Рекомендація № R(87)15
Комітету Міністрів державам-членам, що регулює використання персональних даних у секторі поліції (Схвалено Комітетом Міністрів 17 вересня 1987 на 410-й зустрічі заступників Міністрів).

Комітет Міністрів згідно зі Статтею 15б Статуту Ради Європи,

враховуючи, що мета Ради Європи — досягнення більшої єдності між її членами,

зважаючи на зростаюче використання персональних даних для автоматизованої обробки у секторі поліції та майбутньою користю від застосування комп'ютерів та інших технічних засобів у цій сфері,

беручи до уваги стурбованість можливою загрозою приватності особи, що виникає внаслідок неправильного застосування методів автоматизованої обробки,

визнаючи необхідність збалансування інтересів суспільства щодо запобігання й припинення кримінальних правопорушень і підтримання громадського порядку, з одного боку, та інтересів особи і її права на приватність, з іншого боку,

пам'ятаючи про положення Конвенції про захисту осіб стосовно автоматизованої обробки персональних даних від 28 січня 1981 року, і зокрема про винятки дозволені на підставі Статті 9,

усвідомлюючи також положення Статті 8 Конвенції про захист прав людини та основних свобод,

Рекомендує урядам держав-членів:

керуватися в їх внутрішньому законодавстві та практиці принципами, доданими до цієї Рекомендації; та

забезпечувати доступність для громадськості положень, доданих до цих Рекомендацій, зокрема що стосуються прав, які надаються індивідам через їх застосування.

Додаток до Рекомендації № R(87)15
Сфера застосування і визначення

Принципи, що містяться в цій Рекомендації, стосуються збирання, зберігання, використання та передачі персональних даних які є об'єктом автоматизованої обробки, в цілях поліції.

В цілях цієї Рекомендації вираз "персональні дані" означає будь-яку інформацію, що стосується ідентифікованої чи не ідентифікованої особи. Особа не повинна розглядатися як така, що ідентифікується, якщо ідентифікація вимагає невиправданих витрат часу, коштів або людських ресурсів.

Вираз "у цілях поліції" означає всі завдання, які можуть розв'язувати органи поліції для запобігання чи припинення кримінальних правопорушень та досягнення громадського порядку.

Вираз "відповідальний орган" (контролер файлу) означає орган, службу чи будь-яку іншу організацію, уповноважену згідно з національним Законом вирішувати питання про цілі автоматизованого файлу, категорії персональних даних, що мають зберігатися, та операцій, які можуть застосовуватися до них.

Держави-члени можуть застосовувати принципи, що містяться в цій Рекомендації, до персональних даних, що не підлягають автоматизованій обробці.

Ручна обробка даних не повинна проводитись, якщо її метою є невиконання положень цієї Рекомендації.

Держави-члени можуть поширювати принципи, що містяться в цій Рекомендації, на дані, що стосуються груп людей, асоціацій, фундацій, компаній або будь-якої іншої організації, що складається безпосередньо або опосередковано з індивідів, незалежно від того, чи такі організації мають статус юридичної особи.

Положення цієї Рекомендації не повинні витлумачуватися як такі, що обмежують або якось перешкоджають можливості держав-членів поширювати при потребі окремі з цих принципів на збирання, зберігання та використання персональних даних в цілях державної безпеки.

Основні принципи

Принцип 1 - Контроль та повідомлення

1.1 Кожна держава-член повинна мати незалежний наглядовий орган за межами поліцейського сектору, який би відповідав за забезпечення поваги до принципів, викладених у цій Рекомендації.

1.2 Нові технічні засоби обробки даних можуть запроваджуватися лише в разі, коли вжито всіх розумних заходів щоб їх використання відповідало духові існуючого законодавства про захист даних.

1.3 Відповідальний орган повинен радитись із наглядовим органом заздалегідь у будь-якому випадку, коли застосування методів автоматизованої обробки породжує проблему із втіленням цієї Рекомендації.

1.4 Постійні автоматизовані файли повинні повідомлятися наглядовому органу. Повідомлення повинно вказувати на характер кожного задекларованого файлу, установу відповідальну за його обробку, її цілі, тип даних, що містяться у файлі, а також осіб, яким ці дані передаються.

Тимчасові (*ad hoc*) файли, які були створені під час конкретного розслідування, також повинні повідомлятися контролюючого органу у відповідності з умовами, встановленими останнім, або згідно з національним законодавством.

Принцип 2 - Збір даних

2.1 Збір персональних даних у цілях поліції повинен обмежуватись тією мірою, якою необхідно для відвернення реальної небезпеки чи припинення кримінального правопорушення особливого характеру. Будь-який виняток з цього положення повинен бути предметом спеціального національного законодавства.

2.2 Якщо дані про індивіда були зібрані і зберігаються без його відома, і якщо дані не знищені, він повинен бути поінформований, у разі доцільності, що інформація про нього тримається як тільки предмет діяльності поліції більше не цікавить її.

2.3 Збір даних за допомогою технічних чи інших автоматизованих засобів може здійснювати лише у відповідності до особистих положень.

2.4 Збір даних про осіб лише на тій підставі, що вони мають особливе расове походження, особливі релігійні переконання, сексуальну поведінку чи політичні погляди або належать до особливих рухів чи організацій, які не оголошені поза законом, повинен заборонятися. Збір даних, що торкаються цих питань, може здійснюватися у разі виняткової потреби для цілей конкретного розслідування.

Принцип 3 - Зберігання даних

3.1 Наскільки можливо, зберігання персональних даних для цілей поліції має обмежуватися точними даними, які необхідні поліції для виконання її підрозділами правомірних завдань у межах внутрішнього законодавства та обов'язків, визначених міжнародним правом.

3.2 Наскільки можливо, різні категорії даних мають розрізнятися при зберіганні за ступенем їх точності або надійності, а саме: дані, що ґрунтуються на фактах, мають відрізнятися від тих, що основані на міркуваннях чи особистих оцінках.

3.3 Якщо дані зібрані для адміністративних цілей зберігатимуться постійно, їх слід тримати в окремому файлі. В будь-якому разі, слід вжити заходів, щоб адміністративні дані не підпадали під привила, що застосовуються для поліцейських даних.

Принцип 4 - Використання даних поліцією

4. Згідно з Принципом 5, особливі дані, зібрані й збережені поліцією для цілей поліції, мають використовуватися винятково в цих цілях.

Принцип 5 - Передача даних

5.1 Повідомлення у межах сектору поліції

Передача даних між підрозділами поліції для використання їх у цілях поліції повинна дозволятися, якщо існує законна підстава для їх передачі у межах законних повноважень цих підрозділів.

5.2 і. Повідомлення іншим державним органам

Передача даних іншим державним органам дозволяється в окремих випадках, якщо:

а) існує чіткий законний обов'язок або дозвіл чи з санкції наглядового органу, або якщо

б) ці дані необхідні одержувачу для виконання ним його правомірного завдання, при цьому передбачається, що ціль збирання чи обробки, яка здійснюватиметься одержувачем, не є несумісною з первинною обробкою, а правові зобов'язання передаючого органу, не суперечать цьому.

5.2 іі. Крім того, передача іншим державним органам дозволяється винятково у таких окремих випадках:

а) коли повідомлення, поза всяким сумнівом, здійснюється в інтересах суб'єкта даних або коли останній дав на це згоду чи коли обставини вказують на явну презумпцію такої згоди;

б) коли передача даних необхідна для відвернення серйозної навислої небезпеки.

