навіть застосовуючі обмеження права на приватність персональних даних в інтересах національної безпеки, економічного добробуту та прав людини слід виходити з принципу пропорційності. Тобто застосуванню обмежень у кожному конкретному випадку повинна передувати оцінка задіяних інтересів, наслідків дій правоохоронних органів, які обмежують права громадян тощо. Таку функцію повинен виконувати незалежний контрольний орган, насамперед, суд. Для цього законодавство повинно детально визначити порядок і підстави застосування обмежень, умови, межі, строки та інші суттєві ознаки цих обмежень.

Законом України від 18 січня 2001 року №2246-III внесенні суттєві зміни, які ліквідують багато недоліків Закону України "Про оперативно-розшукову діяльність" і покликані зміцнити законність в діяльності правоохоронних органів:

- змінами до завдань оперативно-розшукової діяльності, передбаченими в статті 1 Закону, виключається проведення оперативних заходів щодо інших протиправних діянь, ніж тих, відповідальність за які передбачена Кримінальним кодексом України;
- посилені вимоги щодо підстав для проведення оперативно-розшукової діяльності, що вимагає від правоохоронних органів детального обґрунтування необхідності проведення цих заходів. Згідно з частиною першою статті 6 Закону, підставою є "наявність достатньої інформації, одержаної в установленому законом порядку, що потребує перевірки за допомогою оперативно-розшукових заходів і засобів";

[23] Gaskin vs. the United Kingdom. - Judgment of 7 July 1989 // Judgments and decisions. - Series A no. 160

- обмежується втручання інших осіб у діяльність оперативних підрозділів і підкреслюється обмежений характер оперативних заходів. Якщо за попередньою редакцією пункту 1 статті 7, оперативні підрозділи були зобов'язані "виконувати письмові доручення слідчого, вказівки прокурора та ухвали суду і запити повноважних державних органів, установ та організацій про проведення оперативно-розшукових заходів", то за новою редакцією "у межах своїх повноважень відповідно до законів, що становлять правову основу оперативно-розшукової діяльності, вживати необхідних оперативно-розшукових заходів...";
- конкретизуються випадки застосування технічних засобів одержання інформації, процедура судового і прокурорського контролю (нагляду) за законністю цих дій, а також використання здобутої інформації у кримінальному судочинстві. Зокрема, передбачається, що "застосування цих заходів проводиться виключно з метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншим способом одержати інформацію неможливо". А рішення про надання або відмову в наданні дозволу на вжиття оперативних заходів і засобів приймає суд за поданням керівника відповідного оперативного підрозділу або його заступника, про що повідомляється прокуророві протягом доби. При цьому, "за результатами здійснення зазначених оперативно-розшукових заходів складається протокол з відповідними додатками, який підлягає використанню як джерело доказів у кримінальному судочинстві";
- внесення змін до статті 9 Закону надає суттєві гарантії забезпечення прав людини під час оперативно-розшукової діяльності. Зокрема, якщо раніше Законом чітко не встановлювався обов'язок оперативних органів заводити оперативно-розшукову справу у кожному випадку проведення заходів, то за новою редакцією "без заведення оперативно-розшукової справи проведення оперативно-розшукових заходів, крім випадку, передбаченого частиною четвертою цієї статті, забороняється". Про заведення справи виноситься постанова, яка затверджується керівником або заступником керівника правоохоронного органу. Постанова повинна містити підстави і мету заведення оперативно-розшукової справи, що покращує можливості для відомчого контролю за здійсненням оперативної діяльності;
- доповнення Закону України "Про оперативно-розшукову діяльність" статтями 9-1 "Строки ведення оперативно-розшукових справ" і 9-2 "Закриття оперативно-розшукових справ" встановлює процесуальні правила, які гарантують додержання часових рамок здійснення оперативно-розшукової діяльності, а значить і відповідних обмежень прав людини у часі.

Разом з цими позитивними змінами в регулюванні оперативно-розшукової діяльності в Україні слід, однак відмітити ті недоліки, які залишились у відповідному законодавстві і мають наслідком порушення права людини на приватність інформації персонального характеру.

Перш за все, це стосується питання доступу до інформації, яка збирається про особу під час оперативно-розшукової діяльності. Зокрема, частина 9 статті 9 Закону України "Про оперативно-розшукову діяльність" надає громадянам України та іншим особам право "у встановленому законом порядку одержати від органів, на які покладено здійснення оперативно-розшукової діяльності, письмове пояснення з приводу обмеження їх прав і свобод та оскаржити ці дії до суду". Тобто одержати можна пояснення щодо застосування передбачених Законом України "Про оперативно-розшукову діяльність" заходів, а не самі відомості, що були одержані в ході такої діяльності. Крім того, сам факт негласного збирання і використання інформації про особу не визнається обмеженням права.

