

РЕШЕНИЕ № 2
София, 12 март 2015 г.
конституционно дело № 8/2014 г.
съдия-докладчик Кети Маркова
(Обн., ДВ, бр. 23 от 27.03.2015 г.)

Конституционният съд в състав: Председател: Димитър Токушев, членове: Благовест Пунев, Пламен Киров, Красен Стойчев, Цанка Цанкова, Стефка Стоева, Румен Ненков, Кети Маркова, Георги Ангелов, Борис Велчев, Гроздан Илиев,
при участието на секретар-протоколиста Гергана Иванова, разгледа в
закрито заседание на 12 март 2015 г. конституционно дело № 8/2014 г.,
докладвано от съдията Кети Маркова.

Производството е по чл. 149, ал. 1, т. 2 от Конституцията на Република България.

Делото е образувано по искане на омбудсмана на Република България на основание чл. 150, ал. 3 от Конституцията, с което Конституционният съд е сезиран да установи противоконституционност на чл. 250а - чл. 250е, чл. 251 и чл. 251а от Закона за електронните съобщения (ЗЕС) (обн., ДВ, бр. 41/2007 г., последно изм. и доп., ДВ, бр. 14/2015 г.).

В искането си омбудсманът поддържа противоконституционност на разпоредбите на чл. 250а - чл. 250е, чл. 251 и чл. 251а ЗЕС като противоречащи на чл. 4, ал. 2, чл. 5, ал. 4, чл. 32, ал. 1 и чл. 34 от Конституцията на Република България и намира, че нарушават конституционно защитени права и свободи на гражданите. Изложено е, че оспорените разпоредби са приети със Закона за изменение и допълнение на ЗЕС (ЗИДЗЕС), обн., ДВ, бр. 17/2010 г., с който е транспонирана Директива 2006/24/ЕО на Европейския парламент и на Съвета от 15.03.2006г. 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. С тях по същество се въвежда задължение за 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, уреждат се редът и условията за достъп до тези данни и лицата, които имат право на достъп до тях. Установен е периодът на съхранение, възможността за неговото удължаване, формулирани са и целите, в изпълнение на които е създадена оспорената законодателна уредба. Вносителят

твърди, че съхраняването на трафичните данни и тяхното използване по начина и със средствата, уредени от закона, макар и да преследва законна цел в обществен интерес, по своята същност представлява неоправдана и непропорционална намеса в личния живот на гражданите, а следователно и нарушение на конституционно защитената неприкосновеност на свободата и тайната на кореспонденцията. Аргументирайки позицията си за установяване противоконституционността на оспорените разпоредби, омбудсманът се позовава на Решението от 8.04.2014 г. на Съда на Европейския съюз, разширен състав, по съединени дела C-293/12 и C-594/12, с което транспонираната със ЗИДЗЕС Директива 2006/24/ЕО е обявена за невалидна поради несъответствието ѝ с разпоредбите на чл. 7, чл. 8 и чл. 52, § 1 от Хартата на основните права на Европейския съюз (Хартата), както и на практиката на Конституционния съд.

С определение от 12.06.2014 г. Конституционният съд е допуснал искането за разглеждане по същество и като заинтересувани страни в производството по делото са конституирани: Народното събрание, президентът на Република България, Върховният касационен съд, Върховният административен съд, главният прокурор, Министерският съвет, министърът на правосъдието, министърът на вътрешните работи, министърът на транспорта, информационните технологии и съобщенията, Комисията за защита на личните данни, Комисията за регулиране на съобщенията, Националното бюро за контрол на специалните разузнавателни средства, Висшият адвокатски съвет, Съюзът на юристите в България, Българският хелзинкски комитет, Асоциацията по европейска интеграция и права на човека, Фондация „Български адвокати за правата на човека”, Фондация „Програма Достъп до информация”, Институтът за модерна политика и Асоциация „Телекомуникации”.

От постъпилите по делото писмени становища на заинтересуваните страни мотивирана позиция за основателност на искането на омбудсмана и неговото цялостно уважаване са изразили: президентът на Република България, Върховният касационен съд, Върховният административен съд, главният прокурор, министърът на транспорта, информационните технологии и съобщенията, Комисията за защита на личните данни, Фондация „Български адвокати за правата на човека”, Фондация „Програма Достъп до информация” и Институтът за модерна политика. Изложени синтезирано, в обобщен вид, съображенията в подкрепа на искането на посочените заинтересувани страни се свеждат основно до следното: Конституционните норми на чл. 32, ал. 2 и чл. 34, ал. 2 представляват изключения от регламентирани с чл. 32, ал. 1 и чл. 34, ал. 1 на основния закон права на гражданите, поради което, макар и да са уредени със закон, тези изключения не могат да излизат от установената конституционна рамка. Освен това дори и при наличието на

безспорна легитимна цел на ограничението, последното следва да се подчинява на принципите на необходимост и съразмерност. Всяка намеса в личната сфера на гражданите трябва да се осъществява по силата на ясни, точни, безпротиворечиви и подлежащи на еднозначно тълкуване законови правила, каквито характеристики считат, че оспорените разпоредби на ЗЕС нямат. Изтъква се, че чл. 34, ал. 2 от Конституцията допуска като изключение установеното по силата на ал. 1 основно право на гражданите на неприкосновеност на свободата и тайната на кореспонденцията и на другите съобщения само когато това се налага за разкриване или предотвратяване на тежки престъпления, докато с оспорената норма на чл. 250а ЗЕС е предвиден един доста по-широк обхват. Освен това разглежданата мярка, представляваща по съществото си сериозна намеса в личната сфера на индивида, макар и формално предвидена в закон и създадена да преследва и осигури легитимна цел, трябва да е и пропорционална на съответната цел, т. е. да не е прекомерна. Именно това изискване не е спазено според посочената група заинтересувани страни, които излагат аргументирани съображения в подкрепа на тезата си за прекомерност на намесата в твърде деликатната лична сфера на гражданите.

