Р Е П У Б Л И К А Б Ъ Л Г А Р И Я

Н А Р О Д Н О С Ъ Б Р А Н И Е

Проект

З А К О Н

за изменение и допълнение на Закона за електронните съобщения

(Обн., ДВ, бр. 41 от 2007 г.; изм. и доп., бр. 109 от 2007 г., бр. 36, 43 и 69 от 2008 г., бр. 17, 35, 37 и 42 от 2009 г.; Решение № 3 на Конституционния съд от 2009 г. – бр. 45 от 2009 г.; изм. и доп., бр. 82, 89 и 93 от 2009 г.)

§ 1. В чл. 107 се създава т. 13а:

"13а. задълженията и изискванията за осигуряване на условия за прихващане на електронни съобщения, свързани със защита на националната сигурност и опазване на обществения ред;".

§ 2. Създават се чл. 250а, 250б и 250в:

"Чл. 250а. (1) 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, както и за издирване на лица, предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, съхраняват за срок 12 месеца данни, създадени или обработени в процеса на тяхната дейност, които са необходими за:

1. проследяване и идентифициране на източника на връзката;

2. идентифициране на направлението на връзката;

3. идентифициране на датата, часа и продължителността на връзката;

4. идентифициране на типа на връзката;

5. идентифициране на крайното електронно съобщително устройство на потребителя или на това, което се представя за негово крайно устройство;

6. установяване на идентификатор на ползваните клетки.

(2) Други данни, включително разкриващи съдържанието на съобщенията, не могат да бъдат съхранявани по този ред.

(3) Предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, са длъжни да унищожат данните след изтичането на срока по ал. 1 с изключение на данните, до които е имало достъп чрез предприятията и те са били съхранени.

(4) При достъп до данните, осъществен от специализирана дирекция "Оперативни технически операции" на

Министерството на вътрешните работи чрез интерфейс, ръководителят на органа, отправил искане за достъп, уведомява предприятието за необходимостта от запазване на данните.

(5) Данните по ал. 1 се обработват и съхраняват в съответствие с изискванията на Закона за защита на личните данни.

Чл. 250б. (1) Предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, осигуряват чрез интерфейс на специализирана дирекция "Оперативни технически операции" на Министерството на вътрешните работи достъп за извършване на справки за данните по чл. 250а, ал. 1, за целите, при условията и по реда, предвидени в този закон.

(2) Предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, в случаите, в които не е осигурен достъп чрез интерфейс, в срок до 8 часа от постъпване в деловодството на предприятието на разпореждането за достъп по чл. 250в, ал. 4 и чл. 251, ал. 2 предоставят данните директно на органите, които са поискали достъп.

(3) За нуждите на наказателното производство данните по чл. 250а, ал. 1 се предоставят на съда и на органите на досъдебното производство при условията и по реда на Наказателно-процесуалния кодекс директно от предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги.

Чл. 250в. (1) Право да искат извършване на справки за данните по чл. 250а, ал. 1 съобразно тяхната компетентност имат ръководителите на:

1. специализираните дирекции, териториалните дирекции и самостоятелните териториални отдели на Държавна агенция "Национална сигурност";

2. Главна дирекция "Криминална полиция", Главна дирекция "Борба с организираната престъпност", Главна дирекция "Охранителна полиция", Главна дирекция "Гранична полиция", дирекция "Вътрешна сигурност", Столичната дирекция на вътрешните работи, областните дирекции на Министерството на вътрешните работи и териториалните звена на Главна дирекция "Борба с организираната престъпност";

3. службите "Военна информация" и "Военна полиция" към министъра на отбраната;

4. Националната разузнавателна служба.

(2) 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. правното основание и целта, за която е необходим достъпът;

3. периода от време, който да обхваща справката;

4. данните, които следва да се отразят в справката;

5. определеното длъжностно лице, на което да се предоставят данните.

(3) За направените искания органите по ал. 1 водят специален регистър, който не е публичен.

(4) Достъпът до данните по чл. 250а, ал. 1 се осъществява след разрешение от председателя на районния съд или от оправомощен от него съдия по седалище на органа, който е поискал достъп, за което се издава разпореждане за предоставяне на достъп до данните.

