ВІД РЕДАКЦІЙНОЇ КОЛЕГІЇ

неофіційний переклад

ВИСНОВКИ
ЄВРОПЕЙСЬКОГО НАГЛЯДАЧА ІЗ ЗАХИСТУ ДАНИХ

від 26.09.2005 р.
щодо проекту Директиви Європейського Парламенту і Ради

“ПРО ЗАТРИМАННЯ ДАНИХ, ЩО ОБРОБЛЯЮТЬСЯ У ЗВ’ЯЗКУ З НАДАННЯМ ПУБЛІЧНИХ ЕЛЕКТРОННИХ КОМУНІКАЦІЙНИХ ПОСЛУГ, І ВНЕСЕННЯ ЗМІН ДО ДИРЕКТИВИ 2002/58/ЄС*”

Європейський наглядач із захисту даних –

Беручи до уваги Договір про Європейський Союз (ЄС), і, зокрема, його статтю 286,

Беручи до уваги Хартію основоположних прав Європейського Союзу, і, зокрема, його статтю 8,

Беручи до уваги Директиву 95/46/ЄС Європейського Парламенту і Ради від 24.10.1995 р. “Про захист осіб у зв'язку із обробкою персональних даних і вільним обігом цих даних”[1] та Директиву 2002/58/ЄС Європейського Парламенту і Ради від 12.07.2002 р. “Про обробку персональних даних та захист таємниці у секторі телекомунікацій”[2],

Беручи до уваги Постанову № 45/2001 Європейського Парламенту і Ради від 18.12.2000 р. “Про захист осіб у зв'язку із обробкою персональних даних установами і органами Спільноти щодо вільного руху таких даних”[3], і. зокрема, її статтю 41,

Беручи до уваги запит про Висновок відповідно до статті 28(2) Постанови ЄС № 45/2001, одержаний від Комісії 23.09.2005 р.,

Надав цей Висновок:

I. Вступ

1. Комісар ЄС із захисту даних (далі – КЄСЗД) вітає той факт, що з ним консультуються на підставі статті 28(2) Постанови (ЄС) № 45/2001. Зважаючи на обов'язковий зміст статті 28(2) Постанови (ЄС) № 45/2001, цей Висновок повинен бути згаданий в преамбулі Директиви.

2. КЄСЗД визнає важливість для правоохоронних органів мати у своєму розпорядженні всі необхідні юридичні інструменти, зокрема, для боротьби із тероризмом та іншими серйозними злочинами. Доступність даних трафіку і місцезнаходження публічних електронних послуг є ключовим інструментом у діяльності правоохоронних органів і може сприяти безпеці людей. Проте, це не передбачає необхідності у нових інструментах, згаданих у цьому Проекті.

3. Якщо розглядати Проект лише винятково з перспективи захисту даних, то дані трафіка і місцезнаходження не повинні взагалі затримуватися для правоохоронної цілі. Саме з цих причин Директива 2002/58/ЄС встановлює принцип, що дані трафіка повинні бути стерті відразу, як тільки їх зберігання більше не потрібне для цілей, безпосередньо пов'язаних з комунікацією (в тому числі з метою складання рахунків). Винятки мають ґрунтуватися на жорстких підставах.

4. У цьому Висновку КЄСЗД висвітлює вплив Проекту на захист персональних даних. До цього, слід звернути увагу на те, що неврахування важливості Проекту для правоохоронної діяльності матиме своїм наслідком позбавлення осіб права мати захист їх приватності.

5. Цей Висновок КЄСЗД повинен розглядатися у світлі зазначених у ньому зауважень. КЄСЗД віддає перевагу збалансованому підходу, в якому необхідність і пропорційність втручання в захист даних відграють основну роль.

6. Проект повинен розглядатися як реакція на ініціативу Французької Республіки, Ірландії, Королівства Швеція і Об'єднаного Королівства щодо проекту Рамкового Рішення про за-

---

* *Від редакції*. Щодо Директиви 2002/58/ЄС див. “Правова інформатика” № 2 (18)/2008.

тримання даних, що обробляються і зберігаються у зв’язку з наданням публічно доступних електронних комунікаційних послуг або даних публічних комунікаційних мереж з метою запобігання, розслідування, виявлення і переслідування злочинів і проступків, включаючи тероризм.

II. Загальні спостереження

Вплив Проекту на захист персональних даних

7. Для КЄСЗД є суттєвим, щоб Проект дотримувався основоположних прав. Законодавчий захід, який би шкодив захисту, гарантованому правом Спільноти, а також, зокрема, прецедентним правом Суду справедливості і Європейського суду з прав людини, є не тільки неприйнятним, але й незаконним. Обставини в суспільстві, можливо, змінилися внаслідок терористичних нападів, однак ці зміни не можуть мати наслідком те, щоб високі стандарти захисту в правовій державі були поставлені під загрозу. Захист надається згідно із законом незалежно від фактичних потреб правоохоронців. Більше того, якщо це необхідно в демократичному суспільстві, то прецедентне право безпосередньо дозволяє винятки.

9. Проект має прямий вплив на захист, наданий статтею 8 Європейської Конвенції “Про захист прав людини та основоположних свобод” (далі – ЄКПЛ). Згідно із прецедентним правом Європейського суду з прав людини:

- зберігання інформації про особу розглядалося як втручання у приватне життя, хоча б вона не містила ніяких вразливих даних (Amann[4]);
- таке ж правило застосовується до практики “фіксування” телефонних розмов, завдяки автоматичній реєстрації набраних номерів, часу та тривалості кожної розмови (Malone[5]);
- обґрунтування втручання повинно переважити шкідливий вплив, який саме існування юридичних приписів з цього питання може мати для суб'єктів (Dudgeon[6]).