Законодателната уредба, с която е транспонирана Директива 2006/24/ЕО, не съдържа и достатъчно надеждни и убедителни гаранции, че няма да се допуснат злоупотреби както от страна на търговците (предприятията), предоставящи съответните услуги, така и от държавните органи, имащи достъп до генерираните трафични данни. Посочват също, че съхраняването на един толкова значителен обем данни в продължителен период (от една година, с възможност за удължаване до шест месеца), позволява да се направи достатъчно точен личностен профил за всеки, когато неговите контакти, местонахождение и придвижване се подложат на съответния анализ и оценка, а това представлява драстично вмешателство в конституционно защитения личен живот на хора, които никога и по никакъв начин не са участвали и не са били съпричастни към извършването на каквито и да било престъпления. Ето защо не може да се намери разумно основание по отношение на тях да бъде прилагана подобна мярка, легитимирана като средство за борба с тежката престъпност, още по-малко да се приеме, че същата е необходима. При тези съображения, обосноваващи разбирането им, че въведените с оспорените разпоредби ограничения на неприкосновеността на личния живот и на свободата на кореспонденцията и другите съобщения не могат да бъдат квалифицирани като наложителното, подходящо и съразмерно правно средство за постигане на целения правен резултат, посочените заинтересувани страни поддържат, че нормите на чл. 250а - 250е, чл. 251 и чл. 251а ЗЕС следва да бъдат обявени за противоконституционни.

Като подробно е обосновал изложеното виждане, в своето писмено становище

Висшият адвокатски съвет е изразил и алтернативна позиция – ако Конституционният съд не сподели аргументите за цялостна противоконституционност на оспорените разпоредби, да се произнесе, като приеме частичната основателност на искането на омбудсмана. Поддържа, че за противоконституционни следва да бъдат обявени най-малко чл. 250а, ал. 2 в частта „и престъпления по чл. 319а - чл. 319е от Наказателния кодекс, както и за издирване на лица”, и чл. 250б, ал. 1, т. 3 и 4 ЗЕС. Водещите аргументи в тази част на становището се свеждат на първо място до наличието на формално противоречие между посочената част от текста на чл. 250а, ал. 2 ЗЕС с чл. 34, ал. 2 от Конституцията и, второ – до констатацията, че визираните в чл. 250б, ал. 1, т. 3 и 4 ЗЕС органи нямат никаква компетентност и правомощия в областта на разкриването и разследването на тежки престъпления.

Министерството на вътрешните работи и Националното бюро за контрол на специалните разузнавателни средства поддържат, че искането на омбудсмана е изцяло неоснователно, тъй като оспорваните разпоредби на ЗЕС изцяло отговарят на изискванията на пропорционалност и съразмерност, а срокът от 12 месеца е разумен и осигуряващ ефективност на въведената със закона ограничителна мярка, доколкото с нея се постига една легитимна цел – защита на обществената сигурност и законосъобразното провеждане на наказателното производство. Освен това са предвидени органи и механизми за контрол, които създават достатъчно гаранции срещу възможни злоупотреби от отделни органи и служби във връзка с достъпа им до данните за личния живот на гражданите (напр. чл. 332а ЗЕС, уреждащ административнонаказателна отговорност за длъжностни лица или предприятия, предоставящи електронни съобщителни мрежи и/или услуги, за нарушения на задължения или злоупотреба с данни по чл. 250а ЗЕС – глоба в размер от 1000 до 10 000 лв.).

Съюзът на юристите в България намира, че атакуваните текстове на ЗЕС не попадат под защитата на чл. 32 и чл. 34 от Конституцията, доколкото не става дума за огласяване или създаване на каквато и да е публичност по отношение на данните, свързани с личния живот на гражданите. Още по-малко съхраняването на такива данни би могло да бъде окачествено като нарушение на тайната на кореспонденцията, а доводите за наличие на непропорционална и неоправдана намеса в правата на гражданите представлява въпрос на законодателна целесъобразност, поради което и не може да бъде предмет на преценка за конституционосъобразност.

Комисията за регулиране на съобщенията е представила становище, че не е в позиция и с компетентност да даде оценка за съответствието на оспорените от омбудсмана разпоредби на ЗЕС с Конституцията, включително и относно пропорционалността на намесата в личния живот на гражданите, тъй като тези въпроси не са свързани с дейността на Комисията като

секторен регулатор.

Останалите конституирани страни не са депозирали писмени становища по искането.

Конституционният съд, като обсъди доводите в искането, с което е сезиран, изложените в него съображения, становищата на страните и релевантната правна уредба, за да се произнесе, взе предвид следното:

Предмет на проверка за конституционност са нормите на чл. 250а - чл. 250е, чл. 251 и чл. 251а ЗЕС, които гласят следното:

Чл. 250а. (1) Предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, съхраняват за срок от 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) Данните по ал. 1 се съхраняват за нуждите на разкриването и разследването на тежки престъпления и престъпления по чл. 319а - 319е от Наказателния кодекс, както и за издирване на лица.

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

(4) Предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, са длъжни да унищожат данните след изтичането на срока по ал. 1.

(5) За данни, до които е осъществен достъп и са били съхранени, ръководителят на органа, отправил искане за достъп, може да поиска предприятието, което ги е предоставило, да ги запази за срок не по-дълъг от 6 месеца, считано от датата на предоставяне.

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

Чл. 250б. (1) Право да искат извършване на справка 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 "Национална полиция", Главна дирекция "Борба с организираната престъпност" и териториалните ѝ звена, Главна дирекция "Гранична полиция" и териториалните ѝ звена, дирекция "Вътрешна сигурност", Столичната дирекция на вътрешните работи и областните дирекции на Министерството на вътрешните работи;*
- 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 мотивирано писмено искане от съответния ръководител на органите по ал. 1, съдържащо:

- 1. правното основание и целта, за която е необходим достъпът;*
- 2. регистрационния номер на преписката, за която е необходимо извършване на справка;*
- 3. данните, които следва да се отразят в справката;*
- 4. периода от време, който да обхваща справка;*
- 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.

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

(2) Разпореждането по ал. 1 задължително съдържа:

- 1. данните, които следва да се отразят в справката;*
- 2. периода от време, който да обхваща справка;*
- 3. определеното длъжностно лице, на което да се предоставят данните;*
- 4. име, длъжност и подпис на съдията.*

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

(4) 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.

(5) Достъпът до данни по чл. 250а, ал. 1, които се отнасят до председател на районен съд, негов възходящ, низходящ, брат или сестра, съпруг или лице, с което се намира във фактическо съпругеско съжителство, се осъществява след разрешение от председателя на съответния окръжен съд.

Чл. 250г. (1) Предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, са длъжни да осигурят възможност 24 часа в денонощието, 7 дни в седмицата за постъпване на разпореждането по чл. 250в, ал. 1 и по чл. 251, ал. 2.