(5) Разпореждането за предоставяне на достъп до данните по чл. 250а, ал. 1 задължително съдържа:

1. периода от време, който да обхваща справката;

2. данните, които следва да се отразят в справката;

3. определеното длъжностно лице, на което да се предоставят данните;

4. име, длъжност и подпис на съдията.

(6) За дадените разрешения или откази в съответните районни съдилища се води специален регистър, който не е публичен.

(7) Специализираната дирекция "Оперативни технически операции" на Министерството на вътрешните работи извършва справка за данните по чл. 250а, ал. 1 след постъпване на разпореждане за достъп. Постъпилото разпореждане за достъп се регистрира в специален регистър, който не е публичен.

(8) Справка за данните по чл. 250а, ал. 1 в специализирана дирекция "Оперативни технически операции" на Министерството на вътрешните работи могат да извършват единствено длъжностни лица, писмено оправомощени от министъра на вътрешните работи.

(9) При наличие на техническа възможност ръководителят на специализирана дирекция "Оперативни технически операции" на Министерството на вътрешните работи дава писмено разпореждане за изготвяне на исканата справка, което се отразява върху изготвеното искане.

(10) След изготвянето ѝ справката се подписва от ръководителя на специализирана дирекция "Оперативни технически операции" на Министерството на вътрешните работи или от писмено оправомощено от него длъжностно лице. Справката се регистрира в специален регистър и се изпраща на определеното в искането длъжностно лице, на което да се предоставят данните. Искането и разпореждането се връщат на съответната структура по ал. 1."

§ 3. Член 251 се изменя така:

“Чл. 251. (1) Данните по чл. 250а, ал. 1 могат да се предоставят по молба и на компетентен орган на друга държава, когато това е предвидено в международен договор, който е в сила за Република България.

(2) Достъпът до данните по чл. 250а, ал. 1 се осъществява при постъпило искане от ръководител на главна или специализирана дирекция по чл. 250в, ал. 1, т. 1 и 2, след писмено разрешение от председателя на Софийския градски съд или от оправомощен от него съдия, за което се издава разпореждане за предоставяне на достъп до данните. За дадените разрешения или откази в Софийския градски съд се води специален регистър, който не е публичен.

(3) За резултата от изготвената справка за данните по чл. 250а, ал. 1 компетентният орган на другата държава се уведомява по предвидения в международния договор ред.”

§ 4. Навсякъде в чл. 251а думите “чл. 251” се заменят с “чл. 250а”.

§ 5. Създават се чл. 261а и 261б:

“Чл. 261а. (1) Комисията за защита на личните данни е наблюдаващ орган относно сигурността на данните, съхранявани съгласно чл. 250а, ал. 1.

(2) Като наблюдаващ орган Комисията за защита на личните данни упражнява надзор върху дейността на предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, за спазване на следните правила при съхранение на данните по чл. 250а, ал. 1 за гарантиране тяхната защита и сигурност:

1. съхраняваните данни са от същото качество и са предмет на същата сигурност и защита като аналогичните данни в мрежата;

2. осигуряване на подходящи технически и организационни мерки, за да бъдат защитени данните от случайно или незаконно унищожаване, случайна загуба или промяна или от непозволено или незаконно съхраняване, обработване, достъп или разкриване;

3. осигуряване на подходящи технически и организационни мерки, за да се гарантира, че до данните може да има достъп само специално упълномощен персонал;

4. данните, с изключение на онези, които са били предоставени на компетентните органи и са били запазени от тях, се унищожават в края на периода за съхранение освен в изрично предвидените от закона случаи.

(3) За осъществяване на дейността си по ал. 2 Комисията за защита на личните данни има право:

1. да изисква в рамките на своята компетентност информация от предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги;

2. да дава задължителни указания, които подлежат на незабавно изпълнение.

(4) Предприятията, предоставящи обществени електронни мрежи и/или услуги, ежегодно до 31 март предоставят на Комисията за защита на личните данни в качеството ѝ на наблюдаващ орган статистическа информация за:

1. случаите, при които са били предоставени данни на компетентните органи по чл. 250б, ал. 3 и чл. 250в, ал. 1;

2. времето, изтекло от началната дата на съхранението до датата, на която компетентните органи са поискали предаването на данните;

3. случаите, при които не е могло да се отговори на искането за данни.

