КОМИСИЯ ЗА ЗАЩИТА
НА ЛИЧНИТЕ ДАННИ

София 1592,
бул. „Проф. Цветан Лазаров" 2
тел.: 02/915 35 15
факс: 02/915 35 25
e-mail: kzld@cpdp.bg
www.cpdp.bg

С Т А Н О В И Щ Е

НА

КОМИСИЯТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

С РЕГ. № П-3654/2014 г.

гр. София, 04.07.2014 г.

ОТНОСНО: *Изразяване на становище по конституционно дело № 8/2014 г.*

Комисията за защита на личните данни (КЗЛД) в състав: Председател - Венцислав Караджов и членове - Цанко Цолов, Цветелин Софрониев, Мария Матева и Веселин Целков на заседание, проведено на 02.07.2014 г., разгледа преписка с вх. П-3654/16.06.2014 г. от Конституционния съд.

Преписката е по повод депозираното от Омбудсмана на Република България искане за установяване на противоконституционност на разпоредбите на чл. 250а – чл. 250е, чл. 251 и чл. 251а от Закона за електронните съобщения (ЗЕС). На Комисията за защита на личните данни е дадена възможност да представи писмено становище по делото в 20-дневен срок, считано от датата на получаване на писмото. Искането е за установяване на противоконституционност на посочените текстове от ЗЕС поради противоречие с чл. 5, ал. 4, чл. 32, ал. 1 и чл. 34 от Конституцията на Република България (КРБ).

Становище на Комисията за защита на личните данни

Във връзка с конкретните искания за обявяване на противоконституционност на изчерпателно посочените текстове от ЗЕС, и при отчитане на предметната си компетентност, Комисията за защита на личните данни изразява следното становище:

Съгласно член 15 от Директива 2002/58/ЕО за електронната неприкосновеност, държавите-членки могат да приемат законодателни мерки, за да ограничат обхвата на правата и задълженията, предвидени в член 5 (конфиденциалност на комуникациите), член 6 (данни за трафик), член 8, параграф 1, 2, 3, и 4 (показване и ограничаване на идентификацията на повикваща и свързана линия) и член 9 (данни за местонахождение, различни от данни за трафик) от Директивата. Такова ограничаване е допустимо и законосъобразно, когато то представлява необходима, подходяща и пропорционална мярка в рамките на демократично общество, за да гарантира националната сигурност (т.е. държавната сигурност), националната отбрана, обществената безопасност и превенцията, разследването, разкриването и преследването на криминални деяния или неразрешено използване на електронна комуникационна система, както е посочено в член 13, параграф 1 от Директива 95/46/ЕО (принципи, отнасящи се до качеството на данните; информация, която съответното физическо лице следва да получи; право на достъп на физическите лица; публичност на операциите по обработката). В тази връзка, директивата предвижда държавите-членки да могат, *inter alia*, да одобрят законодателни мерки, предвиждащи съхранението на данни за ограничен период, на основанията изложени в посочената разпоредба на чл. 15 от Директива 2002/58/ЕО за електронната неприкосновеност. Всички такива мерки трябва да бъдат в съответствие с общите принципи на законодателството на Общността, включително онези, упоменати в член 6, параграф 1 и 2 от Договора за Европейския съюз (зачитане на правата, свободите и принципите, определени в Хартата на основните права на ЕС и Европейската Конвенция за защита на правата на човека и основните свободи).

Въпреки, че със своето Решение от 8 април 2014 г. Съдът на ЕС обяви 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, която е транспонирана в атакуваните текстове на ЗЕС, за невалидна, на ниво ЕС продължава да действа валиден правен акт, който позволява на национално ниво съхраняване на трафични данни. В този смисъл считаме, че само по себе си задържането на трафични данни не противоречи на Конституцията на Република България, но процедурите, залегнали в Закона за електронните съобщения чрез разпоредбите на чл. 250а – чл. 250е, чл. 251 и чл. 251а, регламентиращи достъпа до тези данни, противоречат на разпоредбите на чл. 5, ал. 4, чл. 32, ал. 1 и чл. 34 от Конституцията на Република България.