5.3 і. Повідомлення приватним структурам

Повідомлення даних приватним структурам дозволяється, зокрема, коли існує інше законне зобов'язання або дозвіл чи санкція наглядового органу.

5.3 іі. Повідомлення приватним структурам дозволяється як виняток у таких випадках:

а) повідомлення здійснюється в інтересах суб'єкта даних або коли останній дав на це згоду чи коли обставини вказують на наявність такої згоди;

б) повідомлення необхідне для відвернення серйозної навислої загрози.

5.4 Міжнародна передача

Повідомлення даних органам влади іноземних держав повинно обмежуватися органами поліції. Воно дозволяється лише:

а) коли існує чітке правове забезпечення за внутрішнім чи міжнародним правом;

б) за умови відсутності такого забезпечення, якщо передача необхідна для запобігання серйозної навислої небезпеки або потрібна для припинення серйозного кримінального правопорушення, відповідно до звичайного права,

і забезпечується, щоб національне регулювання захисту особи не було під загрозою порушення.

5.5 і. Запити про повідомлення

Згідно зі спеціальними положеннями внутрішнього законодавства чи міжнародних угод, у запитах про передачу інформації повинна вказуватись організація чи особа, що робить запит, а також причина запиту та її правомірність.

5.5 іі. Умови повідомлення

Якість даних повинна за можливістю перевірятися щонайпізніше в час їх повідомлення. При всіх повідомленнях даних по можливості зазначається юридичне рішення щодо цього, а також рішення не робити передачу і дані, що спираються на точку зору або особисте враження, перевіряються, перш ніж бути переданими, при цьому зазначається міра достовірності й надійності повідомленого.

Якщо виявиться, що дані вже не точні на даний момент їх не слід передавати. Якщо дані, що не є точними або актуальними передано, то організація, яка здійснила передачу, повинна за можливістю інформувати одержувача даних про їх невідповідність.

5.5 iii. Захист передачі

Дані, повідомлені іншим державним органам, приватним структурам чи іноземним органам, не повинні використовуватися в інших цілях, окрім тих, що зазначені в запиті.

Використання даних в інших цілях, що не передбачені в параграфах 5.2 чи 5.4 цього принципу, повинне бути узгоджене з організацією, що здійснює передачу.

5.6 Взаємо-пов'язування файлів і доступ до файлів у діалоговому режимі

Пов'язування файлів до файлів, здійснюване в різних цілях, підлягає одній з умов:

(а)згода наглядового органу для цілей розслідування у випадку певного правопорушення, або

(б) згідно з чітким правовим положенням.

Прямий доступ (доступ у діалоговому режимі) до файлу може дозволятися лише, якщо це узгоджується із внутрішнім законодавством, яке повинне враховувати Принципи 3 - 6 цієї Рекомендації.

Принцип 6 - Доступність для громадськості, право доступу до файлів поліції, право виправлення і право на оскарження

6.1 Наглядовий орган повинен вживати заходів, щоб громадськість була поінформована про існування файлів, які є об'єктом повідомлення, а також про її права стосовно цих файлів. Втілення цього принципу передбачає врахування особливого характеру тимчасових (*ad hoc*) файлів, зокрема потребу уникати серйозних перешкод щодо виконання законного завдання поліцейськими органами.

6.2 Суб'єкт даних повинен мати змогу доступу до поліцейського файлу в розумних інтервалах і без надмірного зволікання згідно з положеннями внутрішнього законодавства.

6.3 Суб'єкт даних повинен мати змогу зробити, де це необхідно, виправлення його даних, що містяться у файлі.

Персональні дані, які через реалізацію права доступу виявились неточними або надмірними чи невідповідними будь-якому з інших принципів, що містяться в цій Рекомендації, повинні або знищуватися, виправлятися або супроводжуватися уточнюючою запискою, доданою до файлу.

Таке знищення або корегування повинні поширюватися наскільки це можливо на всі документи, що супроводжують поліцейський файл, і здійснюватися негайно або принаймні під час подальшої обробки даних або їх наступної передачі.

6.4 Застосування прав доступу, виправлення та знищення може обмежуватись лише тією мірою, наскільки це обмеження є необхідним для виконання законного завдання поліції або необхідне для захисту суб'єкта даних чи прав і свобод інших осіб.

В інтересах суб'єкта даних письмовий коментар повинен не допускатися законом у специфічних справах.

6.5 Відмова в цих правах чи їх обмеження повинне пояснюватися письмово із зазначенням причин. Єдиним випадком, коли відмовляють в ознайомленні з цими причинами, є необхідність виконання правомірного завдання поліції або необхідність захисту прав і свобод інших осіб.

6.6 Якщо в доступі відмовлено, суб'єкт даних повинен мати можливість оскаржити це до наглядового органу або іншого незалежного органу, який має підтвердити, що відмова належно обґрунтована.

Принцип 7 - Тривалість зберігання і оновлення даних

1.1 Повинно забезпечуватися, щоб персональні дані, які зберігалися для поліцейських цілей, знищувалися якщо вони більше не потрібні для цілей, заради яких вони зберігалися.

З цією метою особлива увага звертається на такі критерії: необхідність зберігання даних у світлі висновку слідства в особливому випадку; остаточне судове рішення, зокрема у випадку виправдання; реабілітація; виконаний вирок; амністія; вік суб'єкта даних; особливі категорії даних.

1.2 Правила націлені на зазначення терміну зберігання персональних даних різних категорій, так само як і регулярні перевірки їх якості, мають визначатися за погодженням з наглядовим органом або згідно з внутрішнім законодавством.

Принцип 8 — Схоронність даних

2. Відповідальний орган повинен вжити всіх заходів, щоб забезпечити належну фізичну і логічну схоронність даних і запобігти їх несанкціонованому доступу, передачі чи зміні.

При цьому мають враховуватися характер і зміст файлів.

ПОЯСНЮВАЛЬНА ЗАПИСКА

Вступ

1. Не зважаючи на те, що принципи захисту даних, викладені в Конвенції про захист осіб стосовно автоматизованої обробки персональних даних (відомій також як Конвенція про захист даних) від 28 січня 1981 року, широко застосовуються при збиранні, зберіганні, використання тощо персональних даних як у приватному, так і державному секторах, відчувається необхідність пристосувати їх до специфічних вимог особливих секторів.

2. "Секторний підхід" до захисту даних зумовив прийняття Комітетом Міністрів Ради Європи чотирьох рекомендацій, вироблених її Міжурядовим Комітетом експертів із захисту даних (СІ-РД): Рекомендація № R(81)1 про правила для автоматизованих банків медичних даних (від 23 січня 1981р.), Рекомендація № R(83)10 із захисту персональних даних, використовуваних у наукових дослідженнях та статистиці (від 23 вересня 1983р.), Рекомендація №R(85)20 із захисту персональних даних, використовуваних в цілях прямого маркетингу (від 25 жовтня 1985р.) і Рекомендації № R(86)1 із захисту персональних даних, використовуваних у секторі соціального забезпечення (від 23 січня 1986 р.).

3. У зв'язку з таким секторним підходом, Комітет експертів із захисту даних дійшов висновку про доцільність реагування на проблеми захисту даних, породжених використанням персональних даних у секторі поліції, також про підготовку законодавчого інструменту провадження низки принципів, створених для врегулювання збирання, зберігання, використання, передачі і консервації персональних даних поліцією, який був би витлумачений у межах норм, викладених у Конвенції про захист даних.