(2) Ръководителите на предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, изпращат на Комисията за регулиране на съобщенията списък, в който се посочват:

- 1. актуален адрес за получаване на разпореждането по чл. 250в, ал. 1 и по чл. 251, ал. 2;*
- 2. име, презиме, фамилия и длъжност на оправомощените длъжностни лица, които да получават разпорежданията по чл. 250в, ал. 1 и по чл. 251, ал. 2, както и телефони за връзка с тях; при промяна на данните в срок до 24 часа се уведомява писмено Комисията за регулиране на съобщенията и нейният председател незабавно предоставя списъците на ръководителите на органите по чл. 250б, ал. 1.*

Чл. 250д. (1) Предприятията, предоставящи обществени електронни съобщителни

мрежи и/или услуги, извършват 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.

(2) Предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, във възможно най-кратък срок, но не повече от 72 часа от постъпването в предприятието на разпореждането за достъп по чл. 250в, ал. 1 и по чл. 251, ал. 2, изпращат данните на длъжностното лице по чл. 250в, ал. 2, т. 3. Министърът на вътрешните работи или писмено оправомощени от него длъжностни лица могат да определят конкретен срок, в който данните да бъдат изпратени.

(3) Справка за данните по чл. 250а, ал. 1 в предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, могат да извършват единствено длъжностни лица, писмено оправомощени от съответния ръководител на предприятието.

(4) След изготвянето ѝ справката се подписва от ръководителя на съответното предприятие, предоставящо обществени електронни съобщителни мрежи и/или услуги, или от писмено оправомощено от него длъжностно лице. Справката се регистрира в специален регистър и се изпраща на определеното в разпореждането длъжностно лице, на което да се предоставят данните.

(5) При наличие на възможност разпореждането на съдията и справката по ал. 4 се изпращат по електронен път при спазване изискванията на Закона за електронното управление и Закона за електронния документ и електронния подпис.

Чл. 250е. Справката по чл. 250д, ал. 4, която не се използва при образуване на досъдебно производство, независимо дали представлява класифицирана информация, се унищожават в 6-месечен срок от датата на получаването ѝ от тричленна комисия в състав, определен от съответния ръководител на органите по чл. 250б, ал. 1, за което се изготвя протокол.

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. 250б, 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.

Чл. 251а. (1) Данните по чл. 250а, ал. 1, т. 1 са при:

1. обществена телефонна услуга - телефонният номер на викация и данни за идентифициране на абоната или потребителя;

2. интернет достъп, електронна поща по интернет и интернет телефония - идентификатор, определен за потребителя, идентификатор на потребителя и телефонен номер, определени за всяко съобщение, влизащо в обществената телефонна мрежа, данни за идентифициране на абоната или потребителя, за когото са определени IP адрес, идентификатор на потребителя или телефонен номер в момента на връзката.

(2) Данните по чл. 250а, ал. 1, т. 2 са при:

1. обществена телефонна услуга - набран номер (викан телефонен номер) и в

случаите на допълнителни услуги, като пренасочване или прехвърляне на повикването, номер или номера, към които е маршрутизирано повикването, и данни за идентифициране на абоната или потребителя;

2. електронна поща по интернет и интернет телефония - идентификатор на потребителя или телефонен номер на получателя/ите на интернет телефонно повикване, данни за идентифициране на абоната или потребителя и идентификатор на получателя, за когото е предназначено съобщението.

(3) Данните по чл. 250а, ал. 1, т. 3 са:

1. при обществена телефонна услуга - дата и час на началото и края на връзката;

2. за интернет достъп, електронна поща по интернет и интернет телефония - дата и час на влизане и излизане в/от услугата интернет достъп, основаващи се на определена часова зона, заедно с IP адреса, динамичен или статичен, определен за връзката от доставчика на услугата интернет достъп, и идентификатора на абоната или потребителя, дата и час на влизане и излизане в/от услугата електронна поща по интернет или интернет телефония, основаващи се на определена часова зона.

(4) Данните по чл. 250а, ал. 1, т. 4 са:

1. видът на използваната обществена телефонна услуга;

2. използваната интернет услуга при електронна поща по интернет или интернет телефония.

(5) Данните по чл. 250а, ал. 1, т. 5 са при:

1. фиксирана телефонна услуга - за викация и викания телефонен номер ;

2. обществена телефонна услуга, предоставяна чрез мобилна наземна мрежа - за викащ и викан телефонен номер; международен идентификатор на викация мобилен абонат (IMSI); международен идентификатор на викания мобилен абонат (IMSI); международен идентификатор на викащото мобилно крайно електронно съобщително устройство (IMEI); международен идентификатор на виканото мобилно крайно електронно съобщително устройство (IMEI); в случай на предплатени услуги - дата и час на началното активиране на услугата и етикет за местоположение - идентификатор на клетката, от която е активирана услугата и за идентифициране на абоната или потребителя;

3. интернет достъп, електронна поща по интернет и интернет телефония - викацият телефонен номер за комутируем достъп, цифрова абонатна линия (DSL) или друга крайна точка на инициатора на връзката.

(6) Данни по чл. 250а, ал. 1, т. 6 са административни адреси на клетки на мобилна наземна електронна съобщителна мрежа, от които е генерирано или в които е терминирано повикване.

Конституционният съд взе предвид, че с искането се оспорва закон, с който се нарушават основни лични права на гражданите, най-общо формулирани като право на неприкосновеност на личния живот и на свободата и тайната на кореспонденцията и на другите съобщения – чл. 32, ал. 1 и чл. 34, ал. 1 от Конституцията, които същевременно са обект на защита и от редица международноправни актове, по които България е страна – Всеобщата декларация за правата на човека – чл. 12, Международния пакт за граждански и

политически права – чл. 5 и чл. 17, Хартата на основните права на Европейския съюз – чл. 7, чл. 8 и чл. 52, § 1, и Конвенцията за защита на правата на човека и основните свободи (КЗПЧОС) – чл. 8. С оглед идентичния характер и съдържание на тези права в тяхната регламентация на конституционно ниво и в текстовете на посочените международни актове, последните два от които представляващи и част от европейското законодателство, Съдът счита, че осъществявайки нормения контрол за конституционност по отношение на оспорената уредба на ЗЕС, ще следва да обсъжда и тези международноправни норми в светлината на прогласените от тях принципи и стандарти, наред с практиката по тяхното прилагане на Европейския съд по правата на човека (ЕСПЧ). Този подход не е прецедент в практиката на Конституционния съд, доколкото е бил възприет и с други предходни негови решения (вж. Решение № 7/1996 г. по к.д. № 1/1996 г., Решение № 1/1998 г. по к.д. № 17/1997 г., Решение № 2/1998 г. по к.д. № 15/1997 г., Решение № 4/2006 г. по к.д. № 11/2005 г., Решение № 3/2011 г. по к.д. № 19/2010 г., Решение № 1/2014 г. по к.д. № 22/2013 г., Решение № 3/2004 г. по к.д. № 3/2004 г., раздел V, т. 7).