10. Стаття 6(2) Договору про ЄС передбачає, що Союз повинен поважати основоположні права, гарантовані ЄКПЛ. У попередньому параграфі було показано, що згідно із прецедентним правом Європейського суду з прав людини зобов'язання затримувати дані входить у сферу статті 8 ЄКПЛ. Повинно бути продемонстровано, повною мірою, необхідність і пропорційність зобов'язання затримувати дані.

11. Проект має величезний вплив на принципи захисту даних, визнані правом Спільноти:

- дані можуть затримувати на період довший, аніж періоди, які звичайно використовувались для такого затримання постачальниками публічно доступних електронних комунікаційних послуг або публічною комунікаційною мережею (надалі згадуються як “постачальники”);
- згідно із Директивою 2002/58/ЄС, зокрема статтею 6, дані можуть збиратися і зберігатися з причин, безпосередньо пов'язаних з самою комунікацією, включаючи, зокрема, ціль складання рахунків[7]. Згодом, дані повинні бути стерті. Згідно із цим Проектом затримання з метою застосування кримінального права є обов'язковим;
- запровадження збирання та затримування даних, як це передбачається Проектом, матиме своїм наслідком створення значних баз даних, зокрема завдяки “рибалки даних” (“fishing operations”) у комерційних цілях, що несе особливі ризики для суб’єкта даних;
- Директива 2002/58/ЄС гарантує безпеку і конфіденційність. Цей Проект не може розглядатися з точки зору виключень у цій сфері; потрібні жорсткі гарантії безпеки, а обмеження прав слід висвітлити.

12. І нарешті, як захист приватного життя, так і захист персональних даних визнаються в Хартії про основоположні права, як це було згадано в Пояснювальному меморандумі.

13. Вплив Проекту на захист персональних даних потребує повного аналізу. У цьому аналізі КЄСЗД врахує викладені вище елементи і робить висновок про те, чи потрібна більшість заходів. Простого посилання на чинну правову основу про захист даних (зокрема, Директиву 95/46/ЄС і 2002/58/ЄС) недостатньо.

Необхідність затримання даних трафіку і місцезнаходження

14. КЄСЗД нагадує висновок Робочої групи із захисту даних від 9 листопада 2004 року щодо статті 29 Проекту Рамкового Рішення. Робоча група стверджувала, що обов’язкове затримання даних трафіка згідно із умовами, передбаченими у Проекті Рамкового Рішення, є не-

прийнятним. Цей висновок, окрім іншого, заснований на неможливості надати будь-який доказ щодо необхідності затримання в цілях суспільного порядку, було зроблено завдяки результатам дослідження, які показали, що найбільша кількість даних трафіка не старша шести місяців.

15. На думку КЄСЗД, зауваження Робочої групи із захисту даних щодо статті 29, згадані вище, повинні бути вихідним пунктом для оцінки цього Проекту. Проте, результат цих зауважень не можна механічно перенести на цей Проект. Слід взяти до уваги, що обставини можуть змінюватися. На думку КЄСЗД, для оцінки можуть бути доречними такі обставини.

16. По-перше, було запропоновано деякі ілюстрації для того, щоб продемонструвати, що на практиці правоохоронцям потрібні дані трафіка строком не менш як до одного року. Комісія так само як і Президія Ради відзначила важливість дослідження поліції Об'єднаного Королівства[8], яке свідчить, що, хоча 85 % даних трафіка, потрібних поліції, зібрали менше ніж за шість місяців, однак дані від шести місяців до року використовувалися у складних розслідуваннях серйозніших злочинів. Також були представлені деякі приклади справ. Період затримання в Проекті (один рік для телефонних даних) відображає ці методи правоохоронців.

17. КЄСЗД не переконаний, що ці ілюстрації надають докази необхідності затримання даних трафіка строком до одного року. Той факт, що в деяких випадках доступність даних трафіка і/або місцезнаходження допомогла розкрити злочини, не означає, що ці дані потрібні (взагалі) як інструмент для правоохоронців. Проте, цими ілюстраціями не можна нехтувати. Вони представляють, принаймні, серйозну спробу продемонструвати потребу затримання. Окрім того, ілюстрації прозоро вказують на те, що період затримання більше ніж один рік не потрібен з перспективи поточних методів правоохоронної діяльності.

По-друге, чинні можливості постачальників, згідно із Директивою 2002/58/ЕС, затримувати дані трафіка для цілей складання рахунків не завжди використовуються, оскільки у низці випадків, число яких зростає, затримання даних з метою складання рахунків взагалі не має місця (наперед оплачені картки мобільного зв'язку, передплата за єдиною ставкою тощо). У цих випадках, які на практиці зустрічаються все частіше, дані трафіку і місцезнаходження не зберігатимуться взагалі, а будуть видалені відразу після комунікації. Те ж саме стосується невдалих викликів. Це може впливати на ефективність правоохоронної діяльності.

19. Окрім того, такий розвиток телекомунікаційних послуг може призвести до порушень у функціонуванні внутрішнього ринку, серед іншого, завдяки прийняттю (загрозі прийняття) законодавчих заходів в державах-членах згідно зі статтею 15 Директиви 2002/58/ЄС. Наприклад, італійський уряд нещодавно видав декрет, який зобов'язує постачальників зберігати телефонні дані протягом чотирьох років. Це зобов'язання призводитиме до значних витрат.