(5) Министерството на вътрешните работи ежегодно до 31 март изготвя обобщена статистическа информация за извършените справки за данни по чл. 250а, ал. 1, която предоставя на Комисията за защита на личните данни в качеството ѝ на наблюдаващ орган.

(6) Комисията за защита на личните данни ежегодно предоставя на Народното събрание и на Европейската комисия обобщената информация по ал. 4 и 5 в двумесечен срок от получаването ѝ.

(7) В обобщената статистическа информация по ал. 4, 5 и 6 не се съдържат лични данни.

Чл. 261б. Народното събрание чрез комисия, определена с правилника за организацията и дейността му, осъществява парламентарен контрол и наблюдение на процедурите по разрешаване и осъществяване на достъп до данните по чл. 250а, ал. 1, както и за защита на правата и свободите на гражданите срещу незаконосъобразен достъп до тези данни.”

§ 6. В чл. 305 се правят следните изменения и допълнения:

1. В ал. 1 след думата “предоставят” се поставя запетая и се добавя “въвеждат в експлоатация и поддържат”.

2. Алинея 2 се изменя така:

“(2) Техническите параметри, конфигурацията и условията за поддръжка на прихващащите интерфейси, осигурявани от предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, се съгласуват със специализирана дирекция “Оперативни технически операции” на Министерството на вътрешните работи и се утвърждават от министъра на вътрешните работи.”

§ 7. В чл. 332а думите "чл. 251" се заменят с "чл. 250а".

§ 8. В § 1 от Допълнителните разпоредби т. 53 се изменя така:

"53. "Прихващащ интерфейс" е система от мониторинг център и други входно-изходни програмно-технически средства на предприятие, осъществяващо електронни съобщения, чрез която се предоставя достъп до прихващаните електронни съобщения или данните, свързани с повикването."

ДОПЪЛНИТЕЛНА РАЗПОРЕДБА

§ 9. Този закон въвежда изискванията на Директива 2006/24/ЕО на Европейския парламент и на Съвета от 15 март 2006 г. за запазване на данни, създадени или обработени, във връзка с предоставянето на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи и за изменение на Директива 2002/58/ЕО.

ЗАКЛЮЧИТЕЛНА РАЗПОРЕДБА

§ 10. В чл. 360 от Наказателния кодекс (обн., ДВ, бр. 26 от 1968 г.; попр., бр. 29 от 1968 г.; изм. и доп., бр. 92 от 1969 г., бр. 26 и 27 от 1973 г., бр. 89 от 1974 г., бр. 95 от 1975 г., бр. 3 от 1977 г., бр. 54 от 1978 г., бр. 89 от 1979 г., бр. 28 от 1982 г.; попр., бр. 31 от 1982 г.; изм. и доп., бр. 44 от 1984 г., бр. 41 и 79 от 1985 г.; попр., бр. 80 от 1985 г.; изм. и доп., бр. 89 и 90 от 1986 г., бр. 37, 91 и 99 от 1989 г., бр. 10, 31 и 81 от 1990 г., бр. 1 и 86 от 1991 г.; попр., бр. 90 от 1991 г.; изм. и доп., бр. 105 от 1991 г., бр. 54 от 1992 г., бр. 10 от 1993 г., бр. 50 от 1995 г.; Решение № 19 на Конституционния съд от 1995 г. – бр. 97 от 1995 г.; изм. и доп., бр. 102 от 1995 г., бр. 107 от 1996 г., бр. 62 и 85 от 1997 г.; Решение № 19 на Конституционния съд от 1997 г. – бр. 120 от 1997 г.; изм. и доп., бр. 83, 85, 132 133 и 153 от 1998 г., бр. 7, 51 и 81 от 1999 г., бр. 21 и 51 от 2000 г.; Решение № 14 на Конституционния съд от 2000 г. – бр. 98 от 2000 г.; изм. и доп., бр. 41 и 101 от 2001 г., бр. 45 и 92 от 2002 г., бр. 26 и 103 от 2004 г., бр. 24, 43, 76, 86 и 88 от 2005 г., бр. 59, 75 и 102 от 2006 г., бр. 38, 57, 64, 85, 89 и 94 от 2007 г., бр. 19, 67 и 102 от 2008 г. и бр. 12, 23, 27, 32, 47, 80 и 93 от 2009 г.) се правят следните изменения и допълнения:

1. Досегашният текст става ал. 1.