Споделяме искането на Омбудсмана на Република България за обявяването им за противоконституционни поради следните съображения:

1. Цитираните разпоредби на ЗЕС противоречат на чл. 32 ал. 1 от Конституцията, съгласно която конституционна норма личният живот на гражданите е неприкосновен и всеки има право на защита срещу незаконна намеса в личния и семейния му живот и срещу посегателство върху неговата чест, достойнство и добро име.

Разпоредбата на чл. 250а, ал. 1 от ЗЕС регламентира съхраняването на данни, необходими за проследяване и идентифициране на източника на връзката; идентифициране на направлението на връзката; идентифициране на датата, часа и продължителността на връзката; идентифициране на типа връзка; идентифициране на крайното електронно съобщително устройство на потребителя или на това, което се представя за негово крайно устройство и установяване на идентификатор на ползваните клетки. Какво обхващат тези данни се конкретизира в чл. 251а от ЗЕС. От анализа на разпоредбите може да се направи заключение, че данните позволяват да се идентифицира лицето, с което потребителят комуникира, средството, с което комуникира, времето на комуникацията, както и мястото, от където се осъществява комуникацията. Данните позволяват, също така, да се установи честотата, с която потребителят комуникира за определен период с определени лица. Тези данни, както посочва и Съдът на Европейския съюз в параграф 27 от мотивите на цитираното решение, позволяват да се направят изводи за личния живот на лицата - техните навици, социални контакти, място на пребиваване и други. Безспорно това е намеса в личния живот и в свободата на кореспонденцията, които са гарантирани от КРБ.

В подкрепа на това становище могат да се посочат няколко аргумента от трайната практика на Конституционния съд (КС) досежно разпоредбата на чл. 32 ал. 1 от Конституцията.

В Преамбюла на Конституцията достойнството на личността е издигнато във върховен принцип на демократичната държава. Според конституционните разпоредби на чл. 4, ал. 2 и чл. 32, ал. 1, достойнството на личността се гарантира от държавата и всеки има право на защита срещу посегателствата, които го накърняват. Достойнството като присъщо качество на човешката личност, от което произтичат равните и неотменими права на всички членове на човешкото общество, е признато и в Преамбюла на Всеобщата декларация за правата на човека и на международни договори, по които България е страна - Международния пакт за икономическите, социалните и културните права и Международния пакт за гражданските и политическите права. Тези международни договори задължават

държавите - страни по пакта (чл. 2), да гарантират и да осигуряват упражняването на съответно признатите права **(Решение № 20 от 14 юли 1998 г. по конституционно дело № 16 от 1998 г.)**.

В друго свое решение Конституционният съд подчертава, че според чл. 8, т. 1 от Европейската конвенция за защита на правата на човека и основните свободи "всеки има право на зачитане на неговия личен и семеен живот...". Конституцията на Република България в чл. 32, ал. 1 обявява личния живот на гражданите за неприкосновен. В преамбюла на Конституцията за върховен принцип се признават правата на личността, нейното достойнство и сигурност. Според чл. 8, т. 2 от Европейската конвенция за защита правата на човека и основните свободи намеса на държавата в упражняване правото на личен и семеен живот се допуска единствено в случаите, предвидени в закона и необходими в едно демократично общество в интерес на националната и обществената сигурност, за предотвратяване на безредици или престъпления и други случаи **(Решение № 6 от 18 ноември 2004 г. по конституционно дело № 7 от 2004 г.).**

Като преход към следващата част от искането на Омбудсмана, могат да бъдат разгледани още няколко решения на КС, третиращи общо двете посочени разпоредби на чл. 32 ал. 1 и чл. 34 от Конституцията.

Наред с правото на личен живот (изр. 1 на чл. 32 ал. 1), тайната на кореспонденцията (чл. 34) и неприкосновеността на жилището са все конституционно защитени права. Става дума за един комплекс от интереси, които формират обособената интимна сфера на човека, за навлизането в която трябва да съществува преграда, съобразена с морала и манталитета на разумно мислещите хора **(Решение № 7 от 4 април 1996 г. по конституционно дело № 1 от 1996 г.).**