Релевантните обстоятелства, които следва да бъдат взети предвид и са от съществено значение за формиране на изводите по същество по настоящото дело, са следните:

Оспорените от вносителя разпоредби на чл. 250а - чл. 250е, чл. 251 и чл. 251а ЗЕС са приети със ЗИДЗЕС с ДВ, бр. 17/2010 г. и са в сила от 10.05.2010 г. С този закон е транспонирана Директива 2006/24/ЕО на Европейския парламент и на Съвета от 15.03.2006 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.

С решение от 8.04.2014 г., постановено по съединени дела C-293/12 и C-594/12, с предмет преюдициални запитвания на основание чл. 267 ДФЕС Съдът на Европейския съюз (СЕС), голям (разширен) състав е обявил Директива 2006/24/ЕО на Европейския парламент и на Съвета от 15.03.2006 г. за невалидна.

От прегледа на нормотворчеството в областта на запазването и съхраняването на данните от трафика, защитата на основни права на гражданите в национален и европейски мащаб, включително с оглед постигнатия резултат от проведените съдебни процедури на контрол се налагат няколко извода, които Съдът постави в основата на по-нататъшните си разсъждения по съществуващото на настоящия конституционен спор:

1. Обявяването на Директива 2006/24/ЕО за невалидна с цитираното по-горе решение на СЕС не може да има за последица автоматичната отмяна или неприлагане на оспорените законови разпоредби на вътрешното право, с които тя е транспонирана. С нейното обявяване

за невалидна се прекратява единствено задължението на държавите-членки да въведат нейните изисквания в своето вътрешно законодателство. Приетият закон продължава да действа до момента, в който бъде отменен или изменен по надлежния ред от националния законодателен орган или бъде обявен за противоконституционен от Конституционния съд.

2. Въведеният с разпоредбите на чл. 250а - чл. 250е, чл. 251 и чл. 251а ЗЕС режим на запазване, съхранение, достъп, експлоатация и унищожаване на данни от трафика по своя характер и същност безспорно представлява намеса в основни, конституционно защитени права на гражданите и следователно следва да се третира като изключение от правилата, установени с конституционните норми на чл. 32, ал. 1 и чл. 34, ал. 1. Тези права не са абсолютни. Съгласно изискванията на чл. 32, ал. 2 и чл. 34, ал. 2 от Конституцията изключенията следва да са уредени от закон; да се допускат само с разрешение на съдебната власт; и само когато това се налага за разкриване и предотвратяване на тежки престъпления. В случая оспорената уредба е създадена със закон и следователно изпълнява формално първото конституционно изискване.

3. Налице е противоречие с Конституцията на разпоредбата на чл. 250а, ал. 2 ЗЕС относно целта на съхраняването на данни от трафика, а именно за нуждите на разкриването и разследването на престъпления по чл. 319а - 319е от Наказателния кодекс (НК), както и за издирване на лица. Изключението по чл. 34, ал. 2 от Конституцията е допустимо само когато интервенцията в сферата на неприкосновеността на свободата и тайната на кореспонденцията и на другите съобщения се налага за разкриване и предотвратяване на тежки престъпления и то не може да бъде тълкувано и прилагано разширително. Следователно разпоредбата в частта ѝ „и престъпления по чл. 319а - 319е от Наказателния кодекс”, които не са тежки по смисъла на чл. 93, т. 7 НК, с изключение само на това по чл. 319а, ал. 5 НК, доколкото предвидените в санкционните части на съответните норми на особената част на НК за тях наказания не са лишаване от свобода за повече от пет години, доживотен затвор или доживотен затвор без замяна, е противоконституционна. Казаното се отнася и за последната хипотеза – издирване на лица, която самостоятелно няма как да бъде отнесена към конституционната рамка на ограничението освен в случаите, когато издирваното лице е жертва или извършител на тежко престъпление.

Тук следва да се посочи, че българският законодател съществено е разширил и надхвърлил дори изискванията на силно критикуваната в теорията и практиката Директива 2006/24/ЕО (чл. 1, § 1), която, третирайки достъпа до данни от трафика, го ограничава единствено до „разследването, разкриването и проследяването на сериозни престъпления, както те са определени в националното право на всяка държава-членка”. Безспорно,

приложима в случая е нормата, установяваща легалната дефиниция на понятието „тежко престъпление” по смисъла на НК. Интерпретирайки нормативните разрешения, приети с обсъжданата Директива, при съпоставянето им с принципите на Хартата и КЗПЧОС, за да обоснове тезата си за нейните несъвършенства, в решението си СЕС също борави с критерия за тежко престъпление, в обхвата на който безусловно попадат формите на организираната престъпност и тероризма.

4. Подходът на разширяване на приложното поле на транспонираната директива е използван от законодателя и при очертаването на кръга на субектите, които имат право да искат извършване на справка за данните по чл. 250б, ал. 1 ЗЕС. Този кръг Конституционният съд намира за твърде широк, а действащата уредба обективира съществен конституционен проблем. Съобразяването с установения конституционен стандарт всяко ограничение на основни права на гражданите да е уредено със закон включва не само основанието, но също така органите и процедурите, по които ще се изпълнява съответната въведена мярка. В този смисъл е задължително легитимираният субект да разполага с изрично възложена му, и то със закон, компетентност по разкриване и разследване на тежки престъпления, т.е. правомощия, свързани с преследваната със закона легитимна цел. На това изискване обаче не отговарят всички субекти от кръга на визираните в чл. 250б, ал. 1 ЗЕС. Това дава основание да се приеме наличието на противоконституционност на посочената разпоредба съобразно критериите, заложи в чл. 32, ал. 2 и чл. 34, ал. 2 от Конституцията.

5. Конституционното изискване за контрол от съд или друг независим орган изобщо отсъства в процедурата, уредена по чл. 250а, ал. 5 ЗЕС. В тази хипотеза органът, отправил искане за достъп, контактува директно с предприятието, предоставило данните, и без съответното разрешение постига на практика едно продължаване на запазването им за срок до шест месеца, който сам по себе си е значителен.

Също така липсва уреден контрол и върху унищожаването на издадена справка с данни по чл. 250д, ал. 4 ЗЕС, която не се използва за образуване на досъдебно производство – чл. 250е ЗЕС. Ето защо разпоредбите на чл. 250а, ал. 5 и чл. 250е ЗЕС също се оказват несъответни на Конституцията. Несъвършенствата на съдебния контрол, така както той е уреден с оспорените законови текстове, дали и доколко той реално и пълноценно изпълнява предназначението си да не бъдат допускани противозаконни вмешателства в сферата на личния живот на гражданите е въпрос, с който Съдът ще се занимае по-нататък.