20. По-третє, робочі методи правоохоронних органів також зазнали розвитку – розслідування із випередженням використання технічної підтримки стали важливішими. Ці обставини вимагають, щоб органи влади розпоряджалися адекватно і точно сформульованими інструментами для того, щоб дозволити їм виконувати свою роботу з належним ставленням до принципів захисту даних. Один із таких інструментів, яким органи влади звично розпоряджаються, – це консервація даних, або заморожування комунікаційних даних на запит у конкретному розслідуванні. Стверджувалося, що цього інструмента, який сам по собі має менший вплив на ці принципи, аніж інструмент, який пропонується (затримання даних), може не завжди бути достатньо, зокрема, він не дозволяє відслідковувати осіб, причетних до тероризму або іншого серйозного злочину, які раніше не підозрювалися в злочинній діяльності. Проте, для того, щоб визначити, чи насправді такий випадок має місце, потрібно більше доказів.

21. По-четверте, занепокоєння терористичними нападами зростає. КЄСЗД поділяє погляд, виражений у контексті пропозицій про затримання даних, що фізична безпека має, сама собою, першорядну важливість. Суспільство потребує захисту. Для цього уряди зобов'язані продемонструвати, що вони приділяють значну увагу цій потребі, і провести дослідження, а якщо їм доведеться реагувати, то й запровадити нові законодавчі заходи. Йдеться про те, що КЄСЗД повністю підтримує завдання урядів як на національному, так і на європейському рівні – захистити суспільство і продемонструвати, що вони роблять все для захисту даних, в тому числі через прийняття нових, законних і ефективних заходів внаслідок наукових досліджень.

22. КЄСЗД визнає зміни обставин, але поки що не переконаний у необхідності затримання даних трафіку і місцезнаходження в правоохоронних цілях, як це стверджується у Проекті. Він наголошує на важливості принципу права, встановленого Директивою 2002/58/ЄС, який вказує, що дані трафіка повинні бути стерті відразу, як тільки їх зберігання не потрібне більше для цілей, які безпосередньо пов'язані з комунікацією. До того ж, надані ілюстрації не доводять ані те, що чинна правова структура не пропонує інструментів, потрібних для захисту фізичної безпеки, ані те, що держави-члени повністю застосовують свою компетенцію згідно із європейським правом щодо співпраці, наданої їм у межах чинної правової структури.

23. Проте, якщо Європейський Парламент і Рада після обережного зважування інтересів зроблять висновок, що необхідність затримання даних трафіку і місцезнаходження продемонстрована достатньою мірою, КЄСЗД притримуватиметься точки зору, за якою затримка може бути виправдана згідно із правом Спільноти тільки тією мірою, якою дотримується принцип пропорційності і гарантовані адекватні заходи безпеки у відповідності до цього Висновку.

Пропорційність

24. Пропорційність запропонованого нового законодавчого заходу безпосередньо залежить від відповіді на питання: чи є він адекватним потребам суспільства?

25. Перше зауваження стосується питання: чи можна очікувати, що Проект збільшить фізичну безпеку мешканців ЄС? Одна з причин сумніватися в адекватності цього, часто згадувана в публічних дебатах, – це те, що дані трафіка та місцезнаходження не завжди пов'язуються із конкретною особою – знання про телефонний номер (або IP-адресу) не обов'язково ідентифікують особу. Більш серйозна причина для сумніву полягає в тому – чи існування величезних баз даних полегшує правоохоронцям пошук, який їм потрібно провести у конкретній справі?

26. КЄСЗД вважає, що затримка даних трафіка і місцезнаходження за своєю природою не є адекватною чи ефективною відповіддю. Потрібні додаткові заходи для того, щоб гарантувати, що органи влади мають ціль і швидкий доступ до даних, потрібних у певній справі. Затримання даних є адекватним і ефективним тільки в тому разі, коли існує ефективний механізм пошуку.

27. Друге зауваження стосується наявності пропорційності прав суб’єктів у відповіді. Для того, щоб це мало місце, Проект повинен:

- обмежувати періоди затримання. Ці періоди повинні відображати продемонстровані потреби правоохоронної діяльності;
- обмежувати кількість даних, що зберігаються. Ця кількість повинна відображати продемонстровані потреби правоохоронної діяльності та гарантувати неможливість несанкціонованого доступу до даних;
- містити адекватні заходи безпеки, так щоб обмежити доступ і подальше використання, гарантувати безпеку даних і забезпечити, що самі суб'єкти даних могли використати свої права.

28. КЄСЗД наголошує на важливості цих суворих обмежень з адекватними заходами безпеки. У перспективі важливості трьох елементів, згаданих у викладеному вище пункті, держави-члени можуть не вживати додаткових заходів на національному рівні, які ставлять під сумнів пропорційність. Ця потреба в гармонізації буде детальніше висвітлена у Розділі IV.

Адекватні заходи безпеки

29. Наслідком Проекту буде те, що постачальники розпоряджатимуться базами даних, у яких буде зберігатися значна кількість даних трафіка і місцезнаходження.

30. По-перше, Проект має гарантувати, що доступ до даних і подальше їх використання буде обмеженим: тільки згідно із спеціально вказаними обставинами і для обмеженого переліку спеціально вказаних цілей.

31. По-друге, бази даних треба адекватно захищати. Для досягнення цієї мети повинно бути гарантовано, що після закінчення періодів затримання дані будуть ефективно видалені. Не повинно бути ніякого “зливу” даних або несанкціонованої експлуатації даних. Коротше кажучи, вимагається високий рівень захисту даних і адекватні технічні і організаційні заходи безпеки.