Друго решение от 2010 г. също може да бъде отнесено към съхраняваните данни, необходими за проследяване и идентифициране на източника на връзката; идентифициране на направлението на връзката; идентифициране на датата, часа и продължителността на връзката; идентифициране на типа връзка; идентифициране на крайното електронно съобщително устройство на потребителя или на това, което се представя за негово крайно устройство и установяване на идентификатор на ползваните клетки (чл. 250а ал. 1 от ЗЕС). Характерно за тях е, че чрез технически средства и оперативни способи се навлиза в личната сфера не само на контролирани лица, но и в личната сфера на всеки български гражданин, тъй като данните се събират и съхраняват без необходимост от предварително съдебно решение и само въз основа на факта, че едно лице използва интернет като средство на комуникация или средство за информираност. Засягането на граждански права, ползващи се

с конституционна защита (чл. 32 - 34 от Конституцията) и международно признание (чл. 8 КЗПЧОС и чл. 17 МПГПП), изисква приемането и прилагането на гаранции срещу необосновано, произволно ограничаване на неприкосновеността на личния и семеен живот, жилището, свободата и тайната на кореспонденцията. Такива са предварителния, текущия и последващ съдебен контрол **(Решение № 10 от 28 септември 2010 г. по конституционно дело № 10 от 2010 г.).**

Следва да се посочи, че правото на зачитане на личната тайна е основно конституционно право, производно от конституционния принцип на зачитане на личното достойнство (преамбюл на Конституцията) и изрично записано в редица конституционни разпоредби - чл. 30, ал. 3, чл. 32, ал. 1 и 2, чл. 34 и чл. 41, ал. 2 от Конституцията, и може да бъде ограничавана в обществен интерес само с надлежна съдебна процедура **(Решение № 18 от 14 ноември 1997 г. по конституционно дело № 12 от 1997 г.).**

2. Цитираните разпоредби на ЗЕС противоречат и на чл. 34 от Конституцията, съгласно който свободата и тайната на кореспонденцията и на другите съобщения са неприкосновени. Изключения от това правило се допускат само с разрешение на съдебната власт, когато това се налага за разкриване или предотвратяване на тежки престъпления.

Комисията за защита на личните данни счита, че ал. 1 на чл. 34 от Конституцията прогласява свободата и тайната на кореспонденцията като основно лично право. Частната сфера на индивида и публичната сфера на обществото не са абсолютно независими, а принципът за господството на правото предполага, че държавата чрез правното регулиране следва да защити и балансира всяка индивидуална свобода, която не трябва да се използва против свободата и сигурността на другите граждани и публичните интереси в гражданското общество. Разбира се, необходимостта от баланс при защитата на свободата на всички правни субекти и сигурността на обществото не обуславя възможността от въвеждане на произволни ограничения на неприкосновеността на кореспонденцията от страна на учредените власти. Ето защо още във втората алинея на същия конституционен текст учредителната власт формулира цел и установява процедура, когато пределите на свободата на кореспонденцията могат да бъдат стеснявани в условията на нормалното развитие на демократичното общество. Според разпоредбата на чл. 34, ал. 2 единствено когато информацията в кореспонденцията може да осуети разкриване или да доведе до извършване на тежки престъпления и само след като е дадено разрешение от съдебната власт, е възможно да бъде разкривана тайната на кореспонденцията. Предвиденият съдебен контрол гарантира

основните права на гражданите, прогласени от Конституцията. На второ място, ограничението на неприкосновеността на кореспонденцията не е и не може да бъде безусловно, а както предвижда чл. 34, ал. 2 на Конституцията - само за разкриване или предотвратяване на тежки престъпления. Конституционният съд в свои решения неднократно е потвърждавал разбирането си, че за да бъде в съответствие с Конституцията, разкриването на тайната на кореспонденцията трябва напълно да отговаря на изискванията за ограничаване на правото, предвидени в чл. 34, ал. 2 на основния закон на Република България **(Решение № 4 от 18 април 2006 г. по конституционно дело № 11 от 2005 г.).**

И в предходно решение, съдът подчертава, че Конституцията в чл. 34, ал. 2 установява изключителното право на съдебната власт да разреши разкриването тайната на кореспонденцията **(Решение № 1 от 10 февруари 1998 г. по конституционно дело № 17 от 1997 г.).**

3. Цитираните разпоредби от закона за електронните съобщения противоречат на чл. 5, ал. 4 от Конституцията на Република България, съгласно който международните договори, ратифицирани по конституционен ред, обнародвани и влезли в сила за Република България, са част от вътрешното право на страната. Те имат предимство пред тези норми на вътрешното законодателство, които им противоречат.

