

КОМЕНТАР

до проекту Закону України
про моніторинг телекомунікацій
(реєстраційний № 4042 від 07.08.2003 р.)

Служба безпеки підготувала і подала через Кабінет Міністрів до Верховної Ради проект закону про моніторинг телекомунікацій. Не торкаючись історії питання про запровадження системи суцільного стеження в українських телекомунікаціях, дозволимо дати коментар цього проекту з точки зору відповідності його чинному законодавству України і потенційним наслідкам від його запровадження.

Як справедливо зазначають розробники проекту, “на сьогодні тенденція проникнення інформаційно-телекомунікаційних технологій в усі сфери особистого життя та суспільних відносин не тільки зберігається, а й посилюється”. Дійсно, сучасні технології значною мірою розширили можливості для розвитку людини, а разом з тим, й створили нові загрози. Але згадувана “тенденція проникнення” здається, що розуміється розробниками законопроекту буквально, як керівництво до дії.

Розглянемо доцільність прийняття такого законопроекту. Чи є потреба у ньому для суспільства?

У пояснювальній записці до законопроекту зазначається, що “законів, які б регулювали відносини правоохоронних органів та операторів телекомунікацій з питань створення та використання засобів отримання інформації з каналів телекомунікацій у процесі оперативно-розшукової, контррозвідувальної та розвідувальної діяльності, на сьогодні в Україні не має”.

Таке твердження не відповідає дійсності. Використання засобів негласного зняття інформації з каналів зв'язку (надалі ЗНЗІ) правоохоронними і розвідувальними органами регламентується низкою чинних законів і підзаконних нормативних актів. Окрім Конституції, це – Кримінальний та Кримінально-процесуальний кодекси, закони України про оперативно-розшукову діяльність, про контррозвідувальну діяльність; про розвідувальні органи України, про боротьбу з тероризмом, про прокуратуру, Службу безпеки, Державну прикордонну службу України, державну охорону органів державної влади України та посадових осіб, статус суддів, забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві, державний захист працівників суду і правоохоронних органів, інші законодавчі акти та міжнародно-правові угоди і договори, учасником яких є Україна. Як ми бачимо, чинне законодавство врегульовує використання ЗНЗІ.

Щодо створення ЗНЗІ також існують відповідні правила, встановлені Указом Президента України “Про впорядкування виготовлення, придбання та застосування технічних засобів для зняття інформації з каналів зв'язку” від 13.04.2001 р., а також Ліцензійними умовами провадження господарської діяльності з розроблення, виготовлення спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації, торгівлі спеціальними технічними засобами для зняття інформації з каналів зв'язку, іншими засобами негласного отримання інформації від 29.01.2001р. (затвердженими спільним наказом СБУ і Держкомітету з питань регуляторної політики і підприємництва).

Слід відзначити, що положення вищезазначених нормативних актів, що стосуються використання і створення ЗНЗІ доволі докладно визначають права і обов'язки суб'єктів відносин, визначають процедуру застосування негласних засобів і гарантії додержання законності. Хоча містять й недоліки, що нерідко приводять до порушення прав і свобод громадян¹.

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

Розробники законопроекту вважають, що “сили та засоби, якими володіють на сьогодні правоохоронні органи, тактика їх застосування та чинне законодавство не дають можливості ефективно протидіяти...” злочинності. При цьому однак, на жаль жодного прикладу не наводиться. Що саме “заважає” правоохоронцям боротися із злочинністю? І що приховує загадкова назва “моніторинг телекомунікацій”?

Законопроектом передбачається запровадження системи “моніторингу” в усіх телекомунікаційних мережах загального користування. Зазначена система “моніторингу” запроваджується в обов'язковому порядку і на постійній основі, а використання телекомунікаційного обладнання без обладнання для “моніторингу” буде заборонено. Під моніторингом розробники проекту розуміють “*спостереження, відбір за визначеними ознаками, оброблення та реєстрація сеансу зв'язку в мережах телекомунікацій*”.

Однак контекстний аналіз законопроекту дозволяє дійти висновку, що йдеться не про “спостереження”, а про **перехоплення** комунікацій (зв'язку), яке буде здійснюватись автоматизовано на постійній основі з “віддалених робочих місць доступу до системи моніторингу” безпосередньо спецслужбами. Тобто працівники спецслужб будуть мати можливість з свого робочого місця шляхом “натисканням на кнопку” перехоплювати усі комунікації (телефонні дзвінки, електронну кореспонденцію та інші види електронних повідомлень користувачів телекомунікацій), навіть без відвідування операторів.

