ЧЕТВЪРТО ОТДЕЛЕНИЕ

ДЕЛО „ЕКИМДЖИЕВ И ДРУГИ СРЕЩУ БЪЛГАРИЯ“

(Жалба № 70078/12)

РЕШЕНИЕ

Член 8 • Личен живот • Кореспонденция • Неадекватни правни гаранции срещу произвол и злоупотреба при използване на СРС, запазване и достъп до трафични данни

СТРАСБУРГ

11.01.2022 г.

*Настоящото решение става окончателно при наличието на обстоятелствата, посочени в член 44, алинея 2 от Конвенцията. То може да бъде предмет на редакционен преглед.*

**СЪДЪРЖАНИЕ**

ВЪВЕДЕНИЕ 1

ОПИСАНИЕ НА ФАКТИТЕ 1

БЪЛГАРСКО ЗАКОНОДАТЕЛСТВО И ПРАКТИКА 2

I. СПЕЦИАЛНИ РАЗУЗНАВАТЕЛНИ СРЕДСТВА 2

А. Значение на термина „специални РАЗУЗНАВАТЕЛНИ средства“ и най-често използваните оперативни способи 2

Б. Обща рамка и развитие на съответното законодателство 3

В. Случаи, които могат да наложат използването на специални разузнавателни средства 4

Г. Лица или обекти, по отношение на които могат да бъдат използвани СРС 6

1. Общи правила 6

2. Правила относно кореспонденцията между адвокат и клиент 7

Д. Процедури за издаване на разрешение 8

1. Органи, оправомощени да искат използване на СРС 8

2. Съдържание на искането за използване на СРС 9

(а) Самото искане 9

(б) Материали в подкрепа на искането 10

3. Органи, оправомощени да издават разрешения за използване на СРС 10

4. Ред на разглеждане на исканията за използване на СРС 12

(а) Съответни законови разпоредби и съдебна практика 12

(б) Информация за практиката на съдилищата във връзка с разглеждането на искания за използване на СРС, получена на базата на годишните доклади на Националното бюро 12

(в) Други официални данни за практиката на съдилищата 13

(i) В Софийски градски съд през 2013 -17 г. 13

(α) Наказателно и дисциплинарно производство срещу председателя на СГС 13

(β) Доклад от април 2017 г. на заместник-председателите на Софийски градски съд 14

(γ) Примери за разрешения за използване на СРС, издадени от Софийски градски съд през 2012 -13 г. 15

(ii) В Специализирания наказателен съд през 2015 - 2019 г. 18

(iii) В обобшение 20

(г) Изисквания за публично оповестяване 20

5. Допълнителен контрол от страна на органите, използващи специални разузнавателни средства 20

6. Последващо разрешение в неотложни случаи 22

Е. Максимален срок за прилагането на СРС 23

Ж. Ситуации, при които прилагането на СРС трябва да бъде прекратено 23

З. Обработка на информация, получена чрез прилагане на специални разузнавателни средства 24

1. Цели, за които може да се използва информацията 24

2. Средства за прихващане на електронни съобщения 24

3. Етапи на обработка 25

(a) „Материален носител“ и „производен носител на данни“ 25

(b) Веществено доказателствено средство 25

(c) Унищожаване на информация, която не е от значение 27

4. Правила за разрешеното използване на резултати, получени извън направеното искане 28

5. Релевантни разпоредби на Закона за защита на класифицираната информация от 2002 г. 29

И. Органи, упражняващи контрол върху използването на специални разузнавателни средства 30

1. Съдии, издали разрешение за използване на СРС 30

2. Национално бюро 30

(а) Начин на избиране и мандат на членовете на Националното бюро 31

(i) Законови разпоредби 31

(ii) Членове на Националното бюро за периода 2013 -2018 г. и след 2018 г. 32

(б) Правомощия на Националното бюро 33

(i) За достъп до материали 33

(ii) Даване на указания и определяне на образци 34

(iii) Сезиране на компетентните органи за нередности 35

(iv) Брой проверки на Националното бюро 35

3. Парламентарна комисия 35

(а) Начин на избиране на членовете на комисията 36

(б) Правомощия на комисията 36

З. Уведомяване на лица, по отношение на които се използват СРС 36

И. Гражданска отговорност на органите за неправомерно използване на СРС 38

Й. Наказателна отговорност на длъжностните лица за неправомерно използване на СРС 42