На нашу думку, будь-яке незалежно від способів, методів і засобів збирання, зберігання, використання і поширення інформації персонального характеру без згоди особи (негласно) є обмеженням її прав. Оперативно-розшукова діяльність, під час якої збирається інформація про особу таємно від неї, з самого початку, тобто з моменту заведення оперативно-розшукової справи, є обмеженням прав і свобод людини.

Частина 10 статті 9 Закону забороняє передачу і розголошення відомостей про нерозкриті злочини або такі, що можуть зашкодити слідству чи інтересам людини, безпеці України тощо. Згідно з частиною 13 цієї статті в попередній редакції "не підлягають передачі і розголошенню результати оперативно-розшукової діяльності, які відповідно до законодавства України становлять державну, військову і службову таємницю, а також відомості, що стосуються особистого життя, честі, гідності людини". Внаслідок змін, внесених Законом України від 18 січня 2001 року, слова "військову і службову" були виключені з тексту статті, що є позитивним прикладом "викорчування хвороби засекречування" з правових норм, що регулюють інформаційні питання.

Частина 13 статті 9 Закону України передбачає, що не підлягають передачі і розголошенню результати оперативно-розшукової діяльності, які становлять державну таємницю. Регламентація цього питання за чинним законодавством України не гарантує права доступу значного кола суб'єктів даних до інформації персонального характеру, яка була зібрана і використовувалась під час оперативно-розшукової діяльності.

Затверджений наказом Голови Служби безпеки України від 1 березня 20001 року № 52 Звід відомостей, що становлять державну таємницю, відносить до державної таємниці у сфері державної безпеки і охорони правопорядку відомості "про факт підготовки та проведення, а також результати негласних оперативно-розшукових заходів із застосуванням оперативно-технічних засобів стосовно осіб, які готують або вчинили особливо небезпечні злочини проти держави" (п.4.18), а також "ті самі відомості стосовно осіб, які готують або вчинили інші тяжкі злочини" (п. 4.18.1). До останнього пункту є примітка, що "у разі використання отриманої інформації як доказ у кримінальному процесі, зниження її ступеня секретності чи розсекречення здійснюється згідно з чинним законодавством України".

Таким чином, незалежно від підтвердження чи не підтвердження фатів причетності людини до підготовки або вчинення особливо небезпечного злочину проти держави, використання чи невикористання цих відомостей у кримінальному судочинстві, доступ до першої з вказаних категорій відомостей із ступнем секретності "Цілком таємно" для громадян, яких стосується інформація, заборонений.

Доступ до другої категорії відомостей із ступнем секретності "Таємно", незалежно від підтвердження чи не підтвердження фатів причетності людини до підготовки або вчинення іншого тяжкого злочину проти держави, можливий лише після прийняття рішення про зниження ступеня її секретності чи розсекречення і лише у випадку використання отриманої інформації як доказ у кримінальному процесі.

Однак доступ людини до інформації персонального характеру, яку одержали оперативні органи в інших випадках, також практично неможливий. Частина 12 статті 9 Закону "Про оперативно-розшукову діяльність" забороняє зберігання і обов'язує відповідальних осіб оперативних органів знищувати "одержані внаслідок оперативно-розшукової діяльності відомості, що стосуються особистого життя, честі, гідності людини, якщо вони не містять інформацію про вчинення заборонених законом дій".

Закон не дає визначення поняттю "відомості, що стосуються особистого життя, честі, гідності людини", а воно може тлумачитись як завгодно широко чи вузько. Насправді, громадянин ніколи не зможе дізнатися, яку саме інформацію про нього було зібрано, використано і знищено.

Отже, ті позитивні надбання, які впроваджені в Закон України "Про оперативно-розшукову діяльність" потребують свого подальшого розвитку шляхом розширення гарантій забезпечення права людини на приватність інформації персонального характеру.

Більшість питань обробки персональних данних в діяльності правоохоронних органів України регулюються секретними відомчими нормативними актами. В той же час, стаття 32 Конституції України встановлює, що випадки застосування обмежень права на приватність персональних даних повинні **визначатися законом**. Це означає, що підзаконні нормативні акти, а тим більше відомчі "для службового користування" не можуть встановлювати будь-яких обмежень прав і свобод людини.

Для ліквідації існуючих недоліків і прогалин у законодавстві, що регулює оборобку персональних даних в діяльності правоохоронних органів, вимагається прийняття як

базового закону, що захищатиме право громадян на приватність персональних даних, так і спеціальних законів з обробки персональних даних у діяльності правоохоронних органів України. В цьому може бути корисним досвід європейських країн.

Приведення нормативно-правового регулювання діяльності правоохоронних органів і практики його застосування у відповідність до вироблених міжнародною спільнотою правових стандартів, повинно сприяти ефективній реалізації права громадян на приватність персональних даних, а також повноцінній участі України в міжнародному співробітництві з різних питань правоохоронної діяльності, зокрема, на регіональному європейському рівні.