Для чого таке “спрошення”?

За чинним Законом України “Про оперативно-розшукову діяльність” (ОРД) для застосування ЗНЗІ потрібно виконання низки умов і дотримання процедури, що гарантує додержання законності. Виключний перелік підстав для застосування ЗНЗІ визначений у статті 16 Закону, а гарантії законності і обмеження для застосування ЗНЗІ визначаються у статті 18. Це, по-перше, одержання дозволу на підставі рішення суду; по-друге, повідомлення прокурору протягом доби. І, нарешті, надзвичайно важливий критерій – застосування ЗНЗІ проводиться виключно з **метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншим способом одержати інформацію неможливо (!)**.

Чому висуваються такі вимоги до застосування ЗНЗІ за чинним законодавством?

Законодавець, сформулювавши особливі вимоги до застосування ЗНЗІ, так само як і до негласного проникнення до житла чи до іншого володіння особи, визнав, що ця діяльність є потенційно **більш загрозливою** для прав і свобод громадян, оскільки являє собою втручання у приватне життя, недоторканність якого гарантується статтею 34 Конституції України і статтею 8 Європейської Конвенції про захист прав людини. Саме тому, процедура застосування ЗНЗІ не може запроваджуватися на узагальненій рутинній основі, бо це є винятковим заходом оперативної (а не систематичної!) роботи правоохоронних органів, який застосовується до визначених осіб на визначений термін за рішенням суду.

Отже, запропоноване в законопроекті “спрошення” закладеного в Законі про ОРД механізму – спрощує можливість неконтрольованого застосування ЗНЗІ, і підвищує ризик порушення прав і свобод громадян України, а отже й безпеки як окремої людини, так і усього громадянського суспільства від втрати контролю над спецслужбами. Невипадково, розробники “забули” включити вимогу щодо такої виключної підстави для застосування ЗНЗІ як “неможливість одержання інформації іншим способом до тексту законопроекту”, бо планується систематичне застосування моніторингу, інакше “вичинка овчини не варта”.

Чи виправданий ризик?

Можливий аргумент спецслужб, що цей ризик є ціною за безпеку суспільства, не є в дійсності аргументом, бо не підтверджений жодним прикладом. Для цього, щонайменше потрібно довести, що запровадження саме цієї (потенційно небезпечної!) системи моніторингу покращить у порівнянні з існуючим правовим механізмом рівень безпеки

суспільства настільки, що це виправдовуватиме підвищення ризику порушення права громадян на приватність і втрати контролю суспільством над спецслужбами.

Такий підхід до оцінки правомірності втручання у приватне життя сформулював Європейський Суд з прав людини у своїй практиці. Обмеження права на приватність повинні:

- запроваджуватися на підставі закону;
- мати легітимну ціль;
- бути необхідними у демократичному суспільстві.

Загальним критерієм для встановлення балансу між конкуруючими інтересами є дотримання принципу **пропорційності** при впровадженні обмежень. Цей принцип був сформульований Європейським Судом з прав людини таким чином:

- “фраза “бути необхідним у демократичному суспільстві” означає, щоб бути сумісним з Конвенцією, втручання повинно, серед іншого, відповідати “нагальній соціальній потребі” і бути “пропорційним до законної мети, що переслідується”; і далі, “закон, що надає свободу вибору під час здійснення повноважень повинен передбачати їх обсяги”²;

- “застосування на практиці заходів негласного стеження за кореспонденцією не є відкритим для ознайомлення зацікавленою особою або громадського загалу, надана законодавством виконавцям свобода дій у необмеженому об’ємі суперечить принципу верховенства права. Отже, закон повинен визначати межі розсуду компетентних органів і способи їх застосування з достатньою ясністю, з урахуванням легітимної мети їх застосування у конкретному випадку, для надання індивідам адекватного захисту проти свавільного втручання”³.

Надання спецслужбам права застосовувати ЗНЗІ з робочих місць віддаленого доступу є надмірним і не виправданим розширенням їх повноважень, що порушує принцип пропорційності!

