Изх. № 90/05.11.2009 г.

ДО МИНИСТЪРА НА
ВЪТРЕШНИТЕ РАБОТИ
Г-Н ЦВЕТАН ЦВЕТАНОВ

СТАНОВИЩЕ

НА

ПРОГРАМА ДОСТЪП ДО ИНФОРМАЦИЯ

ПО ЗАКОНОПРОЕКТ ЗА ИЗМЕНЕНИЕ И ДОПЪЛНЕНИЕ НА ЗАКОНА ЗА ЕЛЕКТРОННИТЕ СЪОБЩЕНИЯ

Уважаеми господин министър,

След запознаване с текста на публикувания в интернет страницата на Министерството на вътрешните работи проект за закон за изменение и допълнение на Закона за електронните съобщения (ЗЕС) и след общественото му обсъждане на 02.11.2009 г. съгласно чл. 26, ал.2 от Закона за нормативните актове, представяме в писмен вид в определения от Вас срок бележките и предложенията на *Програма Достъп до Информация*.

I. Основни моменти в проекта:

1. Задължението за съхраняване на данни по действащия чл.251 от ЗЕС се разширява, като се предлага това да става за нуждите на разкриването и разследването на престъпления, за които е предвидено наказание лишаване от свобода две или повече години и престъпления по глава девета "а" от Наказателния кодекс (НК).

2. Въвежда се задължение за съхраняване на данни, необходими за издирване на лица.

3. Създава се интерфейс, чрез който специализирана дирекция „Оперативни технически операции" (ДОТО) при МВР има **директен достъп** до данните по чл. 250а, ал. 1.

4. Определят се органите, които имат право да искат достъп до данните по чл. 250а, ал. 1.

5. Определят се реквизитите на искането за достъп до данните по чл.250а, ал. 1.

6. Определя се Комисията за защита на личните данни (КЗЛД) за **наблюдаващ орган.**

7. КЗЛД предоставя ежегодно статистически данни на Народното събрание и на Европейската комисия.

8. Увеличава се размерът на глобата за противозаконно нарушаване неприкосновеността на кореспонденцията по чл. 171, ал. 1 НК.

I. <u>Резюме на становището</u>

От мотивите към проекта става ясно, че МВР констатира проблеми в практиката, на които основава необходимостта от законодателна промяна. Още тук трябва да се подчертае, че това няма общо с въвеждането на директива и Директива 2006/24/ЕО вече е въведена с редакцията на ЗЕС (изм. и доп. ДВ бр.17/2009 г.).

Безпокойство будят следните моменти в текста:

- Предоставянето на пряк, постоянен и безконтролен достъп на специализирана дирекция „Оперативни технически операции" (ДОТО) към МВР до данните по чл. 251а, ал. 1.
- Обезсмислянето на съществуващия предварителен съдебен контрол чрез наличието на пряк достъп на ДОТО и липсата на изискване съдебното разрешение за достъп да се предяви на предприятията по ЗЕС.
- Липсата на изискване за мотивиране на искането за достъп до данни от страна на поискалите тази достъп органи и звена.
- Липсата на финансово обезпечение на въвеждането в експлоатация на интерфейса.
- Липсата на ефективен последващ контрол за възможни злоупотреби и незаконна намеса в личния живот от страна на изпълнителната власт.

Правото на защита на личните данни е основно човешко право. Задължения за гарантирането на това право, особено при обработката на лични данни, възниква за държавни институции, административни структури, частни търговски дружества и т.н.

На основата на стандартите на Съвета на Европа и Европейския Съюз, следва да се подчертае, че достъпът до лични данни трябва да бъде винаги <u>с предварително определена законна цел, пропорционален на постигането на тази цел и да се прилага стеснително</u>. Трябва да има ясна процедура за достъп и ефективен предварителен и последващ контрол.

Предлаганият проект не съответства на така изведените основни положения. Чрез създаването на интерфейс за директен достъп до данни се обезсмисля предвиденият в чл. 250в съдебен контрол. Подобна практика противоречи на изискването за пропорционалност при намесата в личния живот и нарушаването неприкосновеността на кореспонденцията.

Друга съществена необходимост за гарантиране правото на неприкосновеност на личния живот е упражняването на ефективен контрол върху

ограниченията на това право. Необходим е независим от изпълнителната власт парламентарен контрол. Определянето на наблюдаващ, а не контролиращ орган не е достатъчна гаранция за спазването на основни права.