II. ПРЕДСТАВЯНЕ НА ДОКУМЕНТИ В ГРАЖДАНСКОТО ПРОИЗВОДСТВО 42

III. ЗАПАЗВАНЕ И ДОСТЪП ДО ТРАФИЧНИ ДАННИ 43

A. Общо развитие на правния режим 43

Б. Режимът в понастоящем 44

1. Видове комуникационни данни, подлежащи на запазване 44

2. Цели, за които се запазват тези данни 45

3. Правила за обработване на запазените данни от доставчиците на комуникационни услуги 46

4. Унищожаване на запазени данни, до които органите не са осъществили достъп 46

5. Процедура за получаване на разрешение 46

(a) Органи, оправомощени да търсят достъп 46

(б) Съдържание на искането за достъп 47

(в) Органи с правомощия да издават разрешения за достъп...48

(г) Ред за разглеждане на искането за достъп 49

(д) Последващо разрешение в неотложни случаи 50

6. Процедура за достъп до запазените данни 50

7. Съхранение на запазените данни, до които органите имат достъп 52

8. Унищожаване на запазените данни, до които органите имат достъп 52

9. Органи, упражняващи надзор върху запазването и достъпа до трафични данни 53

(a) Съдии, издали съответните разрешения за достъп 53

(б) Комисия за защита на личните данни 53

(i) Начин на избиране и мандат на членовете на Комисията 53

(ii) Правомощия на Комисията по ЗЕС. 53

(α) Да получава информация 54

(β) Да дава указания и препоръки 54

(γ) Да налага санкции 55

(в) Парламентарна комисия 55

(i) Ред за избор на членовете на Комисията 55

(ii) Правомощия на Комисията по ЗЕС. 55

(α) Да получава информация 55

(β) Да дава указания 56

(iii) Сезиране на компетентните органи за нередности 56

10. Изисквания за уведомяване 57

(a) В случай на незаконен достъп или опит за достъп 57

(b) В случай на нарушение на сигурността на личните данни 57

IV. РЕЛЕВАНТНИ РАЗПОРЕДБИ ЗА ЗАЩИТА НА ДАННИТЕ 57

A. Приложно поле 57

Б. Относно обработването на лични данни от частни лица 58

1. Ограничения на правата на субектите на данни 58

2. Средства за правна защита 58

В. Относно обработването на лични данни от компетентните органи за целите на правоприлагането 58

1. Условия, при които обработването е законосъобразно 58

2. Възможни ограничения на правата на субектите на данни 59

3. Надзорни органи 60

4. Средства за правна защита 60

РЕЛЕВАНТНИ РЕШЕНИЯ НА КОМИТЕТА НА МИНИСТРИТЕ НА СЪВЕТА НА ЕВРОПА 60

РЕЛЕВАНТНО ПРАВО НА ЕВРОПЕЙСКИЯ СЪЮЗ 62

I. ДИРЕКТИВА ЗА ПРАВОТО НА НЕПРИКОСНОВЕНОСТ НА ЛИЧНИЯ ЖИВОТ В ЕЛЕКТРОННИТЕ КОМУНИКАЦИИ 62

II. ДИРЕКТИВА ОТНОСНО ЗАПАЗВАНЕТО НА ДАННИ 62

III. ОБЩ РЕГЛАМЕНТ ОТНОСНО ЗАЩИТАТА НА ДАННИТЕ.63

IV. ДИРЕКТИВА ОТНОСНО ПРАВОПРИЛАГАНЕТО 64

V. ПРАКТИКА НА СЪДА НА ЕС ПО ЧЛЕН 15, ПАРАГРАФ 1 ОТ ДИРЕКТИВАТА ЗА ПРАВОТО НА НЕПРИКОСНОВЕНОСТ НА ЛИЧНИЯ ЖИВОТ В ЕЛЕКТРОННИТЕ КОМУНИКАЦИИ 64