6. Конституционният съд намира за необходимо изрично да изтъкне, че само по себе си събирането и запазването на данни от телекомуникационен трафик не представлява дейност, забранена от Конституцията или такава, която дефинитивно следва да бъде отречена

и поради несъвместимост с основните права на гражданите, регулирани от Хартата и КЗПЧОС. Този извод следва от комплексната оценка на вида и характеристиката на подлежащите на запазване данни, от една страна, и, от друга – наличието на безспорна легитимна цел, която е от общ интерес както за Съюза, така и за националните държави.

Анализът на създадената с оспорените разпоредби конфигурация на предвидените мерки и средствата за тяхното осъществяване ясно показва, че генерираните и запазени данни за определения със закона период от 12 месеца съдържат пълната информация кой, с кого, кога, как, с кое конкретно устройство и къде точно е осъществявал комуникациите си. Тук следва да се внесе изричното уточнение, че в обхвата на подлежащите на съхраняване по силата на закона данни не влиза самото съдържание на кореспонденцията, т.е. не става дума за запазване на записи на разговори, текстови съобщения и т.н. Въпреки това генерирането и запазването на описания значителен обем данни без повод, и то за фиксиран в закона достатъчно продължителен срок, по отношение на един неперсонифициран кръг лица (практически всички, използващи различните съвременни комуникации като форма на общуване) дава възможност да се направят достатъчно обосновани и точни заключения за личния живот на хората, обичайните им действия, навиците им в ежедневието, включително контакти, социална среда, местопребиваване – постоянно и временно, пътувания, с тяхната честота, време и точни дестинации. В тази посока на разсъждения следва да се съобрази също, че при подробно и детайлно оценяване и анализ на генерираните данни от телекомуникационен трафик могат да се изведат и достатъчно съдържателни изводи дори за интимния живот на хората, сексуалната им ориентация, здравословното им състояние (психично и/или соматично), професионалната им или политическа принадлежност, активностите или пристрастията им, евентуалните им проблеми с правосъдието. Проследяването на данните в един продължителен период позволява да се достигне още по-далеч – до личните предпочитания на индивида, дори неговите склонности, увлечения и слабости. А това означава само едно: осигурена напълно реална възможност за съставянето на достатъчно подробен и ясен профил на личността не само без нейното изрично съгласие, но и без тя изобщо да има представа или дори да подозира, че това се случва в действителност. Комплексната оценка на всички аспекти на проблема предполага два допълнителни въпроса или по-точно други две негови страни: за съдбата на професионалната тайна и нейната защита; и второ: защитено и гарантирано в достатъчна степен ли е правото на личността суверенно и по собствена преценка да решава дали и в какъв обем да прави определени факти и обстоятелства от неприкосновения си личен живот публично достояние, или най-малкото на отделни други субекти – т.нар. право на информационно самоопределение.

Следващият въпрос, който следва да бъде обсъден, е допустима и конституционно търпима ли е тази намеса в основните права на гражданите, предвид така очертаните ѝ параметри. Както вече се посочи по-горе, запазването на данни от целия телекомуникационен трафик (фиксирана и мобилна телефония, интернет достъп, електронна поща по интернет и интернет телефония) без повод и с цел квалифицирана употреба за нуждите на предотвратяването, разкриването и разследването на тежки престъпления не може дефинитивно да се отрече. То не може да се третира като противоконституционно, ако конституционната проверка установи, че са спазени изискванията ограничението да е уредено със закон, да е в рамките на предвиденото с основния закон изключение, да е подчинено на легитимна/и цел/и от общ интерес, каквито несъмнено представляват борбата с тежките престъпления, повишаването на обществената сигурност, борбата с международния тероризъм и опазването на международния мир и сигурност, както и да е съобразен принципът за пропорционалност.

Особено важно е, че част от престъпленията не биха могли да бъдат убедително разкрити и пълноценно разследвани без изследване и анализ на трафичните данни (напр. деянията, свързани с детска порнография, трафик на хора и др.), поради което е неприемливо предварителното отричане на въведените с оспорените разпоредби мерки. За постигането на така формулираните легитимни цели трябва да е необходимо и подходящо именно такова запазване на данните в условията на демократичното общество, при което намесата да не е прекомерна съобразно принципа на пропорционалността, с чиято същност, съдържание и критерии Конституционният съд многократно се е занимавал (вж. напр. Решение № 7/1996 г. по к.д. № 1/1996 г., Решение № 20/1998 г. по к.д. № 16/1998 г., Решение № 1/2002 г. по к.д. № 17/2001 г., Решение № 5/2003 г. по к.д. № 5/2003 г., Решение № 15/2010 г. по к.д. № 9/2010 г., Решение № 2/2011 г. по к.д. № 2/2011 г., Решение № 13/2012 г. по к.д. № 6/2012 г.).

Предмет на множество решения и богата прецедентна практика на ЕСПЧ е решаването на въпроса за рамката на възможната и допустима намеса на държавата в основните човешки права от гледна точка на тяхното съдържание в контекста на същността и различните проявни форми на принципа на пропорционалността (вж. в т.с.м. Решението по делото С и Марпър срещу Обединеното кралство/S and Margaret v. U. K., 2008 г., Малоун срещу Обединеното кралство/Malone v. U.K., 1984 г., Вебер и Саравия срещу Германия/Weber and Saravia v. Germany, 2006 г., Аман срещу Швейцария/Aman v. Switzerland, 2000 г., Асоциация за европейска интеграция и права на човека и Екимджиев срещу България, 2008 г.).

За преценката дали и доколко предвидената с оспорената законодателна уредба мярка, представляваща намеса в сферата на личния живот на гражданите, е пропорционална на

защитаваната цел, е наложително да се обсъди още един особено съществен довод в искането на омбудсмана, подкрепен и в голяма част от становищата на заинтересуваните страни – че на запазване подлежат абсолютно всички данни от телекомуникационен трафик, т.е. засегнати практически са всички граждани, осъществяващи комуникации, а не само онези, за които има данни или най-малкото улики, че са извършили тежко престъпление, че са съпричастни с организации на международния тероризъм и т.н.