32. Високий рівень безпеки даних є навіть важливішим, оскільки просте існування даних може призвести до запитів на доступ і користування ними як мінімум трьох груп користувачів:

- самі постачальники. Вони можуть спокуситися використати дані для своїх власних комерційних цілей. Необхідні гарантії для запобігання копіювання цих файлів;

- органи влади, відповідальні за правоохоронну діяльність: Проект пропонує їм право мати доступ, але тільки у спеціально визначених випадках і згідно із національним законодавством (стаття 3(2) Проекту). Не повинно бути доступу з метою “копання” чи “виловлювання“ (“fishing operations”) даних. Обмін даних з органами влади в інших державах-членах має бути врегульовано прозоро;

- розвідувальні служби (які уповноважені гарантувати національну безпеку).

33. Щодо доступу розвідувальних служб КЄСЗД відзначає, що згідно зі статтею 33 Договору про ЄС і статті 64 Договору про ЄС втручання в межах Третьої і Першої опори не повинно впливати на здійснення повноважень, доручених державами-членами щодо підтримки правопорядку і гарантування національної безпеки. На думку КЄСЗД, наслідком цих положень є недостатня компетенція ЄС керувати доступом сил безпеки або розвідувальних служб до даних, затриманих постачальниками. Іншими словами, ані доступ цих служб до даних трафіку і місцезнаходження, що знаходяться у постачальників, ані подальше використання інформації, набутої цими службами, не регулюється правом ЄС. Саме держави-члени повинні вжити необхідних заходів для того, щоб врегулювати доступ розвідувальних служб.

34. По-третє, наслідки, описані в попередніх параграфах, мають потенційний вплив на суб'єкта даних. Додаткові заходи безпеки є потрібними для того, щоб гарантувати, що він як суб'єкт даних може просто і швидко скористатися своїми правами. КЄСЗД указує на потребу ефективного контролю щодо доступу і подальшого користування, бажано з боку судових органів держав-членів. Ці заходи безпеки повинні також застосовуватися у випадку доступу і подальшого користування даними трафіку з боку органів влади в інших державах-членах.

35. У цьому контексті КЄСЗД посилається на ініціативи нової правової структури щодо захисту даних, застосовної до правоохоронної діяльності (у Третій опорі Договору про ЄС). На його думку, така правова структура вимагає додаткових заходів безпеки і не може обмежуватися лише повторним підтвердженням загальних принципів захисту даних у Першій опорі[9].

36. По-четверте, існує пряма залежність між адекватністю заходів безпеки і витратами на ці заходи. Саме тому адекватний закон про затримання даних повинен містити стимули для постачальників інвестувати у технічну інфраструктуру. Такий стимул міг би полягати у тому, що постачальникам компенсуються додаткові витрати на адекватні заходи безпеки.

37. Підсумовуючи, адекватні заходи безпеки повинні:

- обмежити доступ до даних і їх подальше використання;

- надати адекватні технічні і організаційні заходи безпеки для захисту баз даних. Це включає в себе видалення даних в кінці періоду затримання і визнання запитів на доступ і користування різними групами клієнтів;

- гарантувати суб'єктам даних користування їх правами, а не тільки підтвердити загальні принципи захисту даних;

- містити стимули постачальникам інвестувати в технічну інфраструктуру.

III. Правова основа і проект рамкового рішення

38. Проект заснований на Договорі про ЄС, зокрема статті 95, а мета згідно зі статтею 1 Проекту передбачає гармонізацію зобов’язань постачальників щодо обробки і затримання даних трафіку. Стверджується, що ці дані повинні надаватися тільки уповноваженим національним органам влади в окремих справах, пов'язаних із кримінальними правопорушеннями, але потребує врегулювання, точніше, визначення мети так само, як і доступ і подальше використання даних за розсудом держав-членів з урахуванням заходів безпеки в Спільноті.

39. У цьому Проект більш обмежений, аніж Проект Рамкового Рішення, який базується на статті 31(1)(c) Договору про ЄС і містить додаткові положення про доступ до даних, так само, як і про запити на доступ від інших держав-членів. Пояснювальний меморандум обґрунтовує таке обмеження сфери Проекту. Він стверджує, що доступ до інформації і обмін нею між правоохоронними органами є питанням, яке виходить за межі сфери дії Договору про ЄС.

40. КЄСЗД не переконало це твердження Пояснювального меморандуму. Втручання Спільноти на підставі статті 95 Договору про ЄС мало усунути бар'єри у торгівлі. Згідно із прецедентним правом Суду справедливості таке втручання повинно бути необхідним для сприяння усуненню таких бар’єрів. Проте, законодавець Спільноти повинен гарантувати повагу основоположних прав (стаття 6(2) Договору про ЄС). Незважаючи на все це, встановлення на рівні Спільноти норм щодо затримання даних в інтересах внутрішнього ринку може вимагати, щоб дотримання основоположних прав відбулося на рівні Спільноти. Якщо законодавець Спільноти не може встановити норми про доступ і використання даних, він не може виконати свої зобов'язання за статтею 6 Договору про ЄС, оскільки ці норми необхідні для гарантування того, що дані затримуються з дотриманням основоположних прав. Іншими словами, норми про доступ і використання даних є невіддільними від самого обов'язку затримання даних.

41. Щодо призначення уповноважених органів із захисту даних у правоохоронній діяльності КЄСЗД визнає, що це справа держав-членів. Подібним чином це стосується і судового захисту. Ці умови гарантують дотримання повною мірою законодавства про захист даних.