ПРАВОТО 67

I. ТАЙНО НАБЛЮДЕНИЕ 67

A. Допустимост 67

1. Твърденията на страните 67

(a) Статут на жертва на жалбоподателите 67

(i) Правителството 67

(ii) Жалбоподателите 68

(б) Изчерпване на вътрешноправните средства за защита 68

2. Оценката на Съда 69

(a) Дали жалбата е „по същество същата“ 69

(б) Дали Съдът е възпрепятстван да разгледа жалбата от член 46 от Конвенцията 69

(в) Статут на жертва и изчерпване на вътрешноправните средства за защита 70

(г) Заключение относно допустимостта на жалбата 71

Б. По същество на оплакванията 71

1. Статут на жертва на жалбоподателите и наличие на намеса 71

(a) Твърденията на страните 71

(b) Оценката на Съда 71

(i) Общи принципи 71

(ii) Прилагане на тези принципи 71

(α) Обхват на приложимия закон 71

(β) Наличие на ефективни средства за защита 72

(γ) Заключение 76

2. Оправдание за намесата 76

(a) Твърденията на страните 76

(i) Жалбоподателите 76

(ii) Правителството 78

(b) Оценката на Съда 80

(i) Общи принципи 80

(ii) Прилагане на тези принципи 81

(α) Достъпност на закона 82

(β) Основания, при които може да се прибегне до прилагане на тайно наблюдение, и лица, по отношение на които могат да се приложи тайно наблюдение 82

(γ) Срок на мерките за прилагане на СРС 85

(δ) Процедури за издаване на разрешение 86

(ε) Процедури за съхраняване, достъп, преглед, използване, съобщаване и унищожаване на данни от прилагане на СРС 91

(στ) Наблюдение на системата 95

(ζ) Уведомяване 98

(η) Средства за правна защита 99

(θ) Заключение 100

II. ЗАПАЗВАНЕ И ДОСТЪП ДО ТРАФИЧНИ ДАННИ 101

A. Допустимост 102

1. Твърденията на страните 102

(a) Статут на пострадал на жалбоподателите 102

(i) Правителството 102

(ii) Жалбоподателите 102

(b) Изчерпване на вътрешните средства за правна защита 102

2. Оценката на Съда 103

B. Основателност 104

1. Статут на пострадал на жалбоподателите и наличие на намеса 104

(a) Твърденията на страните 104

(b) Оценката на Съда 104

(i) Запазване на трафични данни от доставчиците на комуникационни услуги 104

(ii) Достъп на органите до запазените трафични данни 105

(α) Обхват на приложимия закон 106

(β) Наличие на ефективни средства за правна защита 106

(γ) Заключение 106

2. Обоснованост на намесата 107

(a) Твърденията на страните 107

(i) Жалбоподателите 107

(ii) Правителството 108

(b) Оценката на Съда 110

(i) Общи принципи 110

(ii) Прилагане на тези принципи 110

(α) Достъпност на закона 110

(β) Защита на запазените данни от доставчиците на съобщителни услуги 110

(γ) Основания, при които органите могат да имат достъп до запазените данни 111

(δ) Процедура за получаване на достъп 111

(ε) Време, през който което органите могат да съхраняват и използват данни, които не се използват впоследствие в наказателното производство 113

(στ) Процедури за съхраняване, достъп, преглед, използване, съобщаване и унищожаване на данни, до които органите имат достъп 114

(ζ) Правила за надзор 114

(η) Уведомяване 116

(θ) Средства за правна защита 116

(ι) Заключение 117

III. ПРИЛОЖЕНИЕ НА ЧЛ. 41 ОТ КОНВЕНЦИЯТА 118

A. Вреди 118

1. Исканията на жалбоподателите и коментарите на правителството по тях 118

2. Оценката на Съда 118

B. Разходи и разноски 119

1. Исканията на жалбоподателите и коментарите на правителството по тях 119

2. Оценката на Съда 119

C. Лихва за забава 120

1. **По делото „Екимджиев и други срещу България“,**

Европейският съд по правата на човека (четвърто отделение), заседаващ в Камара, в състав:

Тим Айке, *председател*,  
 Йонко Грозев, Фарис Вехабович, Юлия Антоанела Моток, Армен Харутюнян, Габриеле Кучко-Щадлмайер, Ана Мария Гера Мартинс, *съдии*,  
и Андреа Тамиети, *секретар на отделение*,

Като взе предвид:

жалбата (№ 70078/12) срещу Република България, подадена в Съда на основание член 34 от Конвенцията за защита правата на човека и основните свободи („Конвенцията“) от двама български граждани, г-н Михаил Тихолов Екимджиев и г-н Александър Емилов Кашъмов, както и от две неправителствени организации - Асоциация за европейска интеграция и права на човека и Фондация „Програма достъп до информация“ („жалбоподатели“) на 19 октомври 2012 г.;

решението за уведомяване на българското правителство („правителството“) за оплакванията по членове 8 и 13 от Конвенцията относно (а) системата за тайно наблюдение в България и (б) системата за запазване на комуникационни данни в България и последващото им използване от страна на властите, както и за обявяване на останалата част от жалбата за недопустима;

становищата на страните;

След закрито заседание, проведено на 07 декември 2021 г.,

Постанови следното решение, прието на тази дата:

ВЪВЕДЕНИЕ

1.  Случаят се отнася до съвместимостта на българското законодателство и практики, свързани с (а) използването на специални разузнавателни средства и (б) запазването и достъпа до комуникационни данни, с член 8 от Конвенцията.