Разпоредбата на чл. 6 от Договора за Европейския съюз изрично признава на Хартата на основните права на ЕС същата юридическа сила, каквато имат Договорите. Съгласно тази разпоредба правата, свободите и принципите, съдържащи се в Хартата, се тълкуват съгласно общите разпоредби на дял VII на Хартата, уреждащи нейното тълкуване и прилагане, и като надлежно се вземат предвид разясненията в Хартата, които посочват източниците на тези разпоредби. В тази връзка чл. 52 от Хартата (обхват и тълкуване на правата и принципите) разписва, че всяко ограничаване на упражняването на правата и свободите, признати от Хартата, трябва да бъде предвидено в закон и да зачита основното съдържание на същите права и свободи. При спазване на принципа на пропорционалност ограничения могат да бъдат налагани, само ако са необходими и ако действително отговарят на признати от Съюза цели от общ интерес или на необходимостта да се защитят правата и свободите на други хора.

Атакуваните текстове от ЗЕС не отговарят на посочените изисквания, поради което считаме, че липсват основания за ограничения в упражняване на правата и свободите, прокламирани от Хартата. Поддържаме становището, че настоящата редакция на текстовете противоречи на разпоредбите на чл. 3 – Право на неприкосновеност на личността, чл. 7 –

Зачитане на личния и семейния живот, Член 8 – Защита на личните данни, изрично признати за основни права на гражданите на ЕС.

4. В допълнение към горните съображения за противоконституционност на настоящата процедура за съхранение и достъп до трафични данни подчертаваме следното:

4.1. Съхраняването на трафичните данни на сървъри, които са извън територията на България, ЕС и ЕИП противоречи на принципите на независимия контрол за защита на данните, не осигурява адекватните мерки за сигурност и не предоставя достатъчно гаранции за законосъобразното обработване на данните, гарантиране на правото на лична неприкосновеност и тайна на кореспонденцията на българските граждани. Не съществува достатъчна гаранция и възможност за проверка относно запазване на съдържанието на комуникацията, която практика трябва да бъде преустановена с обявяването на оспорваните разпоредби от Закона за електронните съобщения за противоконституционни.

Аргумент за търсене на противоконституционност на разпоредбите може да открием и в нормите на закона,определящи срока на задържането, поради тяхната прекомерност. Дългите срокове за задържане на трафични данни рефлектират и върху пропорционалността, като основен принцип в областта на защитата на личните данни. При последващо обсъждане на законодателни предложения в тази насока, законодателят следва да има предвид и необходимостта от утвърждаването на по-кратки срокове за задържане на данните.

4.2. Не на последно място, особено внимание трябва да се обърне на целта на процедурата по задържането на данни. Поради съществени несъответствия на определението за тежки престъпления в българското законодателство с разбирането за това какво е тежка престъпност на европейско ниво, считаме, че е налице противоконституционност на разглежданите текстове на ЗЕС, поради прекралено разширения обхват на процедурата на национално ниво.

Съгласно Наказателния кодекс на Република България тежко престъпление е всяко престъпление, за което е предвидено наказание лишаване от свобода повече от пет години. Други са принципите при определянето на тежката престъпност в ЕС и САЩ въз основа на което законодателство е изработена и приета 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. Считаме, че това принципно различие в законодателствата създава опасност от обработване на данни,

което не съответства на целите възприети от посочените директиви. Българското законодателство следва по-ясно да дефинира целите и обхвата на задържането на трафични данни и по нов начин следва да се определят престъпленията, по отношение на които да бъдат използвани задържаните данни с оглед на това процедурата да служи именно за противодействие на тежката престъпност. Решение в тази посока може да се търси чрез изчерпателно им изреждане в закона. Този списък следва да е съобразен с международното разбиране за тежка престъпност.