42. КЄСЗД звертає увагу на інший пункт, пов’язаний з юридичною основою. Справа саме законодавчого органу Спільноти вибрати адекватну юридичну основу і, відповідно, адекватну законодавчу процедуру. Цей вибір виходить за межі повноважень КЄСЗД. Проте, у світлі важливих проблем, КЄСЗД віддає в теперішній ситуації значну перевагу процедурі спільного ухвалення рішень. Тільки ця процедура встановлює прозорий процес ухвалення рішень за повної участі трьох причетних установ і з належним дотриманням принципів, на яких засновано Союз.

IV. Потреба у гармонізації

43. Проект директиви гармонізує типи даних, які мають бути затримані, періоди часу, протягом якого дані слід затримувати, так само як і цілі, для яких дані можуть надаватися належним органам. Проект передбачає гармонізацію цих елементів. У цьому відношенні він має істотно іншу природу, аніж Проект Рамкового рішення, який передбачав мінімальні норми.

44. КЄСЗД підкреслює потребу повної гармонізації цих елементів, зважаючи на функціонування внутрішнього ринку, потреби правоохоронної діяльності і, останнє за порядком, але не за значенням, – виконання положень ЄКПЛ і принципів захисту даних.

45. Щодо функціонування внутрішнього ринку гармонізація зобов’язань затримувати дані виправдовує вибір юридичної основи Проекту (стаття 95 Договору про ЄС). Дозволяючи відмінності між законами держав-членів, не можна усунути існуючі розлади на внутрішньому ринку електронних комунікацій, які мають місце завдяки прийняттю (або загрозі прийняття) законодавчих заходів в державах-членах згідно зі статтею 15 Директиви 2002/58/ЄС.

46. Це є навіть важливіше, оскільки значна кількість електронних комунікацій стосується юрисдикції більше однієї держави-члена. Серед ілюстративних прикладів можна назвати: телефонні дзвінки за кордон, роумінг, перетин кордонів під час мобільного зв'язку і використання постачальника з держави-члена, іншої, аніж країна проживання особи.

47. Окрім того, в цьому контексті брак гармонізації шкодив би потребам правоохоронної діяльності, оскільки належним органам доведеться підкорятися неоднаковим юридичним вимогам. Це може перешкодити обміну інформацією між органами влади держав-членів.

48. Врешті-решт, КЄСЗД наголошує з посиланням на свої повноваження згідно зі статтею 41 Постанови (ЄС) № 45/2001, що повна гармонізація головних елементів, включених до Проекту, є необхідною для того, щоб підкорятися ЄКПЛ і принципам захисту даних. Будь-яка законодавча міра, яка зобов’язує затримувати дані трафіку і місцезнаходження, має чітко обмежувати кількість даних, які затримуються, періоди затримання і (цілі, з якими здійснюється) доступ, а також подальше використання даних для того, щоб бути прийнятним з перспективи захисту даних, та для того, щоб виконати вимоги необхідності і пропорційності.

V. Коментарі до статей проекту

Стаття 3: Зобов'язання затримувати дані

49. Стаття 3 – ключове положення Проекту. Стаття 3(1) запроваджує зобов’язання затримувати дані трафіка і місцезнаходження, тоді як стаття 3(2) надає чинності принципу обмежен-

ня мети. Стаття 3(2) викладає три важливих обмеження. Затримання даних повинно здійснюватися тільки:

- уповноваженими національними органами;
- у спеціально визначених випадках;
- з метою запобігання, розслідування, виявлення і судового переслідування серйозних кримінальних злочинів, наприклад, таких, як тероризм і організована злочинність.

Стаття 3(2) посилається на національне законодавство держав-членів за визначенням подальших обмежень.

50. КЄСЗД підтримує статтю 3(2) як важливе положення, однак вважає, що ці обмеження не є достатньо точними, що доступ і подальше використання повинно бути врегульоване згідно із Директивою, а також, що потрібні додаткові заходи безпеки. Як було сказано, в Розділі III цього Висновку, КЄСЗД не переконаний, що невключення (точних) умов про доступ і подальше використання даних трафіку і місцезнаходження – неминучий наслідок юридичної основи Проекту (стаття 95 Договору про Європейський Союз). Це потягнуло за собою наступні коментарі.

51. По-перше. Не вказано, що інші зацікавлені сторони, подібно до самих постачальників, не мають доступу до даних. За статтею 6 Директиви 2002/58/ЄС постачальники можуть тільки обробляти дані трафіка до закінчення періоду, на який дані затримуються, з метою складання рахунків. На думку КЄСЗД, немає жодного виправдання на доступ постачальниками або іншими зацікавленими сторонами, окрім випадку доступу, передбаченого Директивою 2002/58/ЄС і на умовах цієї Директиви.

52. КЄСЗД рекомендує додати в текст припис з тим, щоб гарантувати, що крім уповноважених органів жодна особа не матиме доступу до даних. Цей припис може бути сформульованим наступним чином: “дані можуть бути доступними і/або оброблятися тільки з метою, згаданою в статті 3(2)” або “постачальники повинні ефективно гарантувати те, що доступ надається лише уповноваженим органам”.

53. По-друге. Обмеження спеціально визначеними випадками, як видається, забороняє звичний доступ до “виловлювання даних” або до отримання/відбору даних. Проте, текст Проекту повинен спеціально визначити, що дані можуть надаватися тільки в разі, коли це необхідно у зв'язку із певним злочином.