1. ИЗЛОЖЕНИЕ НА ФАКТИТЕ

2.  Четиримата жалбоподатели са двама адвокати и две неправителствени организации, свързани с тях.

3.  Първият жалбоподател, г-н Екимджиев, е роден през 1964 г. и живее в гр. Пловдив. Той е адвокат, чиято практика включва процесуално представителство в различни национални дела, както и представителство на жалбоподатели пред този Съд.

4.  Вторият жалбоподател, Асоциацията за европейска интеграция и права на човека, е основана през 1998 г. със седалище в гр. Пловдив. Първият жалбоподател, г-н Екимджиев, е председател на управителния ѝ съвет.

5.  Третият жалбоподател, г-н A. E. Кашъмов, е роден през 1971 г. и живее в гр. София. Той също е адвокат, чиято практика включва процесуално представителство в различни национални дела и представителство на жалбоподатели пред този Съд.

6.  Четвъртият жалбоподател, Фондация „Програма за достъп до информация“, е основана през 1997 г. със седалище в гр. София. Третият жалбоподател, г-н A. E. Кашъмов, е ръководител на нейния правен екип.

7.  Първоначално първият и вторият жалбоподател са представлявани пред Съда от г-жа С. Стефанова и г-жа Г. Черничерска, адвокати, практикуващи в гр. Пловдив, а след това съответно от г-жа Т. Екимджиева и г-жа М.Докова-Костадинова, също адвокати, практикуващи в гр. Пловдив.

8.  Третият жалбоподател е представляван от г-н A. A. Кашъмов, адвокат, практикуващ в гр. София. Четвъртият жалбоподател е представляван от третия жалбоподател, г-н A. E. Кашъмов.

9.  Правителството е представлявано от своя правителствен агент - г-жа М. Димитрова от Министерството на правосъдието.

10.  Жалбоподателите твърдят, че естеството на дейността им ги излага както на риск от прилагане на СРС, така и на риск от достъп до комуникационните им данни от властите съгласно законодателството, уреждащо тази материя в България. Те не твърдят, че по отношение на тях действително са използвани СРС или че е осъществен достъп от страна на властите до тяхна кореспонденция.

ПРИЛОЖИМО БЪЛГАРСКО ЗАКОНОДАТЕЛСТВО И ПРАКТИКА

* 1. СПЕЦИАЛНИ РАЗУЗНАВАТЕЛНИ СРЕДСТВА

**А. Значение на термина „специални разузнавателни средства“ и най-често използваните оперативни способи**

11.  В България общият термин „специални разузнавателни средства“ включва електронни или механични устройства, позволяващи изготвянето на веществени доказателствени средства (видео и звукозаписи, фотоснимки и белязани предмети), и оперативните способи за тяхното прилагане (чл. 2, ал. 1 и 2 от Закона за специалните разузнавателни средства от 1997 г. и чл. 172, ал. 1 от Наказателно-процесуалния кодекс). Тези способи са: а) наблюдение, б) подслушване, в) проследяване, г) проникване (в превозни средства или помещения), д) белязване и проверка на кореспонденцията или компютризираната информация, е) контролирана доставка, ж) доверителна сделка и з) разследването чрез служител под прикритие (чл. 2, ал. 3 от ЗСРС и член 172, ал. 1 от НПК). В членове 5 - 10в се дефинира всеки от тези способи. В чл. 6 по-специално се пояснява, че подслушването включва прихващане както на телефонна, така и на електронна комуникация.