4. Враховуючи зростання ролі поліції в житті людей, зумовлену новими загрозами суспільству у вигляді тероризму, наркобізнесу тощо, а також загальним зростанням злочинності, було визнане за необхідне виробити чинні керівні принципи для сектору поліції, які б підкреслювали таке необхідне в наших суспільствах збалансування прав особи та правомірної діяльності поліції, коли остання звертається за допомогою до технологій обробки даних.

5. Беручи до уваги, що параграф другий Статті 9 цієї Конвенції дозволяє державам-членам відхилятися від принципів захисту даних Конвенції з метою "припинення кримінальних правопорушень" комітет експертів уповноважив робочу групу окреслити проблеми, що виникають при використанні персональних даних у секторі поліції й виробити чіткі пропозиції щодо їх вирішення. Робочу групу склали експерти з Бельгії, Франції, Італії, Нідерландів, Португалії, Швеції, Швейцарії та Об'єднаного Королівства. Під головуванням д-ра Р. Швейзера (Швейцарія) робоча група провела п'ять зустрічей.

6. Протягом першої зустрічі (19 і 20 грудня 1983р.) робоча група спробувала визначити, якою мірою законодавства держав-членів забезпечені спеціальними

положеннями, що регулюють використання персональних даних у секторі поліції. Крім того, було зроблено широкий огляд проблем цього сектору щодо захисту даних. У зв'язку з цими завданнями робоча група була забезпечена дослідженням, проведеним консультантом, професором Х. Маісл (Франція).

7. Під час другої зустрічі (з 18 по 20 червня 1984р.) члени робочої групи поглибили вивчення питань, врахувавши відповіді отримані від держав-членів на запитання. Крім того, робоча група проаналізувала відповідні судові прецеденти Європейського Суду та Європейської Комісії з прав людини у контексті Статті 8 Європейської Конвенції з прав людини, яка є основоположною для збирання, використання, зберігання тощо персональних даних поліцією.

В процесі обговорення було вироблено проект, який відображає бачення робочою групою шляхів урегулювання використання персональних даних у сфері поліції.

8. На третій зустрічі (з 17 по 19 грудня 1984р.) робоча група приступила до перегляду попереднього проекту. Уважному розгляду було піддано, зокрема, перелік обмежень, викладених у параграфі другому Статті 9 Конвенції про захисту даних. Робоча група дійшла згоди про доцільність заснування спеціальних принципів захисту даних для класичних та вирішальних завдань поліції, пристосувавши їх до особливих вимог, особливо по відношенню до завдання "припинення кримінальних правопорушень".

9. Спираючись на коментарі та огляди, представлені пленарним комітетом, обізнаним про результати робочої групи, робоча група поширила свій аналіз під час подальших зустрічей (5-7 червня 1985, 27-29 листопада 1985р.), щоб вирішити такі питання, як повідомлення даних поліцією третім сторонам і особливо транскордонні потоки даних. Пленарному комітету було представлено остаточний текст проекту пояснювального меморандуму, підготовленого секретаріатом.

10. Комітет експертів схвалив проект рекомендації і проект пояснювального меморандуму на 13-й зустрічі (4-7 листопада 1986р.) після докладного ознайомлення і вирішив надати ці тексти Європейському Комітету з правового співробітництва (CDCJ) для ознайомлення і схвалення.

11. Проект рекомендації і проект пояснювального меморандуму були схвалені Європейським Комітетом з правового співробітництва 22 травня 1987 року.

12. Рекомендація № R(87)15, що регулює використання персональних даних у секторі поліції, була затверджена Комітетом Міністрів Ради Європи 17 вересня 1987р.

Докладні коментарі

Преамбула

13. Техніка все ширше застосовується в роботі поліції. У секторі, де збирання, зберігання величезної кількості персональної інформації необхідне з урахуванням різнопланової й важливої ролі поліції в суспільстві, переваги від використання технічних засобів не заперечні. Різноманітна злочинність вимагає вироблення таких же витончених методів боротьби з правопорушеннями. Комп'ютери дозволили поліції піднести її ефективність у збиранні персональних даних та сприяти швидкому прийняттю рішень у посиленні законності на користь суспільства.

14. Разом з тим, проблеми, що спричинили прийняття Конвенції про захист прав осіб стосовно автоматизованої обробки персональних даних від 28 січня 1981 року у зв'язку з посиленим використанням автоматизації в усіх сферах, особливо гостро відчувається у сфері поліції. Саме в цій сфері наслідки порушення основоположних принципів, викладених у цій Конвенції, особливо тяжко позначаються на індивіді.

15. Преамбула визначає необхідність досягнення збалансованості між інтересами зацікавлених сторін: інтересами особи і його правом на приватність та інтересами суспільства в запобіганні й припиненні кримінальних правопорушень та підтримані громадського порядку.

16. Не дивно, що збалансування важливо досягти в поліцейському секторі. Стаття 8, параграф 2 Європейської Конвенції з прав людини та Стаття 9 Конвенції про захист даних дозволяють робити винятки з прав, які вони пропонують.

17. Незважаючи та те, що преамбула застерігає щодо можливої загрози приватності особи внаслідок неправильного застосування методів автоматизованої обробки, варто мати на увазі, що приватність не можна витлумачувати лише як захист чиєїсь приватної сфери від настирливості. З цієї причини преамбула звертає увагу на Статтю 8 Конвенції про захисту прав людини та основних свобод, на законність застосування певних технічних засобів стеження для отримання даних про людей, і на те, щоб ті узгоджувалися з положеннями Статті 8 та відповідними висновками Європейського Суду з прав людини.

18. Звернення до підслуховування телефонних розмов та перехоплення кореспонденції - приклади зневажання приватного життя у строгому розумінні. Європейський Суд з прав людини ухвалив таке рішення у двох справах (Справа Класса [Klass] та ін., судове рішення від 6 вересня 1978р., серія А, №28; справа Мелоуна [Malone], судове рішення від 2 вересня 1984р., серія А, №82). Принципи 2.2 та 2.3, зокрема, мають витлумачуватися у світлі судових прецедентів цього Суду.

19. Проте преамбула також посилається на положення Конвенції про захист прав осіб стосовно автоматизованої обробки персональних даних від 28 січня 1981 року, які виходять за рамки традиційного визначення приватності, і встановлює низку захисних принципів, розроблених з метою врегулювання збирання, зберігання, використання та передачі персональних даних.

20. Спеціальна увага в преамбулі приділена обмеженням, дозволеним згідно зі Статтею 9 Конвенції захисту даних; це буде нагадуванням про те, що винятки з положень Статті 5 (“якість даних”), Статті 6 (правила про “спеціальні категорії даних”) та Статті 8 (“додаткові гарантії для суб’єкта даних”) санкціонуються лише тоді, коли вони передбачаються законом і є необхідним заходом у демократичному суспільстві винятково в інтересах, серед іншого, “припинення кримінальних правопорушень”. Пам’ятаючи, що Європейський Суд з прав людини своїм рішення у справі Мелоуна визначив кілька чітких критеріїв (точність, переконливість, передбачуваність тощо), можна сподіватися, що принципи, викладені в цьому рекомендаційному правовому документі, повинні служити корисними порадами законодавцю у справі витлумачення обмежень у Статті 9, параграф 2 Конвенції про захист даних при регулюванні збиранні, використанні тощо персональних даних у сфері поліції. Це слід мати на увазі в контексті, наприклад, параграфу 2.1.