II. Нормативна уредба

На първо място, режимът на уредба на съхраняването и достъпа до данни за електронните комуникации следва да е съответен на чл. 32 и чл. 34 от Конституцията на Република България и чл.8 от Европейската Конвенция за правата на човека и основните свободи (ЕКПЧ).

Съгласно законодателството за защита на личните данни /чл.32 от КРБ, чл.8 от ЕКПЧ, Конвенция № 108, Директива 95/46/ЕО/ обработването на лични данни може да става само при предварително и точно определени законосъобразни цели. В Директива 2006/24/ЕО, която се цитира в проекта за изменение на ЗЕС, е предвидено електронните данни да се съхраняват и да бъдат предмет на достъп (две от формите на обработване), **но не предвижда** предоставянето на неограничен достъп чрез интерфейс.

III. Конкретни предложения

1. В настоящия му вид текстът на чл. 250б, ал. 1 в редакцията, предложена от междуведомствената работна група, противоречи на чл. 32, ал.2 от Конституцията, чл.8 от ЕКПЧ, Конвенция № 108 за защита на личните данни при автоматизираната им обработка, Директива 95/46/ЕО и Директива 2006/24/ЕО. В тази връзка подчертаваме следното:

НАРУШЕН е чл.32, ал.2 от Конституцията, който гласи:

"(2) Никой не може да бъде следен, фотографиран, филмиран, записван или подлаган на други подобни действия без негово знание или въпреки неговото изрично несъгласие освен в предвидените от закона случаи."

Текстът изисква прецизното определяне на случаи, което изключва директен технически достъп /чрез интерфейс/ до базите данни. Постоянният достъп до базите данни на практика премахва всякакъв индивидуален подход.[1]

НАРУШЕН е чл.34, ал.2 от Конституцията, който гласи:

"Чл. 34. (1) Свободата и тайната на кореспонденцията и на другите съобщения са неприкосновени.

(2) Изключения от това правило се допускат само с разрешение на съдебната власт, когато това се налага за разкриване или предотвратяване на тежки престъпления."

[1] Срв. още Решение № 13627/11.12.2008 по а.д.№ 11799/2008 на ВАС, Петчленен състав, обн. ДВ бр.108/2008 г.

Тайната на кореспонденцията предполага и тайна на това кой с кого и кога е кореспондирал. Вмешателство е допустимо само след съдебен акт за всеки конкретен случай. Следователно прекият достъп до базите данни НАРУШАВА този текст на Конституцията.

НАРУШЕН е чл.8 от Европейската Конвенция за правата на човека, според който преценката за достъп трябва да се прави за всеки конкретен случай от независима институция[2].

НАРУШЕН е чл.4 от Директива 2006/24/ЕО, който изрично препраща към чл.8 от Европейската Конвенция за правата на човека и спазване на установената от съда практика.

Предложение: В края на чл. 250б, ал. 1 следва да се добави „**за целите и при реда и условията, предвидени в този закон".**

Мотиви: За да са спазени изискванията за индивидуален подход при даване на разрешения за достъп, процедурата следва да включва: а/ искане за достъп до данните по чл. 250а, ал. 1 от съответния орган до компетентния съд, б/ съдебно разрешение, в/ изпращане на разрешението съответното предприятие по ЗЕС, г/ предоставяне на достъп за конкретния случай.

Предложената редакция на чл. 250б, ал. 1 обръща тази процедура и предполага неограничен достъп до базите данни и съдебен контрол *a posteriori* и то само когато специализирана ДОТО към МВР предоставя данните на органите по предложения чл. 250в. Липсата на ефективен съдебен контрол и средства за защита срещу произволна намеса са недопустими. За да се предотврати забавянето в предоставянето на данните, може да се предвидят санкции срещу предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги. Освен това, проектозаконът изрично предвижда в чл. 250б, ал. 3 достъп до данни да се извършва по реда на НПК. Следователно винаги съществува възможността в неотложни случаи да се предостави достъп с разпореждане на наблюдаващ прокурор, като в срок до 24 часа бъде одобрен от съда.

В решението по делото *Мълоун срещу Великобритания* Европейският съд по правата на човека подчертава, че неограничената възможност за намеса в личния живот дадена на изпълнителната власт е противна на принципа на върховенство на закона[3].