2. Създават се ал. 2 и 3:

"(2) Наказанието по ал. 1 се налага и на този, който противозаконно разкрие трафични данни, каквито съгласно Закона за електронните съобщения се събират, обработват, съхраняват

или използват от предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги.

(3) Трафични данни по ал. 2 са определените в § 1, т. 71 от Допълнителните разпоредби на Закона за електронните съобщения.”

Законът е приет от 41-ото Народно събрание на ……
2009 г. и е подпечатан с официалния печат на Народното събрание.

ПРЕДСЕДАТЕЛ НА
НАРОДНОТО СЪБРАНИЕ:

(Цецка Цачева)

МОТИВИ

към проекта на Закон за изменение и допълнение на Закона за електронните съобщения

С проекта на Закон за изменение и допълнение на Закона за електронните съобщения едновременно се отстраняват сериозните проблеми, които възникнаха при работа по разкриване и разследване на престъпления, с последната редакция на нормата на чл. 251 от Закона за електронните съобщения и се въвеждат изискванията на Директива 2006/24/ЕО на Европейския парламент и на Съвета от 15 март 2006 г. за запазване на данни, създадени или обработени, във връзка с предоставянето на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи и за изменение на Директива 2002/58/ЕО.

Така разработените проектни норми въвеждат напълно Директива 2006/24/ЕО, като основните моменти са следните:

- задължават се юридическите лица, осъществяващи обществени електронни съобщителни мрежи или услуги, да съхраняват всички данни, създадени или обработени в процеса на тяхната дейност, отнасящи се до трафика на съобщенията;

- разграничават се данните относно трафика на съобщенията от тяхното съдържание (същината на кореспонденцията, независимо от формата, в която е изразена тя - материална или компютризирана) и режима, който се прилага по отношение на тях;

- гарантира се съхраняването на данните за определен период с оглед използването на всички или на част от тях за разкриването и разследването на престъпления, за които е предвидено наказание лишаване от свобода две или повече години, и на престъпления по глава девета "а" от Наказателния кодекс, както и за издирване на лица.

Предвид това, че с този закон се въвеждат изискванията на Директива 2006/24/ЕО, при дефиниране на понятието "сериозно престъпление" е отчетено Заявлението на Съвета във връзка с предложението за изменение на Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 г. относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации. Съгласно заявлението при дефиниране на понятието "сериозно престъпление" в националните си законодателства държавите членки следва да отчитат престъпленията, посочени в чл. 2, ал. 2 от Рамково решение 2002/584/ПВР на Съвета от 13 юни 2002 г. относно европейската заповед за арест и процедурите за предаване между държавите членки. В тази разпоредба попадат престъпления, наказуеми с лишаване от свобода не по-малко от 3 години, както и изрично изброените видове престъпни посегателства, за които не се изисква проверка за двойна наказуемост на деянията. Част от тези

престъпления по българския Наказателен кодекс са наказуеми с лишаване от свобода по-малко от три години. Сегашната редакция на чл. 251 също така не дава възможност за използване на данни, събрани и съхранявани от предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги за разкриване и разследване на престъпления, които не са тежки, но които влизат във фокуса на обществения интерес, като:

- приготовление и подбуждане към убийство;

- причиняване на смърт по непредпазливост;

- състави на престъпления против националното и расовото равенство, като участие в тълпа, събрана за нападение на групи от населението, отделни граждани или техни имоти във връзка с националната, етническата или расовата им принадлежност;

- престъпления против изповеданията;

- престъпления против политическите права на гражданите;

- закана с убийство;

- бягство на затворници, както и самоволно освобождаване или пускане от длъжностно лице на затворник да избяга;

- склоняване към проституция, разпространяване на порнографски материали, в т.ч. по интернет, и много други.

Липсата на възможност за незабавна реакция при тези престъпления дава възможност на извършителя да заличи уличаващата го информация и да унищожи данни, които биха могли да послужат за доказване на деянието. Поради това в законопроекта е предвидено, че за нуждите на разкриването и разследването на престъпления, за които е предвидено наказание лишаване от свобода две или повече години, тези данни ще се съхраняват. Изрично са предвидени и престъпленията по глава девета "а" от Наказателния кодекс - компютърните престъпления, тъй като в сегашната редакция за данни, свързани с такива престъпления, към момента няма възможност, а в Рамково решение 2002/584/ПВР изрично обхватът се разпростира и над престъпленията, свързани с компютри.