21. Ясна річ, що перелік обмежень вужчий, ніж суспільні інтереси, окреслені у п’ятому параграфі преамбули. Проте мета цієї Рекомендації полягає в тому, щоб установити спеціальні принципи захисту даних для класичних та вирішальних завдань поліції, а також пристосувати ці принципи до особливих вимог, зокрема заходів з “припинення кримінальних правопорушень”. Зрозуміло, що персональні дані, зібрані й використовувані в цілях, що не підпадають під класичну діяльність поліції, наприклад, в адміністративних цілях, підлягають загальним нормам захисту даних.

Сфера застосування та визначення понять

22. Ці принципи покликані врегульовувати всі критичні моменти, коли виникає питання про захист даних при збиранні, зберіганні, використані й передачі персональних даних. Нагадаємо, що всі ці дані певним чином пов’язані з “цілями поліції”. Останній термін витлумачується з точки зору інтересів суспільства, про які йшлося у п’ятому параграфі Преамбули. Зауважимо, що в цьому остаточному документі термін цей в подальшому уточнюватиметься по тексту, що забезпечуватиме різне витлумачення завдань поліції по боротьбі з кримінальними правопорушеннями і тих які вона повинна виконувати по їх запобіганню й підтриманню громадського порядку.

23. Ця Рекомендація стосуються просто “органів поліції”. Слід пам’ятати, що відповідно до конкретної законодавчої системи можуть співіснувати різні поліцейські

органи. Можливо, не завжди легко їх розрізнити з точки зору розподілу функцій. Проте, незважаючи на номенклатуру ці принципи повинні застосовуватись до будь-якого органу з функціями поліції, що займаються збиранням, зберіганням, використанням та передачею персональних даних у цілях, викладених у третьому параграфі цього розділу.

24. Ця Рекомендація торкається в першу чергу автоматизованих персональних даних; термін "персональні дані" визначається в попередніх рекомендаціях Ради Європи у сфері захисту даних. Варто нагадати, що незалежно від того, вважається особа ідентифікованою чи ні, вона мусить визначатися об'єктно ідентифікованою, враховуючи вишукані методи ідентифікації, наприклад, техніку відбитків пальців, систему розпізнавання голосів, службу банків даних тощо.

25. "Відповідальний орган", згадуваний у цьому розділі, є в дійсності, за термінологією Конвенції, контролером файлу. Відповідно, цей орган буде нести максимальну відповідальність за файл. У Принципі 1.4 буде з'ясовано, що назва відповідального органу для конкретного файлу повинна бути повідомлена наглядового органу.

26. Хоча цей документ присвячується автоматизованим персональним даним, як і законодавство певної кількості держав-членів, загальновідомо, що деяка частина держав Ради Європи все ще більшою мірою покладається на ручні файли. В інших країнах, де комп'ютеризація поліції поставлена добре, дані, що зберігаються в комп'ютерах, можуть бути зрозумілими лише тоді, якщо робиться посилання на ручні файли. Тому не бажано вилучати ручні файли, з цієї причини цим документом визнається, що держави-члени вільні поширювати ці принципи на дані, утримувані в ручній формі. Параграф 38, як буде видно далі, забезпечує вказівки щодо того, як держави-члени повинні трактувати питання ручного утримання даних.

27. З впливом часу, зрозуміло, все більш даних, утримуваних сьогодні в ручній формі, будуть автоматизовані, а тому принципи, що містяться у цьому документі, будуть поширюватися й на них. Проте не слід допускати, щоб держава-член навмисно обходила гарантії, викладені в цьому документі, перетворюючи персональні дані з автоматизованих файлів у ручні файли. Слід визнати, проте, що визначити, чи мав місце навмисний обхід, буває важко, якщо дані знищуються згідно з Принципом 7, а роздруковані дані залишаються.

28. Згідно з Статтею 3, параграф 2, Конвенції про захист даних, цей документ також визнає, що держави-члени мають можливість застосовувати ці принципи до юридичних осіб.

29. Нарешті, стосовно питань державної безпеки, які пояснювальна записка до Конвенції про захист даних подає як "захист державного суверенітету від внутрішньої чи зовнішньої загрози, включаючи захист міжнародних відносин держави", бажано визнавати право держав-членів поширити деякі з гарантій, передбачених цим документом, на сферу держаної безпеки, де їх використання можливе й принагідне.

30. В контексті питання державної безпеки та юридичних осіб, слід пам'ятати, що принципи, викладені в цій Рекомендації, були визнані розробниками як мінімальні гарантії, і що державам-членам залишено право посилювати заходи захисту.

Принцип 1 - Контроль і позначення

31. Органи захисту даних або уповноважені виконують головну функцію за внутрішнім законодавством у захисті даних. Там, де такі органи існують, їм мають бути передані функції, викладені в цієї Рекомендації. Не бажано створювати ще один окремий орган в цілях цієї Рекомендації. Проте, будь-який новий орган, що створюється, повинен бути незалежним від контролю поліції; суттєву якісну можливість містить Рекомендація, уповноважуючи на певних етапах цей орган приймати рішення, оцінюючи межі обмеження діяльності поліції щодо використання персональних даних.

32. Конституційна структура певних держав-членів може вимагати створення кількох незалежних наглядових органів, де органи захисту даних чи уповноваженні ще не існують. Орган не обов'язково має бути колегіальним. Допустимо, що якась особа виконуватиме функцію "забезпечення повагу до принципів викладених у цій Рекомендації". Проте, віддаючи належне важливості цієї ролі, бажано, щоб наглядовий орган, незалежно від його форми, мав достатньо ресурсів, щоб бути ефективним.

33. Слід також наголосити, що відсутність загального законодавства про захист даних не є перешкодою для створення незалежного наглядового органу у сфері поліції. Принципи, викладені в цій Рекомендації, адресовано всім державам-членам і можуть використовуватись країнами, яким ще належить прийняти загальні норми із захисту даних.

34. Цією преамбулою визнається, що, крім, комп'ютерів, інші нові технічні засоби обробки даних також підносять ефективність роботи поліції, наприклад, системи розпізнавання голосів, розпізнані машиною ідентифікаційні картки, технології стеження з використання комп'ютера, електронні системи стеження. Проте, враховуючи можливість їх неправильного використання, важливо, щоб їх запровадження й використання супроводжувалися усвідомленням їх впливу на індивіда. З цією метою Принцип 1.2 рекомендує зважливо підходити до їх запровадження, не вступаючи в конфлікт духом існуючого законодавства із захисту даних. Крім того, потрібні будуть широкі обговорення доцільності впровадження нових технологій, які можуть становити загрозу приватності, якщо це не буде взято до уваги законодавцями під час прийняття норм захисту даних.

35. У зв'язку з цим незалежний наглядовий орган покликаний виконувати важливу роль. Згідно з Принципом 1.3 він має бути посилений у повноваженнях, щоб здійснювати моніторинг за клопотанням відповідального органу, коли останній має намір запроваджувати методи автоматизованої обробки даних, що можуть породити проблеми із застосуванням цих рекомендацій. Принцип 1.3 не передбачає застосування права вето на запровадження таких методів. Проте, вони дозволяють наглядовому органові перевіряти запропоновані методи, щоб переконатися, що ті не обходять принципи, наприклад, що стосуються передачі даних (Принцип 5). Він може порадити відповідальному органові вжити певних заходів, щоб забезпечити дотримання принципів Рекомендації.