54. По-третє. КЄСЗД вітає той факт, що мета доступу обмежена серйозними злочинами, такими як тероризм і організована злочинність. У інших менш серйозних випадках доступ до даних трафіку не завжди буде пропорційний. Проте, КЄСЗД виражає сумніви, чи цього обмеження досить, особливо, коли йтиметься про надання доступу щодо серйозних злочинів, окрім тероризму і організованої злочинності. Практика держав-членів відрізняється. КЄСЗД наголошує в Розділі IV цього Висновку на потребі повної гармонізації головних елементів, включених до Проекту. Саме тому КЄСЗД рекомендує обмежити приписи певними серйозними злочинами.

55. По-четверте. Всупереч проекту Рамкового Рішення Проект не містить припису про доступ. З точки зору КЄСЗД, доступ до даних і їх подальше використання не повинно бути проігнорованим. Вони складають невіддільну частину змісту (див. Розділ III цього Висновку).

56. КЄСЗД рекомендує доповнити Проект однією або кількома статтями про доступ до даних трафіку і місцезнаходження уповноважених органів і про подальше використання даних. Мета цих статей – гарантувати, що дані використовуються тільки для цілей, згаданих у статті 3(2), що органи влади гарантують якість, конфіденційність і безпеку даних, які вони одержали, і що дані будуть стерті, коли вони не будуть більше потрібні для запобігання, розслідування, виявлення і судового переслідування певного злочину. Окрім того, слід вказати, що доступ у певних справах повинен перебувати під судовим контролем держав-членів.

57. По-п'яте. Проект не містить додаткових заходів безпеки для захисту даних. У преамбулі просто посилаються на заходи безпеки в чинному законодавстві, перш за все Директиву 95/46/ЄС і Директиву 2002/58/ЄС. КЄСЗД не погоджується із цим обмеженим підходом до захисту даних, незважаючи на особливу важливість (додаткових) заходів безпеки (див. Розділ II цього Висновку).

58.Саме тому КЄСЗД рекомендує включити параграф про захист даних. У цей параграф можуть бути вставлені попередні рекомендації з приводу статті 3(2), так само як і інші приписи про захист даних, наприклад, приписів, пов'язаних з порядком захисту даних суб'єктом відповідних даних (див. Розділ II цього Висновку), щодо якості даних і безпеки даних, а також щодо даних трафіку та місцезнаходження даних, які не стосуються злочину.

Стаття 4: Затримані категорії даних

59. Загалом, КЄСЗД вітає статтю і Додаток, оскільки:

- визначено законодавчо техніку з функціональним описом у вигляді директивних приписів і технічних деталей у додатку. Це достатньо гнучко для того, щоб адекватно відповісти на технологічні події, і це надає громадянам правової певності;
- відмінність між даними телекомунікації і Інтернет-даними, незважаючи на те, що відмінність стає технологічно менш важливою. Однак, з перспективи захисту даних ця відмінність є важливою, оскільки в Інтернеті межа між змістом даних і даними трафіка не є чіткою;
- рівень гармонізації: Проект передбачає високий рівень гармонізації з вичерпним списком категорій даних, які мають бути затримані (на відміну від проекту Рамкового Рішення, який містив список-мінімум з широким повноваженням держав-членів додавати свої пропозиції щодо переліку даних). З погляду перспективи захисту даних повна гармонізація є суттєвим у стосунках між державами-членами (див. Розділ IV).

60. КЄСЗД рекомендує наступні зміни:

- стаття 4, другий параграф, повинен містити реальніші критерії для того, щоб гарантувати, що дані змісту не включаються. Слід додати наступне речення: “Додаток не може включати дані, які показують зміст комунікації”;
- стаття 5 відкриває можливість для перегляду Додатку директивою Комісії. КЄСЗД радить, що перегляд Додатку з суттєвим впливом на захист даних повинен переважно здійснюватися за допомогою Директиви відповідно до процедури спільного ухвалення рішень[10].

Стаття 7: Періоди затримання даних

61.КЄСЗД вітає той факт, що періоди затримання даних у Проекті значно коротші, аніж періоди, що передбачалися у проекті Рамкового рішення:

- Нагадуючи про сумніви, виражені у цьому Висновку, про доказ необхідності затримання даних трафіку аж до одного року, період тривалістю один рік відображає методи правоохоронної діяльності;
- Ці ілюстрації показують також те, що, виключаючи виняткові випадки, затримання даних протягом довших періодів не відображають практику правоохоронної діяльності;
- Коротший період в шість місяців для даних, пов'язаних з електронними комунікаціями, що мають місце з винятковим або переважним використанням Інтернет, є важливим з точки зору перспектив захисту даних, оскільки затримання даних Інтернет-комунікацій призводить до накопичення значних за обсягом баз даних (ці дані зазвичай не затримуються з метою складання рахунків), межа змісту даних є невизначеною, а їх затримання довше, ніж шість місяців, що не відображає практики потреб правоохоронців.

62.Потрібно прояснити у тексті, що:

- період затримання даних – 6 місяців, один рік – максимальний період їх затримання;
- дані видаляються після закінчення періоду затримання. Потребно також прояснити, як ці дані потрібно видалити. На думку КЄСЗД, постачальнику доведеться видаляти дані автоматизованими засобами, як мінімум, кожен день.

Стаття 8: Вимоги до зберігання затриманих даних

63. Ця стаття близько пов'язана зі статтею 3(2) і містить важливе положення, яке може гарантувати, що доступ у спеціально визначених випадках може бути обмежений даними, які особливо потрібні. Статті 8 і 3(2)припускають, що необхідні дані передаються постачальниками органам влади і що останні не мають прямого доступу до баз даних. КЄСЗД рекомендує закріпити цю презумпцію безпосередньо в тексті.