Основното възражение, което се изтъква в тази връзка е, че преследването на формулираната легитимна цел не може да бъде постигано с цената на една толкова съществена намеса в основните права на хора, нямащи нищо общо с деянията, към чието предотвратяване, разкриване и разследване е насочено предвиденото средство. Този дисбаланс не може да бъде отречен, защото е вярно, че на запазване подлежат генерираните данни от телекомуникация по отношение на всички лица, а не само тези на заподозрените или извършителите на тежки престъпления. Вярно е обаче също, че извън коментиранията мярка практически не съществува друг способ, който, от една страна да бъде насочен само към тези, чието поведение е или би могло да бъде предмет на наказателно преследване, и, от друга – да може да осигури необходимите за целите на разследването достатъчно сведения за авторите на тежки престъпления, за техните връзки, контакти, съучастници, финансиране, местонахождение, ползвани устройства, придвижване, и то основно отнасящи се за времето, предшестващо престъпното деяние. Казус, илюстриращ позицията на съда по този въпрос, би възникнал в случай, когато например извършител на терористичен акт, който до момента на извършване на деянието не е попадал в информационните масиви на полицията във връзка с други предходни свои криминални прояви, за да се е налагала проверка на данни от неговата комуникация, бъде заловен на местопрестъплението. Ако оспорената мярка не съществуваше, за да вменява на предприятията, предоставящи услугите, запазване на данните за целия протичащ трафик, то генерирането и проследяването им по отношение на това лице би могло да започне едва след като извършеното престъпление вече е факт и самоличността на дееца е установена. Ясно е, че в такъв случай информация по горепосочените въпроси, свързани с подготовката, организацията, самото извършване на престъплението и евентуалните съучастници, е невъзможно да бъде събрана, защото ще обхваща само периода от време, следващ престъплението и следователно няма как да обслужи разследването.

В този смисъл съпоставката на защитаваната цел и приложеното средство предполага извода, че по своята същност въведената мярка принципно се оказва съответна, необходима и подходяща, включително и през призмата на критерия за съразмерност на ограничението.

Не така обаче стои въпросът за срока на нейното експлоатиране, заложен в чл. 250а,

ал. 1 ЗЕС – 12 месеца, който при съобразяване на конкретната обществено-политическа ситуация Съдът оценява като несъразмерно дълъг и съществено надхвърлящ необходимото за постигане на дефинираните цели. Натрупването на едногодишна база данни от комуникационен трафик позволява тяхното използване не само за изготвянето на подробен личностен профил (с всички проблеми, които това създава), но и постигане на точна и детайлна диференциация на трайните, обичайни, инцидентни прояви на конкретното лице, неговите контакти, увлечения, интереси, включително с отграничаването на тези, представляващи прецедент в неговото поведение и реакции, а също и систематизиране по различни критерии на местата, които посещава трайно, често, рядко или инцидентно, както и точна идентификация на лицата, с които го прави. По същата схема могат да бъдат категоризирани и разграничени и неговите контакти – лични, служебни, професионални, културни и т.н., и то с оглед спецификата на данните – с една висока степен на точност по отношение интензитета на тяхното осъществяване. Очевидно е, че този срок съдържа всички белези на несъразмерност с целта на въведената мярка, което съществено рефлектира върху оценката за конституционност на целия законов режим на запазване на данните, достъпа до тях и възможното им използване.

По тези съображения Конституционният съд счита, че прекомерно дългият срок на запазване на данните самостоятелно компроментира конституционносъобразността на приетата мярка като цяло, тъй като при тази си регламентация, съобразно предвидения период на ограничението, тя се явява непропорционална.

С решението си от 2.03.2010 г., 1 BvR 256/08, 1 BvR 263/08 и 1 BvR 586/08 Федералният конституционен съд на Германия, Първи сенат се е произнесъл по конституционността на аналогични разпоредби във вътрешното законодателство на страната, отнасящи се до запазването на данни от телекомуникационен трафик. Заклучил е, че запазването на данните не е поначало неоправдано от конституционно гледище, когато е в границите на поставената легитимна цел и във връзка с критерия за пропорционалност. В този смисъл е счел, че мярката не попада под стриктна забрана, каквато би била налице само когато съхраняването на данните е за неопределени или неподлежащи на определяне цели. Въведеният с проверявания приложим германски закон 6-месечен срок на запазване на данните Федералният конституционен съд е намерил за оправдан, макар и фиксиран на приемливата с оглед принципа на пропорционалност горна граница.

Въведеният с оспорените разпоредби на ЗЕС режим на запазване на данните от телекомуникационния трафик страда от редица други несъвършенства и пороци, които също се оказват несъвместими с конституционната граница на допустимата намеса в сферата на

основните права. За да бъде оправдана, нейната материалноправна и процесуалноправна уредба трябва да съдържа ясни, точни и недвусмислени основания и процедури, които да осигуряват достатъчно сериозни и надеждни гаранции, че достъпът на съответните национални органи до запазените данни ще бъде използван само за целите на предотвратяването и разкриването на тежки престъпления и ще обслужва единствено наказателните производства, водени за такива престъпления. Казано с други думи, правната уредба трябва да създава и гарантира сигурност у гражданите, че са изключени всякакви злоупотреби с техните данни както от страна на държавните органи, на които е осигурен достъп до тях, така от търговските дружества (предприятията), предоставящи съответните съобщителни мрежи и услуги, които всъщност ги съхраняват.

Законодателното решение за регламентиране на съдебната санкция за получаване на достъп до трафичните данни е принципно правилно и съответно на изискването за осигуряване на най-високи стандарти на защита, защото се засягат основни права в личната сфера на човека. Прегледът на оспорената уредба обаче показва, че така, както със закона са формулирани процедурите на съдебен контрол, те се оказват повече от формални и непълноценни, поради което не би могло да се очаква, че резултатите от него биха изпълнили главното си предназначение – да се ограничи до обективно възможния минимум нерегламентираният достъп до данните и злоупотребата с тях. Така разпоредбата на чл. 250б, ал. 2, т. 1 - 5 ЗЕС, която урежда изискванията и реквизитите на изискуемото мотивирано писмено искане до компетентния съд, съдържа съществена непълнота, изразяваща се в следното: Освен административните данни – регистрационен номер на преписката, за нуждите на която е предназначена справката и определеното да я получи длъжностно лице, както и исканото съдържание на самата справка с описание на данните и периода, законът изисква единствено посочването на правното основание и целта, за която е необходим достъпът. Мотивационната част на искането изобщо не е изведена от законодателя като отделен негов реквизит, доколкото само правното основание и целта на искането не биха могли да покрият стандартите на ефективна съдебна намеса, когато става дума за толкова съществена интервенция на държавни органи в конституционно защитената сфера на неприкосновеност на личния живот, жилището, кореспонденцията. Компетентният председател на районен съд или оправомощен от него съдия (чл. 250в, ал. 1 ЗЕС), председател на окръжен съд (чл. 250в, ал. 5 ЗЕС), председател на Софийски градски съд, респ. оправомощен съдия (чл. 251, ал. 2 ЗЕС), не би могъл да се произнесе пълноценно, без да са му поднесени фактическите обстоятелства, стоящи в основата на отправеното искане. Няма как без информация за тях съдията да постанови законосъобразен и обоснован акт, с който съответно да разреши достъпа до данните или да постанови отказ.