Які інші наслідки матиме прийняття цього закону, зокрема, для ринку телекомунікацій?

Крім ризику порушення прав і свобод людини, запровадження цієї системи вимагає значних витрат з боку операторів телекомунікацій, на яких покладається обов’язок здійснити впровадження системи за власні кошти. Хоча, йдеться не про інвестиції у безпеку телекомунікаційних мереж, а інвестиції у інфраструктуру стеження за громадянами. Здається, що розробники законопроекту не здійснювали взагалі жодних підрахунків можливих витрат від запровадження і підтримання цієї системи моніторингу, а це варто було б зробити. Зрозуміло, що в кінцевому підрахунку, це віднесеться на збільшення вартості послуг для споживачів.

Крім того, це створюватиме додаткові перешкоди для вільного доступу до ринку телекомунікацій нових операторів, оскільки збільшуватиме розмір потрібних для цього початкових інвестицій. Процедура погодження з спецслужбами технічних вимог до телекомунікаційного обладнання наділяє їх фактично функцією регулятора ринку телекомунікацій, що знову ж таки відкриває можливості для зловживань. Фактично СБУ перетворюється на регулюючий орган, який визначатиме правила гри на цьому ринку і матиме важелі адміністративного впливу на розвиток телекомунікацій в Україні, що не відноситься до сфери функціональних обов’язків цього органу держави.

Слово за операторами...

Як це вплине на міжнародне співробітництво у галузі боротьби із злочинністю?

Важливим для розуміння суті питання є міжнародний аспект, на який неодноразово

² Silver and Others vs. the United Kingdom. - Judgment of 25 March 1983 // Judgments and decisions. - Series A no. 61

³ Amann v. Switzerland [GC], no. 27798/95, § 65, ECHR 2000-II)

дається посилання у пояснювальній записці. Розробники вказують, що запровадження системи моніторингу начебто відповідає європейському підходу. Таке твердження не відповідає дійсності. Ні документи ENFOPOL, ні Конвенція Ради Європи про кіберзлочинність не передбачають запровадження системи моніторингу у вигляді запропонованому розробниками законопроекту. Згадувана Резолюція Ради Європейського Союзу від 17 січня 1995 року про законне перехоплення телекомунікацій (не моніторинг, а саме перехоплення!) вимагає, щоб саме оператори телекомунікацій передавали повідомлення, що перехоплюються (п.3).

Згадування проекту “Рамкового рішення відносно утримання даних трафіку і доступу до цих даних у зв'язку з кримінальним розслідуванням чи судовим переслідуванням” у пояснювальній записці є недоречним, оскільки цей проект був відкликаний з порядку денного Ради ЄС (а не Ради Європи!) ще пізніше тому, через невідповідність його європейським стандартам у галузі прав людини. Саме тому, така система моніторингу ніколи не буде запроваджена в країнах Європейського Союзу. Більше того, країни ЄС та інші країни члени Ради Європи запровадили загальноєвропейські стандарти щодо захисту права на повагу до приватного життя у відповідності з вищезазначеними принципами, сформульованими Європейським Судом з прав людини. Про що, зокрема, свідчить посилання в текстах Конвенції Європол і Шенгенської Конвенції (документи Європейського Союзу) на Рекомендацію Ради Європи, що регулює використання персональних даних у секторі поліції 1987 року⁴.

Нажаль, Україна стоїть осторонь цих процесів, до сих пір не підписавши Конвенцію Ради Європи про захист осіб стосовно автоматизованої обробки персональних даних 1981 року, хоча відповідне доручення Кабінет Міністрів отримав від Президента України ще у 2001 році⁵! Невідповідність українського законодавства європейським стандартам у цій галузі є фактором, що гальмує співробітництво з країнами ЄС у багатьох сферах, не тільки у правоохоронній.

Хочеться сподіватись, що здоровий глузд перемаже!

Андрій Пазюк
12 вересня 2003 року

⁴ Більш докладно про європейські стандарти у галузі використання персональних даних в правоохоронній діяльності можна дізнатись на веб-сторінці “Прайвесі Юкрейн”:

<http://www.internetrights.org.ua/index.php?page=chapters&id=13>

⁵ Указ Президента України від 06.12.2001 № 1193/2001 Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року "Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України"