36. В цілях цього документу "файли поліції" - це всі структуровані/упорядковані персональні дані, які відповідають вимогам служб поліції з точки зору запобігання чи припинення кримінальних правопорушень або підтримання громадського порядку. Файли поліції, як це визначається, сприяють поліції отримувати інформацію, що стосується ідентифікованих чи не ідентифікованих осіб. Принцип 1.4 зобов'язує поліцію або, можливо, якийсь інший орган, призначений національним законодавством, повідомити про свої автоматизовані файли наглядовий орган і охарактеризувати певні деталі, що стосуються кожного автоматизованого файлу.

37. Зауважимо, що це загальна вимога повідомлення. Жодних винятків не робиться щодо файлів, що стосуються винятково припинення кримінальних правопорушень. Як зазначалося раніше, Рекомендація призначена для вироблення спеціальних правил для типових завдань поліції, єдиним винятком з яких, коди це необхідно, є врахування особливостей вимог поліції в контексті "припинення кримінальних правопорушень".

38. Незважаючи на те, що правила повідомлення обмежуються автоматизованими поліцейськими файлами, може бути випадок, що якісь держави-члени скористаються їх правом поширити принципи, викладені в цьому документі, на ручні файли.

Якщо таке станеться, держава-член може зобов'язати поліцію зробити позначення кожного типу утримуваного файлу, контролера файлу, його ціль, характер даних, що містяться в ньому, та осіб, яким ці дані повідомляються. Таке загальне позначення повинно повідомлятися наглядовому органу. Як альтернатива, потребу в повідомлені кожного опису можна уникнути, якщо кожен підрозділ поліції зобов'яжуть забезпечити, щоб його ручні файли узгоджувалися з відповідним описом, розробленому на

центральному рівні. Якщо поліцейський підрозділ не дотримується цього загального опису, він буде зобов'язаний зробити власний опис і повідомити його наглядовому органу.

39. Можливі, звичайно, й інші шляхи поширення цих принципів на ручні файли.

40. Другий під-параграф Принципу 1.4 стосується питання тимчасових (*ad hoc*) файлів, які були заведені під час окремого розслідування.

Позначення кожного тимчасового файлу породжує неприйнятну бюрократію. Проте такі файли не повинні уникати певного виду повідомлення. Національне законодавство може передбачити обставини, за яких на них має бути звернена увага наглядового органу. Можливо, що внутрішнє право вимагатиме лише повідомлення про існування таких файлів або "загального" повідомлення тимчасових файлів певного типу, що дозволить наглядовому органові перевіряти їх, з тим щоб переконатися, що вони відповідають принципам захисту даних.

41. Як альтернатива, у разі відсутності відповідних положень у внутрішньому законодавстві наглядовий орган разом з відповідальним органом, зазначеним раніше, може виробити керівні принципи для повідомлення тимчасових файлів. Наприклад, з діалогу між наглядовим органом та відповідальною організацією з'ясовується, що такі файли повинні повідомлятися після того, як вони вже проіснували прийнятний час або, якщо можна передбачати, що проіснують протягом прийнятного часу. Буде знайдено й інші критерії для повідомлення.

42. Файли, заведенні в цілях окремого розслідування, що швидко надається, не потребують повідомлення.

Принцип 2 - Збір даних

43. Принцип 2.1 виключає необмежений, нерозбірливий збір даних поліцією. Він окреслює якісний і кількісний підхід до Статті 5(c) Конвенції про захист даних, в якій зазначається, що персональні дані мають бути адекватними, відповідними і не надмірними стосовно цілей, задля яких зберігаються. Враховуючи, що стаття 9(a) Конвенції дозволяє обмеження цього принципу з огляду на "припинення кримінальних правопорушень", Принцип 2.1 цієї Рекомендації намагається окреслити межі цих винятків, обмежуючи збирання персональних даних такою мірою, яка необхідна для запобігання реальній небезпеці або припинення певного кримінального правопорушення, якщо тільки внутрішній закон чітко не дозволяє ширші повноваження поліції у зборі інформації. Під "реальною небезпекою" слід розуміти не таку, що пов'язана з особливим кримінальним порушенням, а таку, що включає будь-які обставини, за яких виникає обґрунтована підозра, що серйозні кримінальні правопорушення скоєні чи могли б бути скоєними, до зняття непідтверджених теоретичних припущень. В якості прикладу можна навести таке: обґрунтована підозра, що невизначені наркотики повинні нелегально завезти в країни через порт на не ідентифікованій приватній яхті, виправдовуватиме збір даних про всі такі яхти, що обслуговуються цим портом, але не про всі яхти, їх власників та пасажирів, що використовують всі порти цієї країни.

44. Принцип 2.2 стосується збирання й зберігання даних без відома суб'єкта даних і намагається запропонувати регулюючий механізм на випадок, коли дані, зібрані в такий спосіб, вирішено зберегти, але якщо це не шкодитиме поліції в досягненні поставлених цілей, особу інформують про наявність даних на неї. Звичайно, ця процедура не потрібна, якщо поліція вирішила знищити дані, зібрані на особу без її відома.

Слід погодитись, що принцип 2.2 може виявитись складним для втілення, якщо йдеться про вуличні відео чи подібні засоби масового стеження, що надають інформацію про велику кількість людей. З цієї причини цей принцип рекомендує інформувати тих осіб, що підлягали негласному стеженню, про те, що дані ці ще утримуються на них "якщо доцільно". Поліція сама повинна прийняти таке рішення.

45. Сподіваємось, що держави-члени оцінять цей принцип як корисний, розглядаючи сучасний прецедент Європейської Комісії з прав людини, в якому у контексті Статті 8 Європейської Конвенції з прав людини визнано, що збирання й зберігання даних про особу без повідомлення їй про це може зачіпати питання захисту даних (звернення № 8170/78, X проти Австрії; звернення №9248/81, Лідер проти Швеції).

46. В той час, як Принцип 2.2 робить наголос на збереженні персональних даних, зібраних без відома суб'єкта даних негласними засобами чи нетаємними (наприклад, шляхом постановки питань сусідам суб'єкта даних), Принцип 2.3 зосереджує увагу на збиранні даних технічними засобами стеження або іншими автоматизованими засобами. Спеціальні положення національного законодавства повинні врегульовувати збирання даних такими методами. Так, слід пам'ятати про судові прецеденти Європейського Суду з прав людини, коли вирішується питання щодо прослуховування телефонних розмов. Рішення у справі Мелоуні показує, що така форма технічного стеження може застосовуватися санкціоновано з урахуванням доступних законних правил, які достатньою мірою визначають межі й спосіб застосування повноважень "на розсуд" покладених на органи влади, і супроводжуються адекватними гарантіями захисту від зловживання.

47. Правоохоронні органи діють у рамках встановлених законом, і їх діяльність по збиранню даних регламентується так само. Відповідно, положення внутрішнього законодавства, які повинні брати за їх мінімальну основу положення Конвенції про захист прав людини та основних свобод (1950), повинні поважатись. У зв'язку з цим варто враховувати також судові прецеденти Європейської Комісії та Європейського Суду з прав людини у питаннях арешту або утримання під арештом для допиту, обшуку та конфіскації, методів допиту, взяття проб тіла, відбитків пальців та фотографування тощо. Зрозуміло, що відповідні внутрішні законодавства повинні відповідати положенням Конвенції як вони розтлумачені Європейським Судом з прав людини.