---

[2] Case of Malone v. the UK, Application no. 8691/79
Case of Klass and others v. Germany, Application no. 5029/71

[3] „След като практическото прилагане на мерки за секретно следене на съобщения не подлежи на проверка от страна на засегнатото лице или на обществото, би било противно на принципа за върховенство на закона дискрецията, предоставена на изпълнителната власт, да бъде формулирана като неограничена власт. Следователно, законът трябва да сочи обхвата на всяка такава свобода на усмотрение, предоставена на компетентните органи, и начина на упражнението й, с достатъчна яснота - като се държи сметка и за законната цел на въпросната мярка - за да дава на индивида адекватна защита срещу произволна намеса." - § 68.

2. Проектозаконът за изменение и допълнение на ЗЕС предвижда създаването на чл. 250в, ал. 1, който гласи:

„Право да искат извършване на справки за данните по чл. 250а, ал. 1, съобразно тяхната компетентност имат....” следва изброяване на органите.

Предложение: след думите „съобразно тяхната компетентност имат” да се добави „ръководителите на…”.

***Мотиви*:** дирекциите не са субект на правото, в този смисъл те не притежават праводееспособност. Предлаганото допълнение ще съответства на формулировката в чл. 250в, който предвижда исканията за достъп да се изготвят от съответния ръководител на органите по чл. 250в, ал.1.

3. Предложението на междуведомствената работна група за ал. 2 на чл. 250в от ЗЕС гласи:

„За достъп до данните по чл. 250а, ал. 1 се изготвя писмено искане от съответния ръководител на органите по ал. 1, съдържащо:
1. регистрационния номер на преписката, за която е необходимо извършване на справката;
2. периода от време, който да обхваща справката;
3. данните, които следва да се отразят в справката;
4. определеното длъжностно лице, на което да се предоставят данните.

***Предложение*:** След т. 1 следва да се добави *„правното основание и целта, за която е необходим достъп до данните по чл. 250а, ал. 1*” и следващите точки да се преномерират съответно.

Мотиви: Липсата на основание за искане на достъп до данните по чл. 250а, ал. 1 възпрепятства ефективния контрол на намесата в личния живот и създава възможност за злоупотреби. Единствено при посочено основание съдът би могъл да прецени необходимостта от предоставяне на достъп. Регистрационният номер на преписката, за която е необходима справката не е достатъчна информация за установяване характера на престъплението и дали отговаря на условията по чл. 250а. Според председателя на Софийски градски съд (СГС) съществуващата практика е да се подават мотивирани искания.[4] Това е допълнителен аргумент и новият проект да предвижда мотивиране. Намесата в упражняването на основно човешко право не може да бъде немотивирана.

(Пример: „справката е необходима за разкриване на престъпление по чл. 115 от НК”.)

[4] Позицията на председателя на СГС бе изразена на обществената дискусия на 2.11.2009 г.

4. Предложението на междуведомствената работна група за ал. 5 на чл. 250в от ЗЕС е данните по ЗЕС да се съхраняват за разкриването и разследването на престъпления, наказуеми с „лишаване от свобода" две или повече години, вместо тежки престъпления, както е при сегашния режим. Мотиви са изложени подробно чрез посочване на примери.

Правният подход не може да се сподели. Пренебрегната е нормата на чл.34 от Конституцията. Нуждата от достъп до данни за разкриване на други престъпления означава, че същите трябва да бъдат **изрично посочени в закона**, а не да се разширява наедро обхватът на достъпа. Обяснението, че това щяло да бъде обемно изброяване, е абсолютно неприемливо. Изписването на пет реда повече в проекта се противопоставя на възможността правата на хиляди хора да бъдат накърнени.

5. Предложението на междуведомствената работна група за ал. 5 на чл. 250в от ЗЕС гласи:
„Специализираната дирекция "Оперативни технически операции" при МВР извършва справка за данните по чл. 250а, ал. 1, при постъпване на искане, по което е издадено разрешение. Искането се регистрира в специален регистър, който не е публичен".

Предложение: след думите по чл. 250а, ал. 1 да се добави: *„като изпраща издаденото съдебно разрешение на съответното предприятие. Предприятието е длъжно да осигури исканията достъп в срок от ...*"

***Мотиви*:** Така формулиран чл. 250в, ал. 5 ще отговаря на предложената нормална процедура по предоставяне на достъп да базите данни единствено след съдебен контрол. Определянето на конкретен срок би предотвратило сегашната практика по забавяне на предоставянето на информация от страна на предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги. Биха могли да се предвидят и санкции срещу предприятията, неизпълняващи задълженията си в срок.