64. Положення повинно бути деталізовано, вказуючи, що:

- необхідні дані передаються постачальниками органам влади (див. пункт 63);
- постачальники повинні встановити необхідні технічні пристрої, зокрема, системи пошуку для того, щоб полегшити цілеспрямований доступ до спеціально визначених даних;
- постачальники повинні гарантувати, що тільки їх персонал з відповідними технічними повноваженнями має доступ до баз даних з технічних причин і що ці члени персоналу ознайомлені із внутрішніми правилами конфіденційності щодо особливої уваги до “чутливих” даних;
- передача даних повинна не тільки мати місце без невчасної затримки, але і без показу інших даних трафіку і місцезнаходження, аніж ті, які були потрібні для цілей запиту.

Стаття 9: Статистика

65. Обов’язок постачальників подавати щорічно статистику допомагає установам Спільноти контролювати ефективність застосування цього Проекту. Потрібна адекватна інформація.

66. На думку КЄСЗД, це зобов'язання приводить в дію принцип прозорості. Громадянин має право знати, наскільки ефективним є захист даних у зв’язку з їх затриманням. Тому постачальника потрібно зобов'язати зберігати реєстраційні журнали і систематично виконувати ревізію, для того, щоб надати можливість національним органам із захисту даних контролювати застосування норм про захист даних на практиці[11]. Проект має бути змінений у цьому сенсі.

Стаття 10: Витрати

67. Як було зазначено в Розділі II, існує пряма залежність між адекватністю заходів безпеки і витратами на ці заходи. Саме тому КЄСЗД бере до уваги статтю 10, яка передбачає компенсацію наявних додаткових витрат як важливого положення, яке могло б послужити стимулом, для постачальників інвестування технічної інфраструктури.

68. Згідно із оцінками, поданими в “Оцінці впливу”, переданою Комісією до КЄСЗД, витрати на затримання даних значні. Для великої мережі і постачальника послуг витрати становлять більше ніж 150 мільйонів євро, а протягом 12-місячного періоду затримання з річними експлуатаційними витратами – понад 50 мільйонів євро[12]. Немає жодних цифр про витрати на заходи додаткової безпеки, як, наприклад, дорогі пошукові системи (див. коментар до статті 6), ні про (приблизно) фінансові наслідки повної компенсації додаткових витрат постачальників.

69. На думку КЄСЗД, точніші цифри потрібні для оцінки Проекту в його повному обсязі. Він пропонує висвітлити фінансові наслідки Проекту в Пояснювальному меморандумі.

70. Щодо безпосередньо положення статті 10, залежність між адекватністю заходів безпеки і витратами слід прояснити у тексті припису. Окрім того, Проект повинен передбачати мінімальні стандарти для заходів безпеки, вжитих постачальниками, для того, щоб претендувати на відшкодування з боку держави-члена. На думку КЄСЗД, визначення цих стандартів не можна повністю покласти на держави-члени. Це може поставити під сумнів рівень гармонізації, запровадженої Директивою. До того ж, потрібно взяти до уваги, що держави-члени несуть фінансові наслідки компенсації.

Стаття 11: Поправка до Директиви 2002/58/ЄС

71. Слід висвітлити відношення до статті 15(1) Директиви 2002/58/ЄС, оскільки цей Проект позбавляє це положення більшості його змісту. Посилання в статті 15(1) Директиви 2002/58/ЄС на статтю 6 і статтю 9 (цієї ж Директиви) потрібно видалити або змінити таким чином, щоб прояснити, що держави-члени більше не мають компетенції приймати законодавство відносно злочинів, доповнюючи цей Проект. Будь-яка неоднозначність щодо затримання даних для цілей “малозначних” злочинів – повинна бути усунена.

Стаття 12: Оцінка

72. КЄСЗД вітає, що Проект містить статтю про оцінювання Директиви протягом трьох років після набуття нею чинності. Оцінка є дуже важливою з огляду на сумніви про потрібність Проекту і його пропорційність.

73. КЄСЗД радить передбачити жорстке зобов'язання, яке містить наступні елементи:
- оцінювання повинно охоплювати оцінку ефективності виконання Директиви з перспективи правоохоронної діяльності, так само як і оцінку впливу на основні права суб'єкта даних. Комісія повинна включати будь-які докази, які можуть вплинути на оцінювання;

- оцінювання повинно проходити регулярно (як мінімум, кожні 2 роки);
- Комісію слід зобов'язати представити зміни до Проекту там, де необхідно (як в статті 18 Директиви 2002/58/ЄС).

VI. Висновки

Попередні умови

74. Для КЄСЗД має велике значення, щоб Проект дотримувався основоположних прав. Законодавчий захід, який би завдавав шкоди захисту, гарантованому правом Спільноти і особливо прецедентним правом Суду справедливості і Європейського суду з прав людини, є не тільки неприйнятним, але і незаконним.

75. Необхідність і пропорційність зобов'язання затримувати дані повною мірою мають бути продемонстровані.

76. КЄСЗД визнає зміни обставин, але не переконаний у необхідності затримання даних трафіку і місцезнаходження в цілях правоохоронної діяльності, як це встановлено у Проекті.

77. Тим не менше, КЄСЗД представляє у цьому Висновку свій погляд. Це означає, в першу чергу, що затримання даних трафіку і місцезнаходження не є адекватною або ефективною відповіддю. Потрібні додаткові заходи, щоб гарантувати, що органи влади мають цілеспрямований і швидкий доступ до даних, потрібних в певному випадку. Проект повинен:

- обмежувати періоди затримання потребами правоохоронної діяльності;
- обмежувати кількість даних, які затримуються. Ця кількість повинна відображати потреби правоохоронної діяльності і гарантувати, щоб доступ до даних був неможливим;
- містити адекватні заходи безпеки.