Фактическа обстановка, относима към разглежданите въпроси:

Директива 2006/24/ЕО на Европейския парламент и на Съвета от 15 март 2006 година за запазване на данни, създадени и обработени, във връзка с предоставянето на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи и за изменение на Директива 2002/58/ЕО (Директива 2006/24/ЕО за запазване на трафични данни) е приета като ответна реакция на поредицата от атентати в Ню Йорк, Лондон и Мадрид. Целта на приемането й е хармонизиране на разпоредбите на държавите членки при запазване на данни и гарантиране, че тези данни ще са достъпни за целите на предотвратяването, разкриването и разследването на тежки престъпления, съотносими на посочените атентати. С Директива 2006/24/ЕО не се разрешава запазване на съдържанието на съобщението и на търсената информация.

Още с приемането на Директива 2006/24/ЕО на ниво Европейски съюз започват дискусии във връзка с транспонирането й в отделните страни членки. В някои държави-членки (Германия, Румъния, Чехия) е обявена противоконституционност на националните актове, с които тя е транспонирана или на отделни части от тях.

Конституционният съд на Германия не обявява самото запазване на данни за противоконституционно, а законът, с който е транспонирана Директивата, доколкото той не поставя ясни ограничения на случаите, при които правоприлагащите органи могат да достъпват данни, както и не съдържа достатъчно гаранции за защита срещу нарушаване сигурността на данните.

Румънският конституционен съд определя националния закон, с който се транспонира Директивата, за неясен по отношение на обхвата и целите, с недостатъчно гаранции за защита, и на това основание определя за противоконституционен фиксирания период за задържане на данните от 6 месеца.

Чешкият конституционен съд отменя закона, транспониращ Директивата за запазване на данни отново поради неясна формулировка на текстовете.

В България Върховният административен съд с Решение № 13627 от 11.12.2008 г. отменя като незаконосъобразни текстовете на чл. 5 от Наредба № 40 от 7.01.2008 г. за категориите данни и реда, по който се съхраняват и предоставят от предприятията, предоставящи обществени електронни съобщителни мрежи и /или услуги, за нуждите на националната сигурност и за разкриване на престъпления.

На 8 април 2014 г. Съдът на Европейския съюз обяви Директива 2006/24/ЕО за невалидна. Решението на Съда на ЕС по съединени дела C-293/12 и C-594/12 е с предмет преюдициални запитвания, отправени от върховните съдилища на Австрия и Ирландия. Мотивите на Съда се свеждат до следното:

Директива 2006/24/ЕО не предвижда ясни и точни правила, определящи обхвата на намеса в основните правила, закрепени с чл. 7 и 8 от Хартата на основните права на ЕС и по-специално няма достатъчно гаранции, каквито се изискват от чл. 8, позволяващи да се осигури ефикасна защита на запазените данни срещу рискове от злоупотреба, незаконен достъп и незаконно използване на данните. В Директивата не е предвидено задължение за въвеждането на такива правила и не се гарантира незабавното унищожаване на данните в края на периода за запазването им. Не е регламентиран и въпросът за мястото на съхранение на данните на територията на Съюза по начин, който да гарантира контрола от независим орган. Поради тези причини Съдът смята, че законодателят на ЕС е надхвърлил границите на зачитането на принципа на пропорционалност по отношение чл. 7 и 8 и чл. 52, пар. 1 от Хартата.

Принципът на пропорционалност изисква актовете на институциите на ЕС да са подходящи за постигането на легитимните цели, следвани от разглежданата правна уредба, и да не надхвърлят границите на подходящото и необходимото за постигането на тези цели. В този смисъл законодателството на ЕС трябва да определи ясни и точни правила, уреждащи обхвата и прилагането на въпросната мярка и налагащи минимални гаранции, така че лицата, чиито данни са били задържани, да разполагат с достатъчно способи за ефективна защита на техните лични данни срещу злоупотреби и срещу незаконен достъп и използване на тези данни.

Въпреки решението си за обявяване на директивата за невалидна, Съдът на ЕС не приема основната цел, свързана с противодействието на тежката престъпност и тероризма, като противоречаща на основните права, залегнали в първичното законодателство на Съюза. Нещо повече, потвърждава, че това е цел от обществен интерес.

Директива 2006/24/ЕО за запазване на данните, предмет на решението на Съда на Европейския съюз, няма пряко действие на национално ниво. Нейните разпоредби са

транспонирани в законодателствата на държавите-членки. Важно е да се отбележи, че решението за невалидност на Директивата не отменя възможността за държавите-членки, произтичащи от Директивата 2002/58/ЕО относно правото на неприкосновеност в сектора на електронните комуникации (e-Privacy Directive), да уредят запазването на данни.