Третата предвидена възможност за запазване и предоставяне на тези данни е за издирване на лица. Тук не се отнасят само случаите на обвиняеми и подсъдими, укрили се от наказателно преследване, осъдени или отклонили се от изтърпяване на наказание лица, тъй като при тях тези данни са нужни във връзка с престъпление, а и с други възможни хипотези. Такива са случаите на издирване на безследно изчезнали лица или на лица, които, въпреки че не са обявени за общодържавно издирване като безследно изчезнали, в интерес на запазването на техния живот и здраве е бързото установяване на тяхното местонахождение. Като пример могат да се дадат случаите, в които хора изчезват при преходи или при падане на лавини в планината. В тези случаи няма данни за каквото и да е престъпление, но установяването на идентификатор на ползваните

клетки може да се окаже решаващо за оказването на помощ и спасяването на живота на тези лица.

Изрично е посочено, че други данни, включително разкриващи съдържанието на съобщенията, не могат да бъдат съхранявани по този ред.

В изпълнение на чл. 7, буква "б" от Директива 2006/24/ЕО в чл. 250а, ал. 3 от законопроекта е предвидено задължение за предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, да унищожат данните след изтичане на 12 месеца с изключение на тези, до които е имало достъп и са били съхранени. При достъп до данните, осъществен от специализирана дирекция "Оперативни технически операции" на Министерството на вътрешните работи чрез интерфейс, се предвижда ръководителят на органа, отправил искане за достъп, да уведомява предприятието за необходимостта от запазване на данните.

Предвидени са две възможности за осигуряване на достъп до тези данни чрез интерфейс при специализирана дирекция "Оперативни технически операции" на Министерството на вътрешните работи или директно на органите, които са поискали достъп. В случаите на директно предоставяне на информацията предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, трябва в срок до 8 часа от постъпване на разрешението от съда да предоставят справка с данните на органа, който е поискал информацията. Този срок е съобразен с определения срок в Рамково решение 2006/960/ПВР на Съвета от 18 декември 2006 г. за опростяване обмена на информация и сведения между правоприлагащите органи на държавите - членки на Европейския съюз.

Изрично е предвидено, че за нуждите на наказателното производство данните ще се предоставят на съда и на органите на досъдебното производство при условията и по реда на Наказателно-процесуалния кодекс (чл. 159) директно от предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги. По този начин се спазва принципът на непосредственост (чл. 18), поради което, когато данните са необходими за нуждите на наказателно производство, за да се използват като годен доказателствен материал, следва да са получени директно от администратора на тези данни. В случая това е съответното предприятие, предоставящо обществени електронни съобщителни мрежи и/или услуги.

По този начин осигуряването на достъп чрез интерфейс освобождава предприятията от задължението да предоставят директно и непосредствено данни на оправомощените органи с две изключения:
1) предвиденото в чл. 250б, ал. 3 задължение за предоставяне на данните директно от предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги на съда, и от органите на досъдебното производство при условията на Наказателно-процесуалния кодекс и за целите на наказателното производство, и 2) в случай че осигуреният достъп чрез интерфейс по технически причини не може да бъде използван.

Създадени са нови чл. 250а, 250б и 250в. В новите разпоредби ясно са указани условията и реда за достъп до тези данни, като е предвиден разрешителен режим. В разпоредбата на чл. 250в, ал. 1 лимитативно са посочени органите, които съобразно своята компетентност ще имат право да искат справки за данните.

Предвижда се достъпът до данните по чл. 250а, ал. 1 да се осъществява при постъпило мотивирано искане от съответния ръководител на орган по чл. 250в, ал. 1 след разпореждане от председателя на районния съд или от оправомощен от него съдия по седалище на органа. Нивото на председател на районен съд е напълно достатъчно, за да гарантира спазване на процедурата по достъп на данни. Разпоредбата на чл. 251 регламентира реда за предоставяне на такива данни на компетентен орган на друга държава, когато това е предвидено в международен договор, който е в сила за Република България. В тези случаи предвид международния елемент достъпът до данните се предвижда да бъде осъществен при постъпило мотивирано искане от ръководител на главна или специализирана дирекция по чл. 250в, ал. 1, т. 1 и 2 след писмено разпореждане от председателя на Софийски градски съд или от оправомощен от него съдия.