Освен това компетентността и правомощията на органите по чл. 250б, ал. 1 ЗЕС следва да е обвързана с непосредствения предмет на направеното искане за всеки отделен случай, а това следва да намери законодателно решение с нова и прецизна формулировка на текста на чл. 250б, ал. 2 ЗЕС, каквато действащата редакция на нормата не осигурява. Последното е наложително, тъй като преобладаващата част от легитимирани с оспорените разпоредби органи и структури разполагат и с множество други компетенции, нямащи по същността и характера си никакво отношение към дейностите, изпълняващи формулираната със закона цел – разкриване и разследване на тежките престъпления. Ето защо разпоредбата на чл. 250б, ал. 2 ЗЕС като недостатъчно конкретизирана, се оказва неточна и непрецизна, включително и в контекста на регламентацията на съдебния контрол, а следователно и противоконституционна с оглед границата на допустимото изключение по чл. 32, ал. 2, чл. 34, ал. 2 и принципа на правовата държава по чл. 4, ал. 1 от Конституцията.

Сравнителният анализ на разпоредбите на ЗЕС, предмет на оспорената уредба, и относимите норми на Закона за специалните разузнавателни средства (ЗРС) води до извода, че доколкото между наблюдението и проследяването чрез техническо средство, представляващи оперативни способности, т.е. специални разузнавателни средства по смисъла на чл. 2, ал. 1 и 3 ЗРС, дефинирани като същност и характеристики по чл. 5 и чл. 7 от същия закон, и достъпът до данните, генерирани и запазени по реда на чл. 250а, ал. 1 и сл. ЗЕС, с оглед обсъдените по-горе специфики на последните, може да се констатира сходство, е логично да се търси такова и в основанията и процедурите на предвидения в двата закона съдебен контрол. Това е така, защото и в двата случая се касае за твърде близки по своите характеристики форми на съществена намеса на определени държавни органи в личната сфера на гражданите. За разлика от текстовете на оспорената уредба на ЗЕС, формулираното по чл. 14, ал. 1, т. 1 ЗРС мотивирано писмено искане задължително съдържа пълно и изчерпателно посочване на фактите и обстоятелствата, даващи основание да се предполага, че се подготвя, извършва или е извършено тежко умишлено престъпление. Нещо повече, чл. 14, ал. 1, т. 7 ЗРС изисква и излагане на мотиви за невъзможността необходимите данни да бъдат събрани по друг начин или описание на изключителните трудности, с които е свързано събирането им. От направеното сравнение се налага изводът, че оспорените разпоредби не покриват изискуемите в случая най-високи стандарти на защита и сигурност, което обосновава необходимостта от приемането на нова и значително по-прецизна законодателна регламентация в ЗЕС. Тя следва да осигури действащ механизъм на ефективен съдебен контрол, каквато оценка предвиденият в действащия понастоящем закон очевидно не би могъл да получи.

Твърде обща е формулировката на чл. 250в, ал. 4 ЗЕС, според която 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 Наказателнопроцесуалния кодекс (НПК). Законът не уточнява към кои конкретни норми на НПК насочва препращането, но е ясно, че става дума за приложението на чл. 159 НПК. Сравнителноправният анализ на двете разпоредби предпоставя заключението, че чрез използваната законодателна техника с оспорената разпоредба изцяло се дерогира конституционното изискване за съдебен контрол при искане за достъп до данни от телекомуникационен трафик. Такъв не е предвиден нито в препращащата норма на ЗЕС, нито в специалната норма на НПК. В случая няма никакво основание да се приеме, че въпреки тежката намеса в личната сфера на гражданите, каквато безусловно представлява нарушаването на неприкосновеността на личния живот, свободата и тайната на кореспонденцията, съществува каквато и да било правна възможност за конституционна търпимост на обсъжданата дерогация, и то само защото искането се прави от орган на досъдебното производство.

Следва изрично да се изтъкне, че винаги, когато законът допуска като изключение мерки, в резултат на които се засягат основни права на гражданите, съдебният контрол е задължителен по силата на изричните разпоредби на чл. 30 - 35 от Конституцията. Достатъчно е в тази връзка да се споменат уредените в НПК съдебни производства по вземане и контрол върху мерките за неотклонение задържане под стража и домашен арест в досъдебното производство (чл. 64 - 65 НПК и чл. 62, ал. 2 във връзка с чл. 64 - 65 НПК), съдебният контрол върху забраната за напускане пределите на Република България (чл. 68, ал. 3 - 4 НПК), предварителното съдебно разрешение или последващо одобрение от съдия при освидетелстване (чл. 158, ал. 3 - 4 НПК), претърсване и изземване (чл. 161, ал. 1 - 2 НПК), обиск (чл. 164, ал. 1 и 3 НПК), задържане и изземване на кореспонденцията и електронната поща (чл. 165, ал. 2 и 5 НПК) и др.

Ето защо Конституционният съд счита, че оспореното законодателно решение за елиминиране на съдебния контрол в хипотезата на отправено искане за достъп до трафични данни от орган на досъдебното производство е в противоречие с установените от Конституцията, Хартата и КЗПЧОС стандарти. Доколкото предмет на контрола за конституционност по настоящото дело е само текстът на чл. 250в, ал. 4 ЗЕС, а не и този на чл. 159, ал. 1 НПК, Съдът ограничава произнасянето само до него, като приема, че същият е противоконституционен.

Отстраняването на констатирания порок на оспорената уредба по законодателен път е от особено съществено значение, защото се отнася до правното регулиране на съдебни

процедури за контрол върху достъпа до данни, свързани с основни права на гражданите – неприкосновеност на личния живот и на свободата и тайната на кореспонденцията.

На следващо място е необходимо да се констатира, че изобщо липсва уредена със закона правна възможност, а оттам и основания и процедура засегнатите от мерките лица, чиито данни са били предоставени на съответните държавни органи, но не са послужили за образуване на наказателно производство или образуването е било прекратено, да бъдат уведомени за това кога и на какво основание са били обект на тяхното приложение, както и за какво са били използвани.