48. Принцип 2.4 розглядає питання "вразливих" даних і відображає рекомендацію Статті 6 Конвенції із захисту даних про обмеження збирання й зберігання особливої категорії даних. Це може бути випадок, коли збирання певних "вразливих" даних необхідно в цілях, викладених у Принципі 2.1. Проте, в кожному разі збирання таких даних не повинно здійснюватися просто для того, щоб дозволити поліції скласти файл на якусь групу меншин, чиї звички чи поведінка відповідають закону. Збирання таких даних повинно здійснюватися лише з дозволу, якщо це "абсолютно необхідно в цілях конкретного розслідування". Вираз "конкретне розслідування" повинен розглядатися як загальне обмеження; таке розслідування повинно ґрунтуватися на міцній законодавчій основі, щоб переконати в тому, що серйозне кримінальне правопорушення було вчинено чи могло статись. Збирання "вразливих" даних за таких обставин, повинно бути "абсолютно необхідним" для потреб таких розслідувань.

Посилання на сексуальну поведінку [як підставу для збирання даних] не застосовується щодо вже скоєних правопорушень.

Принцип 3 - Зберігання даних

49. Персональні дані, після того як були зібрані, підлягають рішенню щодо їх зберігання в поліцейських файлах. Принцип 3.1 звертається до вимог точності і обмежень у зберіганні. Дані, що зберігаються, мають бути точними й обмеженими такою мірою, якою це необхідно, щоб забезпечити виконання поліцією її законних завдань. Принцип 3.1 визначає, що, крім національного законодавства, джерелом законної діяльності поліції, яке узаконює збирання даних, може бути міжнародне право, яке у цілях цих Рекомендації взято до уваги, щоб включити міжнародне співробітництво в межах Інтерполу (наприклад, міжнародні правові угоди про співробітництво між силами національних поліцій).

50. Цей принцип важливий з огляду на те, що звертає увагу на факт, коли включення персональних даних до поліцейського файлу може спричинитися до поліцейського запису, а нерозбірливе зберігання даних може зашкодити правам і

свободам особи. Поліція також має бути зацікавленою в тому, щоб мати в розпорядженні лише точні й надійні дані.

51. Слід відзначити, що принцип 3 в цілому є загальною вимогою, що стосується всіх типів даних, зібраних у цілях поліції, як позначалося вище.

52. Принцип 3.2 спрямований на застосування системи класифікації даних. Гадаємо, слід розрізняти підтверджені й непідтверджені дані, що включають оцінку людської поведінки, факти й погляди на них, надійну інформацію (і різні відтінки цього) і здогади; справжню причину віри в те, що інформація точна, і безпідставну віру в її точність.

53. Дані, зібрані й збереженні поліцією для адміністративних цілей (наприклад, інформація про страхування від пожежі, втрати майна тощо), також є предметом загальних принципів зберігання даних. Принцип 3.3 рекомендує, щоб такі дані зберігалися окремо від тих даних, що зібрані в цілях поліції згідно з цим документом, якщо вирішено зберігати їх необмежено. Принципово неправильно було б поширювати на них спеціальний режим поліцейських даних із запровадженням особливого підходу до захисту даних у сфері поліції.

54. Проте не завжди буває можливим забезпечити чіткий поділ даних на дві категорії. І все ж, у такому разі держави-члени повинні вивчити всі підходи, щоб уникнути змішування даних, забезпечуючи щоб адміністративні дані залишалися об'єктом загальних правил захисту даних.

Принцип 4 - Використання даних поліцією

55. Принцип 4 формулює заключне положення: персональні дані, зібрані з метою запобігання й припинення кримінальних правопорушень, або для підтримання громадського порядку ("поліцейські цілі"), повинні використовуватись лише в цих цілях. Проте, абсолютний характер цього правила визначається частково Принципом 5.

Принцип 5 - Повідомлення даних

56. Принцип 5 побудовано так, що б врегульовувати різні форми передачі даних, що може на законних підставах мати місце, а також забезпечувати принципи, що торкаються всіх передбачуваних передач.

57. Передача даних у поліцейській сфері обумовлюється наявністю у поліцейського органу, який одержує дані, правомірного інтересу на це, наприклад, як необхідна одержувачу для запобігання чи боротьби з кримінальними правопорушеннями або підтримання громадського порядку. Встановлюється, що поліцейський підрозділ, що запитує інформацію в іншого поліцейського підрозділу, може повідомити певні дані щоб його запит про інформацію було виконано, причому обидві сторони повинні виконувати вимогу щодо законного інтересу, викладену в Принципі 5.1.

58. При передачі за межі поліцейського сектору умови, що визначають передачу, більш суворі: оскільки комунікація може бути і не в цілях поліції у прямому розумінні. Наголошується винятковий характер обставин, викладених у Принципах 5.2 та 5.3, за яких дозволяється передавати дані. Буде визначено, що обставини (а) та (б) у Принципах 5.2 (ii) та 5.3 (ii) спеціально позначаються як "виняткові".

59. Публічними установами, яких стосується Принцип 5.2, можуть бути, наприклад, органи соціального забезпечення, органи внутрішньої перевірки за сплатою річних податків, імміграційного контролю, органи митної служби тощо.

60. Загальні умови передачі даних таким органам, визначені Принципом 5.2 (i), під-параграфи (а) та (б). Зазначимо, що Принцип 5.2. (i.a) розглядає можливість наглядового органу санкціонувати передачу даних. Пам'ятаючи про цю функцію, підкреслену в Принципі 1, наголошуємо на необхідності незалежності наглядового органу від поліцейського сектору.

“Чітке законне санкціонування”, про яке йдеться в Принципі 5.2 (i.a) може забезпечуватися магістратом (1) мировим суддею; 2) членом магістрату в Англії; 3) посадовою особою).

61. Взаємодопомога між органами поліції і публічними установами, зазначеними вище, також можлива за відсутності обставин, викладених у Принципі 5.2 (i.a). Принцип 5.2 (i.б) дозволятиме, наприклад, органам соціального захисту, що розслідують порушення у секторі соціального захисту, мати доступ о відповідних поліцейських даних, якщо дані є суттєвими для його розслідування. Визнано, що публічні установи, про які йшлося у параграфі 59, займаються діяльністю, подібною якимось чином до поліцейської, а тому інформація, утримувана поліцією, може бути корисною для їх діяльності. Поняття сумісності, згадуване в Принципі 5.2.(i.б), відображає Статтю 5(б) Конвенції про захист даних. Отже, дані можуть передаватися для спорідненої діяльності. “Законні обов’язки” поліції слід трактувати відповідно до внутрішнього законодавства.

62. Принцип 5.2.(ii) викладає дві додаткові обставини, що виправдовують повідомлення; нагадаємо, що дозволятимуть вони повідомлення лише як “виняткове”. Для ілюстрації положення наведемо приклад, коли установа з соціального захисту, зіткнувшись з вимогою мігранта про пільги, повинна перевірити легальний статус останнього в цій країні, звернувшись до поліцейського файлу. Це буде і на користь заявника. Зазначимо, що небезпека, про яку йдеться в (б), повинна буди серйозною і вже навислою. Було вирішено кваліфікувати небезпеку в такий спосіб, як і в Принципі 5.2 (ii), якщо стосується лише виняткових випадків допущення комунікації. Якщо ж існує серйозна, але не термінова загроза, то комунікація має здійснюватися згідно з положеннями Принципу 5.2 (ii.a).