6. Чл. 261а от проектозакона предвижда:
„Комисията за защита на личните данни да е наблюдаващ орган относно сигурността на данните, съхранявани съгласно чл. 250а, ал.1"

Предложение: В края на текста да се добави **„Парламентарният контрол върху дейността на МВР се осъществява от специализирана постоянна комисия на Народното събрание".**

Мотиви: Определянето на **наблюдаващ, а не контролиращ орган** не предоставя необходимите гаранции срещу незаконна намеса в личния живот и

злоупотреби. За да се спази принципът, че ограниченията на основните права следва да се тълкуват стеснително, е необходим не само наблюдаващ, но и **контролиращ орган**.[5]

Съдебното разрешение за достъп до данни по чл. 250, ал. 1 гарантира предварително срещу произволен и безконтролен достъп. Необходимо е обаче ЗЕС да предвижда и контрол през следващите етапи, като например дали се спазват разрешенията и аналогично, дали съхраняваната информация е унищожена съгласно чл. 251 ал. 3, съществуваща редакция. Такъв контролиращ орган би могло да бъде парламентарна комисия, напр. специализираната парламентарна комисия по Закона за специалните разузнавателни средства.[6] Наблюдаващ орган не би имал необходимия капацитет да противодейства на възможни злоупотреби.

КЗЛД е наблюдаващ орган единствено спрямо дейността на предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги. Няма ефективен контрол върху дейността на органите, имащи право да поискат достъп до данните, както и по-специално върху дейността на МВР, включително върху отчетната му дейност съгласно предложения чл. 261а, ал. 5. КЗЛД е оправомощена да изисква статистическа информация от предприятията предоставящи обществени електронни съобщителни мрежи и/или услуги, която да предостави на Европейската комисия съгласно чл. 10 от Директива 2006/24/ЕО. Тя обаче няма подобна власт спрямо МВР. За да се спази принципът „власт контролира власт" е необходимо да се предвиди парламентарен контрол върху дейността на изпълнителната власт. Това не възпрепятства по никакъв начин наблюдаващите функции на КЗЛД относно сигурността на данните.

7. Предложеният проект не предвижда при никакви условия и след изтичането на никакъв период от време право на достъп на засегнатите лица до информацията, че данните им са били обект на достъп по ЗЕС. Нуждата от уредбата на това право произтича от общите принципи на европейското и българското законодателство за защита на личните данни, както и от чл.8 от ЕКПЧ. Аналогична уредба се съдържа в приетите изменения в Закона за специалните разузнавателни средства.[7] Липсата на каквато и да е правна уредба относно уведомяване на лицата, подложени на тайно наблюдение, след време и при определени обстоятелства вече е обявено за нарушение на чл.8 от ЕКПЧ, в частност от страна на България.[8]

---

[5] Вж. също решение по делото Асоциация за европейска интеграция и права на човека и Екимджиев срещу България. Липсата на последващ контрол на използването на СРС е обявено за нарушение на ЕКПЧ.

[6] Решение от 28.06.2007 г., на ЕСПЧ, Екимджиев срещу България, жалба № 62540/2000 г., § 87. Самата специализирана парламентарна комисия е създадена в изпълнение на генералните мерки по решението на ЕСПЧ.

[7] Въвеждането на право на достъп до информация за засегнатите лица при определени условия и след определен срок произтича пряко от цитираното решение на ЕСПЧ /вж. бел.6/, § 90, 91, 93.

[8] Ibidem. § 90.

8. Законопроектът за ЗИД на ЗЕС предвижда изменение на чл. 305, което задължава предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги за своя сметка да въведат в експлоатация и поддържат прихващащи интерфейси.

Предложение: да отпаднат думите „за своя сметка”

***Мотиви*:** Създаването на допълнителни финансови тежести за търговски предприятия накърнява свободната стопанска инициатива, гарантирана от чл. 19 от Конституцията на РБ и е сериозно вмешателство в бизнеса. Задължението е особено неблагоприятно за частния сектор в условията на икономическа криза.

С уважение:

Д-р Гергана Жулева, Изпълнителен директор на ПДИ

Адв. Александър Кашъмов, Ръководител правен екип на ПДИ

Тереза Алексова, юрист в ПДИ