В заключение Конституционният съд счита, че макар и въведена като средство за постигането на една легитимна цел от общ интерес както за Европейския съюз, така и за всяка национална държава, за да бъде оценена като необходима, подходяща и съразмерна в условията на едно демократично общество, обсъжданата мярка по събиране и запазване на данните от целия телекомуникационен трафик (общо и без повод), безспорно представляваща сериозна намеса в личния живот на гражданите, следва да бъде уредена по начин, съобразен с най-високите възможни стандарти на сигурност, каквито действащата правна регламентация като цяло не осигурява. Законът следва да съдържа точни, ясни и предвидими правила, създаващи сигурни гаранции за защита и сигурност (вж. в т.см. Решение на ЕСПЧ по делото Ротару срещу Румъния/Rotaru v. Romania, 2000 г., „Сънди таймс” срещу Обединеното кралство/„Sunday Times” v. United Kingdom, 1979 г.), които принципно да изключват формирането на чувство на заплахата от наблюдение, доколкото обективно всички граждани се оказват потребители на една или повече от формите на съществуващите съвременни комуникации, и то в огромната си част без с поведението и действията си да са дали повод да бъдат свързвани с прояви на тежката, в частност организираната престъпност или тероризма. Това би могло да се постигне единствено с предвиждане на достатъчни по обем и правно съдържание, надеждни, адекватни и ефективни гаранции: 1) че органите, оторизирани да заявяват искания за достъп до данните, ще могат да упражняват това си правомощие само в конкретно и изчерпателно уредени в закона случаи; 2) прецизно уредени основания, органи и процедура за получаване на съдебна санкция за достъп до данните, тяхното използване и унищожаване; 3) законови гаранции за сигурността на самите предоставени данни, обхвата на тяхната употреба, прозрачността и правната защита, включително осигуряване на специализиран контрол срещу нерегламентирания достъп до данните и възможността за предоставянето им на трети лица, извън оторизираните субекти; 4) използването им за цели, различни от конституционно оправданите, и то във всички възможни етапи – генериране, запазване, съхранение, предаване, използване, унищожаване от

лицата, които ги съхраняват; 5) оптимизиране на срока на запазване на данните съобразно установените европейски стандарти, националната и европейската практика; 6) осигуряване на баланс между целта, сериозността на ограничението и предвидените правни средства за защита от неоторизиран достъп до запазените данни от телекомуникация, вкл. и наказателноправни, ако такива бъдат създадени. Само при пълното и точно изпълнение на всички обсъдени критерии би могло да се счете, че законодателната уредба на мярка от вида на въведената би издържала проверката за съответствие с Конституцията. Такъв извод обаче не би могъл да бъде направен по отношение на оспорената от омбудсмана уредба.

Конституционният съд прие, че не отделните разпоредби, а цялата оспорена уредба следва да бъде обявена за противоконституционна. Нормите, предмет на конституционен контрол, са систематично, логически и функционално свързани и съвкупно изграждат структурата на разглежданата правна регламентация на запазването, съхранението, достъпа и контрола относно данните от телекомуникационния трафик. Касае се за съвкупност от правила, които са вътрешно обвързани, поради което следва да се прилагат в своето единство. В цялост те формират единна система от правни норми, въведена с чл. 250а и сл. ЗЕС, която не удовлетворява установените европейски стандарти за гарантиране на конституционно закрепените основни права на гражданите, а отгук и принципа за правовата държава, прогласен с преамбюла и чл. 4, ал. 1 от Конституцията. По тези съображения Съдът прие, че тяхната конституционност следва да бъде преценявана в цялост, а не поотделно. Обратният подход – на търсене и обявяване на частична противоконституционност на отделни норми предвид описаната конкретна структура на оспорената уредба, би довел до възникване на ситуация на нестабилност и несигурност в правното регулиране на обсъжданата материя, и то в резултат на намесата на Конституционния съд, а това е несъвместимо с изискванията на принципа на правовата държава.

Съдът намира за необходимо изрично да изтъкне, че макар борбата срещу тежките престъпления, включително срещу организираната престъпност и тероризма, защитата на държавата, гарантирането на националната сигурност и конституционната система да представляват цели с фундаментално значение, те не могат да оправдаят неограничената намеса в човешките права, поради което всяко законодателно решение в тази така деликатна област следва да осигурява справедлив баланс между интересите на отделната личност и тези на обществото като цяло. В този смисъл Конституционният съд изцяло споделя позицията, изразена от ЕСПЧ в решението му по делото Клас и други срещу Германия/*Klass and others v. Germany*, 1978 г., а именно, че поставянето под наблюдение без адекватни и достатъчни мерки за безопасност може да разруши демокрацията под претекст, че я брани.

Прегледът на конституционната практика на различни европейски конституционни съдилища показва, че националните законодателни актове, с които е транспонирана Директива 2006/24/ЕО, са обявени за противоконституционни – изцяло или отделни части от тях. Основните съображения на конституционните съдилища в Германия, Румъния, Чехия, Словения, Австрия, Полша, аргументиращи взетите решения, се оказват твърде сходни, а някои и напълно идентични с изводите на Конституционния съд на РБ по настоящото дело. Очевидно е, че пороците и несъвършенствата на самата Директива, предпоставили обявяването ѝ за невалидна от СЕС, не само са механично пренесени, но в редица случаи се оказват надхвърлени и задълбочени, какъвто е и случаят със ЗЕС. Последното обяснява преобладаващото разбиране на посочените конституционни съдилища, че приетите формулировки на правните норми в националните законодателства са твърде общи, неясни, неточни, а приетите закони като цяло не създават достатъчно и надеждни гаранции за защита срещу евентуални нарушения по отношение сигурността на данните, поради което и са оценени като противоречащи на националните конституции.

Ето защо, като съобрази всичко гореизложено, Конституционният съд намира, че разпоредбите на чл. 250а - чл. 250е, чл. 251 и чл. 251а ЗЕС противоречат на Конституцията, поради което искането на омбудсмана на Република България е основателно. Това налага Конституционният съд да упражни правомощията си по чл. 149, ал. 1, т. 2 от Конституцията и обяви посочените норми за противоконституционни.

Воден от изложените съображения и на основание чл. 149, ал. 1, т. 2 от Конституцията във връзка с чл. 22, ал. 1 от Закона за Конституционен съд, Конституционният съд

Р Е Ш И:

Обявява за противоконституционни чл. 250а - чл. 250е, чл. 251 и чл. 251а от Закона за електронните съобщения (обн., ДВ, бр. 41/2007 г., последно изм. и доп., ДВ, бр. 14/2015 г.).

Председател: Димитър Токушев