

МОТИВИ

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

След влизането в сила на Закона за изменение и допълнение на Закона за електронните съобщения (ЗЕС) (ДВ. бр. 17 от 06.03.2009 г.) възникнаха следните проблеми:

1. ЗЕС разреши данните, събрани и съхранявани от предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги да бъдат използвани само за тежки престъпления. Това е много по-тясно тълкуване на директивата на ЕС, тъй като в нея се визират "сериозни престъпления", които не са тежки по смисъла на нашето законодателство.

Определение за понятието "сериозно престъпление" е дадено в Съвместно действие от 03.12.1998 № 98/699 Правосъдие и вътрешен ред на Съвета на Европа, прието на основание чл. К 3 от Договора за Европейския съюз относно прането на пари, издирване, замразяване, изземване и конфискация на средствата и облагите от престъпление, и в рамковото решение на Съвета от 26 юни 2001 г. 2001/500, и това са престъпления, наказуеми с лишаване от свобода за повече от една година. С оглед на това степента на обществената опасност на деянията, които са визирани като "сериозни престъпления" по общностното право е по-ниска от понятието "тежко престъпление" по смисъла на чл. 93 от НК.

2. Редакцията на чл. 251 не дава възможност за използване на данните да се използват за предотвратяване, разкриване и разследване на престъпления, които не са тежки, но които влизат във фокуса на обществения интерес като приготвяне и подбуждане към убийство; причиняване на смърт по непредпазливост; престъпления против националното и расово равенство; престъпления против политическите права на гражданите; принуда на

държавен орган; бягство на затворници; обида и клевета; склоняване към проституция, разпространяване на порнографски материали, в т.ч. и по интернет; престъпления против изповеданията; престъпления против кредиторите, престъпления против свободата на събранията, митингите и манифестациите, и т.н.

Липсата на възможност за незабавна реакция при тези престъпления дава възможност на извършителя да заличи уличаващата го информация и да унищожи данни, които могат да служат за доказване на деянието.

3. Дори и при тежки умишлени престъпления като отвличания, грабежи, убийства, причинени с използване на взривни вещества, за които нормата на чл. 251 дава възможност за предоставянето на данни, ще се загуби оперативността и бързината на разследването.

4. Работата по "горещи следи" ще бъде силно затруднена, а ефективността на разследването значително намалена. Сложната процедура по Закона за СРС изисква получаване на разрешение от председателя на окръжен съд и това трябва да става по всяко време на денонощието, 365 дни в годината.

5. Едновременно с това възникват и следните сериозни организационни проблеми:

Съгласно Закона за специалните разузнавателни средства (ЗСРС) единствено специализираната дирекция "Оперативни технически операции" при МВР осигурява и прилага специалните разузнавателни средства. В Закона за електронните съобщения обаче не е посочен субектът, чрез който събраните от операторите данни ще се предоставят на органа по чл. 13 от ЗСРС, т. е. на този, който има право да ги иска.

При това положение следва, че тези данни ще се предоставят на органа по чл. 13 от ЗСРС, т. е. на службите, които имат право да ги искат, направо от оператора, който ги е събрал и съхранява.

Мотивираното искане до съда за предоставяне на данни от операторите съдържа информация, която подлежи на класификация като

държавна тайна по смисъла на чл. 25, Приложение 1, раздел II, т.3 и т. 22 от ЗЗКИ.

Следователно всички оператори, предоставящи електронни услуги, в това число и интернет доставчиците, трябва да изградят звена по сигурността на информацията, да разкрият регистратури за класифицирана информация и, разбира се, служителите им ще трябва да бъдат проучени по реда на ЗЗКИ.

Наред с това всички оператори, предоставящи електронни услуги, в това число и интернет доставчиците, трябва да създадат организация за непрекъснатата 24 часова възможност за предоставяне на данни. В противен случай няма да изпълнят задължението си по закон и ще затруднят или препятстват разкриването на престъпление, което само по себе си е престъпление по смисъла на НК – чл. 296, чл. 270, и други.

5. Не е ясно как ще се прилага предвиденият в ЗСРС ред за унищожаване на информацията. Данните, които се съхраняват от оператора, са необходими за осъществяване на неговата дейност, а съгласно чл. 31, ал. 3 от ЗСРС те следва да бъдат унищожени, ако не се използват за изготвяне на веществени доказателства.

Проектът отстранява посочените проблеми и колизии на правни норми. Той ясно дефинира структурите в Република България, които могат да искат предоставяне на събраните и съхранявани данни, като детайлизира реда за предоставянето им.

Проектът е в съответствие с духа и буквата на Директива 2006/24/ЕО на Европейския парламент и Съвета от 15 март 2006 година, както и със Съвместно действие от 03.12.1998 № 98/699 Правосъдие и вътрешен ред на Съвета на Европа, прието на основание чл. К 3 от Договора за Европейския съюз относно прането на пари, издирване, замразяване, изземване и конфискация на средствата и облагите от престъпление, и рамковото решение на Съвета от 26 юни 2001 г. 2001/500. Проектът не предвижда разход на бюджетни средства.