63. Інколи для поліції буває необхідним передати дані приватним організаціям, хоча й не того рівня, що розглядається у випадку взаємодопомоги між органами поліції та іншими публічними установами. Інколи поліція робить доступними конфіденційні дані про відомих шахраїв, що обкрадають крамниці та банки, чи інформації про викрадені кредитні картки та чеки. Знов-таки, Принцип 5.3 розглядає їх як виняткові випадки, вимагаючи чітких правових зобов’язань чи санкцій (наприклад, згоди члена магістрату) або згоди наглядового органу. За відсутності цих факторів Принцип 5.3 повторює ці ж умови, що викладені в Принципі 5.2 (ii).

64. Слід мати на увазі, що положення Принципі 5.2 та 5.3 стосуються поширення чи повідомлення через радіомовлення публічним установам чи приватним особам ідентифікуючих знімків чи фотографій підозрюваних осіб, що отримані з автоматизованих обробок даних.

65. Принцип 5.4 торкається міжнародної передачі поліцейських даних у суворому розумінні між органами поліції. Звернення до міжнародного права передбачає не лише міжнародні угоди про взаємодопомогу в кримінальних справах, але й співробітництво в межах Інтерполу. Крім того, цей принцип враховує наявність (або намір) угод між сусідніми державами, підписаний з метою поліпшення транскордонної передачі даних між поліцейськими відділами.

66. Стосовно терміну “поліцейські органи”, погоджено, що у деяких державах-членах певні види поліцейської роботи можуть виконуватися організаціями, які не є в суворому розумінні “поліцейськими органами”. Отже, може бути прецедент, що певні функції, які мисляться як такі, що є в компетенції поліції, в окремих державах-членах можуть бути фактично перекладені на неполіцейські установи в інших державах-членах.

67. В цілях Принципу 5.4, таким чином, термін “поліцейські органи” слід розуміти в широкому смислі. Питання повинно ставитись лише таким чином: орган виконує функцію, пов’язану з припиненням кримінальних правопорушень чи досягненням громадського порядку. Нарешті, Принцип 5.4 не слід витлумачувати як такий, що виключає можливість передачі даних іноземним юридичним органам де такі органи

виконують функції, пов'язані із запобіганням і припиненням кримінальних правопорушень. Зрозуміло, що вимоги, викладені в Принципі 5.4 мають поважатись.

68. Міжнародний обмін персональними даними між поліцейськими установами повинен відбуватися лише за умов, викладених або в (а) чи (б). Принцип 5.4 буде корисним, якщо держава-одержувач не є членом Інтерполу, або якщо договір, що санкціонує передачу даних реципієнту, не існує.

69. Текст Принципу 5.4 відображає до певної міри положення Статті 12 Конвенції про захист даних, яка розглядає питання транскордонних потоків даних. Зауважимо, що речення "і передбачає, щоб внутрішні закони захисту особи не порушувались" доповнює концепцію "еквівалентного захисту" в державі-реципієнті в параграфі 3, а Статті 12. Отже, орган, що надсилає, сам повинен задовольняти рівень захисту даних для поліції, що існує в державі, яка одержує. При вирішенні питання, чи повинен направляючий орган ставити умови щодо використання даних в отримуючій державі (наприклад, тривалість бесіди), слід розуміти, що ці умови слід поважати. Обидва Принципи 5.4 (а) та (б) підпадають під застереження.

70. Принцип 5.5 зв'язує низку правил, що врегульовують різні форми повідомлення даних, про які йшлося вище.

Звертаючись до правил, які регулюють передачу даних, розробники керувалися певною мірою положеннями, викладеними в "Правилах про співробітництво поліції та внутрішній контроль за архівами Інтерполу". Крім них відображено положення "Європейської Конвенції про взаємодопомогу у кримінальних справах" від 20 квітня 1959 року.

71. Критерії, сформульовані в Принципі 5.5, спрямовані на забезпечення того, щоб повідомлення даних здійснювалося на законних підставах. Нагадаємо, що Принцип 5.1 зобов'язує орган поліції, що просить дані у іншого органу поліції в межах поліцейського сектору, мати законні підстави для отримання цих даних. Проте, Принцип 5.5 (і) розглядає як внутрішній так і зовнішній обмін даними, що стали предметом правомірних вимог.

72. Встановлюється, що внутрішнє право чи положення міжнародних угод можуть вирішувати питання про виправданість запиту.

73. Принцип 5.5 (іі) не абсолютний за своєю природою. Умови, сформульовані в ньому - "наскільки це можливо" мають задовольнятись. Наприклад, відомо, що в деяких країнах судові рішення не завжди надсилаються до поліції.

74. Як зазначалося раніше, і в інтересах поліції, і в інтересах особистості дані повинні бути точними.

75. Принцип 5.5 (іі) зважає також на те, що в різних країнах існують різні періоди моніторингу. З цієї причини здійснення перевірки якості даних дозволяється до моменту їх передачі.

76. Принцип 5.5 (ііі) дозволяє використання даних винятково в цілях, що відрізняються від цілей доведення правомірності першого запиту про повідомлення. Важливо, щоб повідомляючий орган було поінформовано про наміри щодо використання даних. Слід пам'ятати, що різні цілі повинні стосуватися одного чи більше факторів, що розглядаються в Принципах 5.2 - 5.4.

77. Принципи 5.5 (іі) не застосовуються до передачі в середині поліцейського сектору. Правила, викладені в Принципах 4.1 та 5.1, застосовуються в такому випадку.

78. В той час, коли Принцип 2 формулює загальне положення про збирання даних поліцією, Принцип 5.6 торкається особливої ситуації, коли поліція в пошуках інформації може підключати свої файли до файлів, що утримуються для відмінних цілей, наприклад, органів соціального захисту, списки пасажирів, що зберігаються авіалініями, файли членства в профспілках тощо. Отже, може вестись пошук таких файлів, які б надавали чіткий опис типу правопорушення або осіб, які, можливо, причетні до такого правопорушення.

79. Легітимність такої практики залежить від гарантованості підстави санкції, зазначеної в (а) чи (б). “Чіткі правові забезпечення”, на які є посилання в Принципі 5.6 (б), повинні зазначити умови, за яких може відбутися підключення (поєднання) файлів.

80. Можливість поліції, що має прямий комп’ютеризований й доступ до файлів, що робиться різними органами поліції чи іншими органами, обговорюється в заключному під-параграфі Принципу 5.6. Прямий доступ за таких обставин повинен узгоджуватися з внутрішнім законодавством, яке має відображати відповідно основі принципи цієї Рекомендації.

Принцип 6 — Прозорість, право доступу до поліцейських даних, право на виправлення і право на апеляцію

81. Вимога прозорості для існуючих поліцейських файлів з огляду на права осіб стосовно поліцейських файлів є особливо важливою. Принцип 6.1 покладає завдання з прозорості на наглядовий орган, хоча держави-члени, без сумніву, знайдуть додаткові шляхи втілення цієї вимоги.

82. Вимога прозорості повинна стосуватися в принципі всіх автоматизованих файлів. Проте зрозуміло, що обсяг інформації, що може бути надана для поліцейських файлів, буде залежати від особливих обставин.

Наприклад, більш загальний опис слід надавати *ad hoc* файлу, що стосується делікатного розслідування, яке проводиться.

83. Особа в першу чергу повинна мати право направляти звернення про доступ до поліцейського файлу контролерові цього файлу. Це право принаймні повинно задовольнятися через посередницький чи наглядовий орган. Внутрішнє законодавство повинне вживати відповідні заходи, щоб існувало таке право. Крім того, Принцип 6.2 гарантує доступ суб’єкта даних у розумних проміжках часу і без невиправданої затримки.