Загальна оцінка

78. КЄСЗД підкреслює важливість того факту, що текст Проекту повинен передбачати повну гармонізацію головних її елементів, зокрема, щодо видів даних, які затримуються, періоди часу затримання, так само як і (цілі) доступу і подальше використання даних.

79. По деяких пунктах потрібно подальше роз'яснення, наприклад, щоб гарантувати адекватне видалення даних після закінчення періоду затримання і щоб ефективно запобігти доступу і використанню різними групами хранителів.

80. КЄСЗД пропонує прийняття положень з точки зору перспективи захисту даних щодо:

- спеціальних положень про доступ до даних трафіка і місцезнаходження уповноважених органів влади і про подальше використання даних як суттєвої і невід’ємної частини змісту;
- подальших додаткових заходів безпеки для захисту (на відміну від простого посиланню на заходи безпеки в чинному законодавстві, зокрема Директива 95/46/ЄС і Директива 2002/58/ЄС), між іншим, щоб гарантувати дотримання прав суб’єкта даних;
- подальших стимулів постачальникам інвестувати в адекватну технічну інфраструктуру, зокрема, фінансові стимули. Ця інфраструктура може бути настільки адекватною, наскільки існують ефективні пошукові системи.

Рекомендації для модифікацій Проекту

81. Щодо статті 3(2):

- додавання положення для того, щоб гарантувати, що окрім уповноважених органів жодна особа не матиме доступу до даних. Це положення могло б бути сформульоване таким чином: “дані можуть бути доступними і оброблятися з метою, згаданою в статті 3(2)” або “постачальники повинні гарантувати, що доступ надаватиметься тільки уповноваженим органом”:
- деталізація того, які дані можуть надаватися, якщо це потрібно відносно певного злочину;
- обмеження положень щодо певних серйозних злочинів;
- додавання до Проекту однієї чи більше статей доступу до даних трафіку і місцезнаходження уповноваженими органами влади і про подальше використання даних, так само як і положення про те, що доступ в певних випадках повинен здійснюватися під судовим контролем;
- включення параграфа про захист даних.

82. Щодо статей 4 і 5:

- додавання до статті 4 другого параграфу наступного змісту – “Додаток не може включати дані, які показують зміст комунікації”;

- деталізація того, що захист даних повинен проводитися за допомогою Директиви відповідно до процедури ухвалення спільних рішень.

83. Щодо статті 7, деталізація тексту про те, що:

- періоди строком 6 місяців і один рік є максимальними періодами затримки даних;

- дані видаляються після закінчення періоду затримки. Текст повинен прояснити, як ці дані потрібно видаляти, а саме постачальником автоматизованих засобів, як мінімум, кожного дня.

84. Щодо статті 8, деталізація тексту про те, що:

- необхідні дані передаються постачальниками органам влади;

- постачальники повинні встановити необхідну технічну архітектуру, зокрема, пошукові системи, щоб полегшити цілеспрямований доступ до вказаних даних;

- постачальники повинні гарантувати, що тільки їх персонал має доступ до баз даних. Цей персонал ознайомлений з порядком захисту даних “чутливого” змісту і роботи згідно із внутрішніми правилами забезпечення конфіденційності;

- передача даних не повинна мати невчасну затримку та передбачати надання тільки даних, які задовольняють мету запиту.

85. Щодо статті 9: доповнити положенням, яке зобов'язує постачальника зберігати журнали і виконувати систематичні (само)ревізії для того, щоб надати можливість національним органам із захисту даних контролювати застосування норм про захист даних на практиці.

86. Щодо статті 10 висвітлити в Пояснювальному меморандумі:

- адекватність заходів безпеки і витрат слід прояснити;

- фінансові наслідки впровадження Проекту.

Вчинено у м. Брюссель 26 вересня 2005 року.

Комісар ЄС із захисту даних – Пітер Гастінкс.

---

[1] *ОЖ № L 281, 23.11.1995, с. 31.*

[2] *ОЖ № L 201, 31.7.2002, с.37.*

[3] *ОЖ № L 8, 21.1.2001, с. 1.*

[4] *Judgment of the ECHR of 16 February 2000, Amann, 2000-11, Appl. 27798/95.*

[5] *Judgment of the ECHR of 2 August 1984, Malone, A82, Appl. 8691/79.*

[6] *Judgment of the ECHR of 22 October 1981, Dudgeon, A45, Appl. 7525.*

[7] *Див. пункт 3 цього Висновку.*

[8] *Liberty and security, striking the right balance. Paper by the UK Presidency of the European Union of 7 September 2005.*

[9] *“The Position Paper on Law Enforcement and Information Exchange in the EU”, Краківська конференція із захисту даних, 25-26.04. 2005 р.*

[10] *“The Opinion of the EDPS of 23 March 2005 on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System and the exchange of data between Member States on short stay-visas”(Paragraph 3.12).*

[II] *“The Opinion of the EDPSof 23 March 2005 on the Proposal for a Regulation of theEuropean Parliament and of the Council concerning theVisa Information System and the exchange of databetween Member States on short stay-visas” (Paragraph 3.9).*

[12] *Комісія посилається на цифри ETNO (асоціація операторів телекомунікації ЄС). ОЖ № C 298, 29.11.2005, с. 0001-0012*

Пер. з англ. Р. Тополевського //www.khpg.org.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~