За дадените разрешения или откази в съответните съдилища е предвидено да се води специален регистър, който не е публичен. Специализирана дирекция "Оперативни технически операции" на Министерството на вътрешните работи ще извършва справка за данните по чл. 250а, ал. 1 при постъпване на съдебно разпореждане, което също следва да се регистрира в специален регистър, който не е публичен.

Воденето на всички тези специални регистри ще улесни осъществяването на проверка над извършените справки от органите съобразно дадените разрешения, тъй като ще могат да бъдат съпоставени данните от различни документални източници на информация, съхранявани при органи на изпълнителната и съдебната власт.

Целевият достъп до данните чрез интерфейс допълнително се гарантира с изричното изискване в специализирана дирекция "Оперативни технически операции" на Министерството на вътрешните работи справка да могат да извършват единствено длъжностни лица, писмено оправомощени от министъра на вътрешните работи.

Като гаранция, че такава справка ще бъде извършена единствено при дадено разрешение от съда, изрично е предвидено, че ръководителят на специализирана дирекция "Оперативни технически операции" на Министерството на вътрешните работи следва да дава писмено разпореждане за изготвяне на всяка искана справка, което да бъде отразено върху изготвеното искане. Предвижда се след изготвянето ѝ справката също да се подписва от ръководителя на специализирана дирекция "Оперативни технически операции" на Министерството на вътрешните работи или от писмено оправомощено от него длъжностно лице, както и да бъде регистрирана в специален регистър. След спазването на тази

процедура справката следва да бъде изпратена на определеното в искането длъжностно лице, на което да се предоставят данните.

За наблюдаващ орган относно сигурността на съхраняваните данни е определена Комисията за защита на личните данни, като по този начин се изпълнява задължението по чл. 9 от Директива 2006/24/ЕО за всяка държава членка да определи публичен орган, който да отговаря за наблюдението на прилагането на нейната територия на разпоредбите, приети от държавите членки в съответствие с чл. 7, относно сигурността на съхраняваните данни. В Директива 2006/24/ЕО изрично е указано, че този орган може да е органът по чл. 28 от Директива 95/46/ЕО, като за Република България това е Комисията за защита на личните данни.

Като наблюдаващ орган на Комисията за защита на личните данни се възлага да упражнява надзор върху дейността на предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, за спазване на следните правила за защита и сигурност при съхранението на данните по чл. 250а, ал. 1, така както изисква чл. 7 от Директива 2006/24/ЕО:

- съхраняваните данни са от същото качество и са предмет на същата сигурност и защита като аналогичните данни в мрежата;

- осигуряване на подходящи технически и организационни мерки, за да бъдат защитени данните от случайно или незаконно унищожаване, случайна загуба или промяна или от непозволено или незаконно съхраняване, обработване, достъп или разкриване;

- осигуряване на подходящи технически и организационни мерки, за да се гарантира, че до данните може да има достъп само специално упълномощен персонал;

- данните, с изключение на онези, които са били предоставени на компетентните органи и са били запазени от тях, се унищожават в края на периода за съхранение освен в изрично предвидените от закона случаи.

Предвидени са специални правомощия за Комисията за защита на личните данни при осъществяване на дейността й като наблюдаващ орган:

- да изисква в рамките на своята компетентност информация от предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги;

- да дава задължителни указания, които подлежат на незабавно изпълнение.

В изпълнение на изискването на чл. 10 от Директива 2006/24/ЕО за гарантиране от всяка държава членка, че Комисията ще получава ежегодно статистика за запазването на данни, създадени или обработени, във връзка с предоставянето на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи, това се осигурява с разпоредбата на чл. 261а. Тази статистика няма да съдържа лични данни и ще включва:

- случаите, при които информацията е била предоставена на компетентните органи в съответствие с приложимото национално право;

- времето, изтекло от датата на запазване на данните, до датата, на която компетентни органи са поискали предаването на данните;

- случаите, при които не е могло да се отговори на искането за данни.