84. В принципі звернення про доступ до даних не повинно реєструватися, оскільки це може обмежувати реалізацію права. Проте, якщо держава-член має систему реєстрації, слід потурбуватися, щоб реєстрація утримувалася окремо від кримінальних файлів, утримуваних поліцією. Слід також подумати про знищення реєстру через розумний проміжок часу.

85. У зв’язку з тим, що дані виявляються не точними в результаті застосування права доступу або вважаються неточними, невідповідними чи надмірними в наслідок застосування інших принципів, Принцип 6.3 передбачає, що поліція дбатиме про приведення відповідного файлу в належний порядок. Це може бути зроблено через знищення неточних даних чи виправлення інформації, щоб вона відповідала істинній ситуації. Альтернативою стиранню, як це передбачено Принципом 6.3, є зберігання даних у файлі, але з поміткою про їх дійсний стан. Це може стосуватися заяв, зроблених свідками, які виявились неточними. Доцільніше буде не усувати таку заяву з файлу, а залишити її, додавши правильну версію подій.

86. Другий під-параграф принципу 6.3 викладає графік знищення чи виправлення даних. Зауважимо, що ці заходи застереження стосуються не самого файлу, а повинні застосовуватися до кожного документу, залученого до файлу.

87. Досвід принаймні в одній державі-члені показав, що в принципі можливий санкціонований доступ у переважній більшості випадків. Принцип 6.4 визначає, що у праві доступу (а отже й праві на виправлення та знищення) може бути й відмовлено у викладених випадках.

88. Відзначимо, що обмеження в інтересах суб’єкта даних прав і свобод інших було взято зі Статті 9, під-параграф 2(б) Конвенції про захист даних. У контексті поліцейського сектору це формулювання повинно поширюватися на потребу захисту свідчень чи поліцейських інформаторів.

89. Альтернативне виправдання обмеженого доступу - “обов’язкового для виконання законного завдання поліцією” - не має чіткого відбиття у Статті 9 зазначеної Конвенції. Проте є переконання, що в контексті обмежень права на доступ, застереження Конвенції для “припинення кримінальних правопорушень” є кращим формулюванням.

90. Особа може мати необхідність в отриманні копії її поліцейського файлу, наприклад, у зв’язку з наймом на роботу. Причому, не в її інтересах буде отримання письмової копії чи констатації про те, що міститься у файлі. В такому разі внутрішнє законодавство може санкціонувати усну передачу змісту файлу.

91. Принципи 6.5 та 6.6 формулює певні процедурні гарантії у випадку відмови чи обмеження права доступу, виправлення чи знищення. По-перше, відмова чи обмеження вмотивовуються письмово. Важливо показати, що обов’язок покладений на поліцію принципом 6.4 підпорядковувати права суб’єкта даних вищим інтересам, викладеним тут, виконується.

92. Буде зауважено, що зазначення причин може не вимагатися лише з тих же причин, що виправдовують відмову чи обмеження прав доступу, виправлення чи стирання. Об’єкт даних інформується про його право на апеляцію у зв’язку з відмовою в доступі. Це право має формулюватися у вигляді обґрунтованого рішення, передбаченого положенням 6.5. Якщо причини відмови не зазначаються, бо поліція переслідує вищі інтереси, однак особі повідомляють, як вона може оскаржити це рішення.

93. Принцип 6.6 розроблено з урахуванням практики різних держав-членів у наданні права доступу. У деяких країнах можуть трапитися випадки, коли особа не матиме прямого права доступу до файлу поліції і буде зобов’язана домагатися доступу через вищій наглядовий орган.

94. Згадуваний “інший незалежний орган” означає, що в деяких країнах суд чи трибунал може розглядати апеляції, а не вищій наглядовий орган. Але незалежно від цього суб’єкт даних користуватиметься правом звернутися до суду чи трибуналу, щоб домогтися виправлення, доповнення файлу тощо, якщо йому у цьому було відмовлено.

95. Внутрішнє законодавство визначає посередницькі органи чи наглядовий орган для перевірки поліцейського файлу, з приводу якого виникла суперечка. Може статися, що наглядовий орган не буде зобов’язаний повідомляти дані особі, якщо навіть і не має підстав для відмови у доступі. Суб’єктові даних просто повідомляють, що перевірку поліцейського файлу зроблено і що файл - в порядку. В іншому разі, контролюючий орган може прийняти рішення про повідомлення даних, що містяться у файлі, суб’єкту даних.

Принцип 7 — Тривалість зберігання і поновлення даних

96. Важливо, щоб робилися періодичні перегляди поліцейських файлів з тим, щоб вилучити з них зайву чи неточну інформацію, а також поновити її. Принцип 7.1 перераховує чинники, які слід мати на увазі, коли вирішується питання, чи продовжене зберігання даних залишатиметься необхідними для запобігання чи припинення злочину або підтримання громадського порядку.

97. Принцип 7.2 містить побажання, щоб якість даних перевірялась регулярно відповідно до встановлених правил, і щоб вони консервувалися також на підставі, визначеній правилами. Застосування цього принципу поліпшить виконання завдань, покладених на поліцію Принципом 5.5, під-параграф (ii).

98. Внутрішнє право може санкціонувати заходи по виробленню таких правил. В іншому разі, правила ці могли б формулюватися самім наглядовим органом в консультаціях з поліцією. Якщо поліція сама виробляє правила, вона повинна консультуватися з наглядовим органом стосовно їх змісту та застосування.

99. Зрозуміло, що поліцейські дані становлять цінність з точки зору дослідницьких та статистичних даних. Внутрішнє законодавство про архіви забезпечує шляхи вирішення всіх проблем, які виникають у цьому зв’язку. Якщо необхідно, мають робитися посилання на положення Рекомендації №R(83)10 про захист персональних даних, використовуваних у наукових та статистичних цілях.

Принцип 8 - Захист даних

100. Принцип 8 відображає вимоги фізичної безпеки та конфіденційності. Відповідальний орган, зазначений вище, повинен дбати, щоб лише уповноважений персонал мав доступ до терміналів і щоб повідомлення даних виконувалося відповідно до вимог, які, за Принципом 5, є законними. З цією метою відповідальний орган міг би завести журнал, в якому записувалась би інформація, що розглядається в принципі 5.5 (i).

Зноски

1. Коли ця Рекомендація приймалася: згідно зі Статтею 10(c) Правил процедури зустрічі заступників міністрів, представник Ірландії зберіг право його уряду погоджуватися чи не погоджуватися з цією Рекомендацією; представник Об'єднаного Королівства зберіг право його уряду погоджуватися чи не погоджуватися з Принципами 2.2 та 2.4 цієї Рекомендації; представник Федеративної Республіки Німеччина зарезервував право його уряду погоджуватися чи не погоджуватися з Принципом 2.1 цієї Рекомендації; згідно зі Статтею 10.2 (d) зазначених Правил процедури, представник Швейцарії утримався, наголошуючи, що він зберіг право його уряду погоджуватися чи ні і підкреслив, що його утримання не слід розглядати як вираження незгоди з цією Рекомендацією в цілому.

У своєму листі від 10 грудня 1997 року Ірландський уряд повідомив Секретаріат про своє рішення обмежити резервування, зроблене під час прийняття Рекомендації трьома положеннями – Принципами 2.2, 2.3 та 2.4.