Съгласно член 15 от Директива 2002/58/ЕО за електронната неприкосновеност, държавите-членки могат да приемат законодателни мерки, за да ограничат обхвата на правата и задълженията, предвидени в член 5 (конфиденциалност на комуникациите), член 6 (данни за трафик), член 8, параграф 1, 2, 3, и 4 (показване и ограничаване на идентификацията на повикваща и свързана линия) и член 9 (данни за местонахождение, различни от данни за трафик) от Директивата. Такова ограничаване е допустимо и законосъобразно, когато то представлява необходима, подходяща и пропорционална мярка в рамките на демократично общество, за да гарантира национална сигурност (т.е. държавна сигурност), отбрана, обществена безопасност и превенцията, разследването, разкриването и преследването на криминални нарушения или неразрешено използване на електронна комуникационна система, както е посочено в член 13, параграф 1 от Директива 95/46/ЕО (принципи, отнасящи се до качеството на данните; информация, която съответното физическо лице следва да получи; право на достъп на физическите лица; публичност на операциите по обработката). В тази връзка, директивата предвижда държавите-членки да могат, *inter alia*, да одобрят законодателни мерки, предвиждащи съхранението на данни за ограничен период, оправдани на основанията, изложени в посочената разпоредба на чл. 15 от Директива 2002/58/ЕО за електронната неприкосновеност. Всички такива мерки трябва да бъдат в съответствие с общите принципи на законодателството на Общността, включително онези, упоменати в член 6, параграф 1 и 2 от Договора за Европейския съюз (зачитане на правата, свободите и принципите, определени в Хартата на основните права на ЕС и Европейската Конвенция за защита на правата на човека и основните свободи). В този смисъл е безспорно, че въпреки обявяването на Директива 2006/24 за невалидна, на ниво ЕС продължава да действа валиден правен акт, който позволява на национално ниво съхраняване на данни.

Към настоящия момент Комисията за защита на личните данни разполага с частична информация относно действията, предприети от някои държави-членки на национално ниво като резултат от решението на Съда.

В Холандия се провеждат дебати относно решението на Съда на ЕС. Предмет на тези дебати е дали доставчиците на електронни съобщителни мрежи и/или услуги трябва незабавно да преустановят запазването на данни вследствие решението на Съда и дали това

решение се отнася също и до данните за автоматичното разпознаване на регистрационните табели на автомобилите (ANPR-data). Към настоящия момент телекомуникационните доставчици в Холандия продължават да запазват данни. Този подход ще продължи до окончателното разглеждане в детайли на решението на Съда на ЕС. Отговорна фигура по този въпрос в Холандия е заместник-министърът на правосъдието.

Прилагането на Директивата за запазване на данни е трябвало да влезе в сила на 1 юли 2014 г. в Норвегия, което обаче е поставено под въпрос, предвид произнасянето на Съда на ЕС. Вследствие решението, правителството на Норвегия към момента поставя в режим „на изчакване“ (put on a hold) процеса по приложението на Директивата.

В Швеция, в резултат решението на Съда, националният орган за защита на данните няма да следи дали дейността на телекомуникационните оператори е в съответствие с Директивата за задържане на данни и няма да предприема действия спрямо тях.

На национално ниво, във връзка с решението на Съда и искане от 15.04.2014 г. на Омбудсмана на Република България до Конституционния съд, Комисията за защита на личните данни, в качеството си на наблюдаващ орган относно сигурността на данните (чл. 261а от Закона за електронните съобщения) инициира през м. април 2014 г. създаването на междуведомствена работна група с участието на широк кръг заинтересовани страни, а именно Върховният административен съд, Върховният касационен съд, Прокуратурата на Република България, Министерството на правосъдието, Министерството на вътрешните работи, Министерството на отбраната, Националната разузнавателна служба, Държавната агенция „Национална сигурност“, Министерство на транспорта, информационните технологии и съобщенията, Комисията за регулиране на съобщенията.