В нормата на чл. 261а се предвижда, че както предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, така и Министерството на вътрешните работи следва да предоставят ежегодно до 31 март обобщена статистическа информация на Комисията за защита на лични данни в качеството ѝ на наблюдаващ орган.

С участието на Комисията за защита на лични данни като независим орган с контролни функции се гарантира че данните, които ще се предоставят като обобщена статистическа информация на Народното събрание и на Европейската комисия, ще бъдат такива, каквито са били предоставени от предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, и от Министерството на вътрешните работи без каквато и да е намеса от трета страна.

Предвижда се Народното събрание чрез комисия, определена с правилника за организацията и дейността му, да осъществява парламентарен контрол и наблюдение на процедурите по разрешаване и осъществяване на достъп до данните по чл. 250а, ал. 1, както и за защита на правата и свободите на гражданите срещу незаконосъобразен достъп до тези данни.

Разписването на цялата процедура е съобразено и с разпоредбата на чл. 8.2 от Европейската конвенция за правата на човека, според която намесата на държавните власти в ползването на правото на тайна на кореспонденцията се допуска единствено "в случаите, предвидени в закона, и необходими в едно демократично общество в интерес на националната и обществената сигурност или на икономическото благосъстояние на страната, за предотвратяване на безредици или престъпления, за защита на здравето и морала или на правата и свободите на другите". Така разписаните правни норми са съобразени с това правило, като въвеждат разбираеми и ясно формулирани основания както за достъпа до трафични данни, така и за процедурата за тяхното получаване. Нормите в своята цялост създават достатъчни гаранции срещу злоупотреба с правомощията на отделни органи и служби за достъп до данни, свързани с личния живот на гражданите.

Сегашните редакции на норми, които разписват задължения, са в унисон с разпоредбата на чл. 332а, в която изрично е предвидена административнонаказателна отговорност за всяко длъжностно лице от държавен орган или предприятие, предоставящо обществени електронни съобщителни мрежи и/или услуги, което наруши задълженията си или злоупотреби с данните по чл. 250а. Размерът на глобата, която може да бъде наложена като административно наказание, е от 1000 до 5000 лв.

За да се гарантира напълно защитата на правата на гражданите, свързани с обработката на т.нар. трафични данни, в чл. 360 от Наказателния кодекс се създава ал. 2, с която се предвижда възможност за реализиране на наказателна отговорност спрямо лице, което противозаконно разкрие трафични данни, каквито съгласно Закона за електронните съобщения се събират, обработват, съхраняват или използват от предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги. При тази редакция субект на престъплението може да бъде не само длъжностно лице от държавен орган или предприятие, предоставящо обществени електронни съобщителни мрежи и/или услуги, което наруши задълженията си или злоупотреби с данните по чл. 250а. При тази редакция на материалната наказателноправна норма престъплението ще бъде съставомерно и тогава, когато е извършено както от други лица извън предприятията и държавните органи, така и от други длъжностни лица, на които не са възложени задължения по отношение на тези данни. С това се гарантира и по-висока степен на наказателна защита над трафичните данни, тъй като субект на престъплението може да бъде всяко наказателноотговорно лице, което противозаконно разкрие такива данни. За постигане на яснота и гаранция за защита на правата и свободите на гражданите в чл. 360 от Наказателния кодекс се създава ал. 3, в която понятието "трафични данни" се регламентира съобразно определеното в § 1, т. 71 от Допълнителните разпоредби на Закона за електронните съобщения.

В нормата на чл. 360 от Наказателния кодекс предвиденото наказание е лишаване от свобода до една година или пробация.

В заключение следва да се отбележи, че законопроектът въвежда напълно изискванията на Директива 2006/24/ЕО на Европейския парламент и на Съвета от 15 март 2006 г. за запазване на данни, създадени или обработени, във връзка с предоставянето на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи и за изменение на Директива 2002/58/ЕО, като при неговото изготвяне са съобразени практиките по прилагането на директивата в останалите държави членки и направените в рамките на проведено обществено обсъждане предложения от страна на предприятията и неправителствени организации.

МИНИСТЪР-ПРЕДСЕДАТЕЛ:

(Бойко Борисов)