12.  Според годишните доклади, публикувани от Националното бюро за контрол на специалните разузнавателни средства (вж. параграфи 14, 16 и 108 по-долу), след 2014 г. най-често използваните оперативни способи са: а) наблюдение и б) подслушване:

| **Година** | **Наблюдение** | **Подслушване** |
| --- | --- | --- |
| 2014 | 2773 (24,94%) | 4927 (44,33%) |
| 2015 | 1417 (20,25%) | 3848 (54,97%) |
| 2016 | 1865 (21,56%) | 4717 (54,80%) |
| 2017 | 1699 (21,23%) | 4470 (55,86%) |
| 2018 | 1669 (19,39%) | 5124 (59,53%) |
| 2019 | 1628 (19,22%) | 5076 (59,92%) |
| 2020 | 1372 (18,27%) | 1. ,19%) |

**Б. Обща рамка и развитие на приложимото законодателство**

13.  Специалните разузнавателни средства са уредени за първи път в България със Закона за специалните разузнавателни средства от 1994 г., в сила до 1997 г. Понастоящем правилата, уреждащи специалните разузнавателни средства, са установени главно в Закона за специалните разузнавателни средства от 1997 г., с последващите изменения, членове 172 - 177 от Наказателно-процесуалния кодекс, с последващите изменения, членове 304 - 310 от Закона за електронните съобщения от 2007 г., с последващите изменения, и Правилника за дейността на Националното бюро за контрол на специалните разузнавателни средства, чиято последна редакция е приета през м. октомври 2016 г.

14.  През м. декември 2008 г., след решение на Съда по делото *Асоциация за европейска интеграция и права на човека и Екимджиев срещу България* (№ 62540/00, 28 юни 2007 г.), в което Съдът установи нарушения на членове 8 и 13 от Конвенцията, ЗСРС претърпява значителни изменения. Мотивите към законопроекта за изменение цитират посоченото решение и необходимостта от привеждане на закона в съответствие с изискванията на Конвенцията. Наред с редица други промени, с изменението се създава Национално бюро за контрол на специалните разузнавателни средства („Националното бюро“), независим орган, чиито петима членове се избират от парламента и чиято задача е да контролира използването на специални разузнавателни средства и съхраняването и унищожаването на материали, получени чрез такива средства, и да защитава гражданите срещу неправомерно използване на специални разузнавателни средства.

15.  През м. октомври 2009 г. обаче, преди Националното бюро да започне работа, Парламентът прие допълнителни изменения в ЗСРС, с които Бюрото е премахнато и заменено със специална парламентарна подкомисия. Измененията влизат в сила през м. ноември 2009 г. За повече подробности относно тези изменения и работата на комисията през 2011 г. вж. *Хаджиев срещу България* (№ 22373/04, § 26 - 28, 23 октомври 2012 г.) и *Ленев срещу България* (№ 41452/07, §§ 81 - 83, 4 декември 2012 г.).

16.  С ново изменение на ЗСРС, влязло в сила през м. август 2013 г., Националното бюро е възстановено като „независим държавен орган“ (вижте параграфи 108 - 123 по-долу). Петимата му членове са избрани от Парламента през м. декември 2013 г. и започват своята работа в началото на 2014 г. Специалната парламентарна подкомисия става комисия и продължава да съществува редом с Бюрото (вижте параграф 125 по-долу).

17.  Съответните разпоредби на всички актове, цитирани в параграф 13 по-горе, както и на всички други разпоредби, посочени в текста, са изложени по-долу в редакцията им от 7 декември 2021 г.

**В. Случаи, които могат да наложат използването на специални разузнавателни средства**

18.  Специални разузнавателни средства могат да бъдат използвани, ако това е необходимо за предотвратяване или разкриване на едно или повече „тежки умишлени престъпления“ (чл. 93, точка 7 от Наказателния кодекс определя „тежкото“ престъпление като такова, което се наказва с повече от пет години лишаване от свобода), изброени изчерпателно в чл. 3, ал. 1 от ЗСРС и чл. 172, ал. 2 от Наказателно-процесуалния кодекс, които посочват главите в Наказателния кодекс, в които се съдържат съставите на тези престъпления, или самите разпоредби.[[1]](#footnote-1) Те включват различни престъпления срещу Републиката (като например опит за държавен преврат, държавна измяна, шпионаж и саботаж); терористични престъпления, включително подготовка за такива; убийство; причиняване на тежка телесна повреда; отвличане; изнасилване и някои други сексуални престъпления; трафик на хора; купуване на гласове и някои други изборни престъпления; кражба; грабеж; присвояване; измама; изнудване; търговия с крадени стоки; пране на пари; различни икономически, кредитни и митнически престъпления; квалифицирано подправяне; квалифицирана злоупотреба с власт; възпрепятстване на правосъдието; подкуп; ръководене или участие в организирана престъпна група; някои квалифицирани компютърни престъпления; палеж; някои транспортни престъпления; някои екологични престъпления; различни престъпления с наркотични вещества; разкриване на служебни тайни; дезертьорство по време на война и различни военни престъпления; незаконни действия с ядрени материали; и различни престъпления срещу мира и човечеството.