Целта на работната група е изготвянето на мотивирано предложение за законодателни промени, които да отразяват съображенията на Съда на ЕС. Предвид важността и принципния характер на решението на Съда на Европейския съюз, Комисията за защита на личните данни разчита на максимална ангажираност на компетентните български органи за изработване на съвместна позиция. Постигането на съгласуван подход в рамките на Европейския съюз е от съществено значение при подготовка на национални законодателни промени. Логично развитие е засилване на координацията между държавите-членки и Европейската комисия с оглед на възникналата ситуация с обявяването за невалиден действащ европейски акт.

В качеството си на наблюдаващ орган относно сигурността на данните и в изпълнение на чл. 261а от ЗЕС, Комисията за защита на личните данни вече трета година прави обобщение и анализ на случаите на поискан и предоставен достъп до трафични данни. От

последния анализ, който обхваща периода 01.01. - 31.12.2013 г. Комисията за защита на личните данни достигна до извода, независимо от мотивите в решението на Съда на ЕС, че от гледна точка на защитата на личните данни, настоящата редакция на ЗЕС създава предпоставки за нарушаване на принципа на пропорционалност в две направления:

1. Фактът, че оправомощените по чл. 250б, ал. 1 и чл. 250в, ал. 4 от ЗЕС органи, не отправят никакви искания за достъп до данни, свързани с интернет телефония, интернет достъп и интернет email или това става по-скоро по изключение[1], поставя под въпрос необходимостта и целесъобразността от съхраняване на този вид трафични данни, които касаят неограничен кръг български граждани ползващи интернет като средство за комуникация или средство за информация.

2. Срокът за съхранение на трафични данни съобразно действащия ЗЕС (една година) е прекомерно дълъг[2]. Установява се, че оптимално необходимата възраст на данните, е по правило 3 (три) месеца. Целесъобразно е, при бъдещи законодателни промени (вкл. на ниво ЕС) да се намали максимално допустимия срок за запазване на данните (напр. до три месеца) с възможност за удължаване до максимум 1 година по отношение на данни, за които вече е бил поискан и предоставен достъп.

В контекста на текущите дебати в ЕС относно необходимите действия след решението на Съда на ЕС, следва да се отбележи и общото виждане на Работната група по чл. 29 (висш консултативен орган на ниво ЕС в областта на защитата на личните данни)[3]. Според работната група, въпреки обявяването на Директива 2006/24 за невалидна, продължават да съществуват правни основания за задържане на данни, а именно текстовете на Директивата за електронна неприкосновеност. В случаите, в които националните законодателства предвиждат съхраняването на данни за целите на чл. 15 от тази директива, последните трябва да гарантират, че при съхраняването на данните е налице диференциация, ограничения и изключения, както и че достъпът и използването на данните от компетентните национални органи е надлежно мотивиран и ограничен, вкл. по отношение на категориите данни и засегнатите лица. Работната група призовава също държавите-членки да гарантират при

---

[1] От 98258 случаи на поискан достъп до трафични данни за 2013 г. данни за интернет достъп са поискани в 1067 случая, за интернет телефония - в 1 случай и нито един случай за интернет e-mail.

[2] От 98258 случаи на поискан достъп до трафични данни 78148 са били поискани в рамките на тримесечния период от запазване на данните ("възраст на данните"). В 10904 случаи данните са били на "възраст" от 6 месеца, считано от датата на запазването им, в 4032 – на "възраст" от 9 месеца и в 5159– на едногодишна възраст. Едва 15 на брой са случаите, в които достъп е бил осъществен в рамките на едногодишния срок за съхранение на данни, но на основание чл. 250а, ал. 5 от ЗЕС е поискано запазването им за допълнителен срок до 6 месеца, считано от датата на първоначалния достъп.

[3] Дискусиите по този въпрос в рамките на работната група са приключили. Предстоящо е обнародването на изявлението на консултативния орган.

бъдещи законодателни изменения ефективна защита срещу незаконосъобразен достъп до данните, вкл. гаранции, че данните не се съхраняват извън контрола на съответния национален орган за защита на данните каквато практика се констатира от Комисията за защита на лични данни в България.

ПРЕДСЕДАТЕЛ:

Венцислав Караджов

ЧЛЕНОВЕ:

Цанко Цолов

Цветелин Софрониев

Мария Матева

Веселин Целков