19.  Според годишните доклади на Националното бюро двете престъпления, които са причина за най-голям брой случаи на използване на СРС от 2014 г. насам, са тези по чл. 321 от Наказателния кодекс (ръководене или участие в организирана престъпна група, което престъпление, независимо от мястото на извършване на територията на България, е под юрисдикцията на Специализирания наказателен съд след създаването му през 2011 - 2012 г. – вижте параграф 46 по-долу) и по чл. 354а от Наказателния кодекс (производство, преработване, придобиване или държане на наркотични вещества или техни аналози без надлежно разрешение с цел разпространение, или разпространение на наркотични вещества или техни аналози, които, ако са извършени от организирани престъпни групи, също са под юрисдикцията на Специализирания наказателен съд след създаването му през 2011 - 2012 г.):

| **Година** | **Организирани престъпни групи** | **Наркотични вещества** |
| --- | --- | --- |
| 2014 | 20,90% | 29,30% |
| 2015 | 34,15% | 19,00% |
| 2016 | 42,05% | 14,00% |
| 2017 | 43,52% | 14,63% |
| 2018 | 53,17% | 14,28% |
| 2019 | 48,78% | 14,91% |
| 2020 | 51,11% | 13,86% |

20.  Допълнителното условие е, че за предотвратяването или разкриването на едно или повече от тези престъпления могат да се използват специални разузнавателни средства само ако необходимите данни не могат да бъдат събрани по друг начин или събирането им е свързано с изключителни трудности (чл. 3, ал. 1 *in fine* от ЗСРС).

21.  Когато се прилагат за предотвратяване или разкриване на такива престъпления, специалните разузнавателни средства се използват за получаването на доказателства за тях (чл. 3, ал. 2).

22.  Специални разузнавателни средства могат да се използват и за дейности, свързани с националната сигурност (чл. 4 от ЗСРС).[[2]](#footnote-2) Правителството твърди, че на практика националната сигурност никога не е посочвана като самостоятелно основание за използване на СРС и че исканията за използване на СРС винаги се основават на необходимостта от предотвратяване или разкриване на престъпление. Те се позовават на две становища, изготвени от Националното бюро и ДАНС за целите на настоящото производство. В становището си Бюрото посочва, че при инспекциите е установило, че органите, които искат да използват СРС, винаги посочват съответното престъпление. В становището си ДАНС заявява, че поради начина, по който следва да се тълкува чл.14, ал. 1 и 3 от ЗСРС (вж. параграфи 39 и 41 по-долу), в исканията за използване на СРС винаги трябва да е посочено съответното престъпление.

**Г. Лица или обекти, по отношение на които могат да бъдат използвани СРС**

*1. Общи правила*

23.  Съгласно чл. 12, ал. 1-3 от ЗСРС специални разузнавателни средства могат да се използват по отношение на: а) лица, заподозрени или използвани, без да им е известен престъпния характер на дейността за подготовката или извършването на едно или повече от посочените по-горе „тежки умишлени престъпления“; б) лица или обекти, свързани с националната сигурност; в) обекти, необходими за установяването на самоличността на такива лица; г) лица, които са се съгласили по отношение на тях да бъдат използвани СРС за опазване на живота или имуществото им; или д) свидетел в наказателно производство, който се е съгласил по отношение на него да бъдат използвани СРС, за да се разкрие извършването на едно от престъпленията, изброени в чл. 12, ал. 3, от друго лице (включително терористични престъпления, държане за заложници, трафик на хора, вземане и даване на подкуп и ръководене или членство в организирана престъпна група).

24.  Според годишните доклади на Националното бюро броят на лицата, по отношение на които се използват СРС всяка година от 2011 г. насам, е следният:

| **Година** | **Лица, по отношение на които се използват СРС** | **От тях, по собствено желание** |
| --- | --- | --- |
| 2011 | 8184 | не е посочено |
| 2012 | 5902 | не е посочено |
| 2013 | 4452 | не е посочено |
| 2014 | 4202 | 162 |
| 2015 | 2638 | 79 |
| 2016 | 2749 | 73 |
| 2017 | 2748 | 55 |
| 2018 | 3046 | 62 |
| 2019 | 3310 | не е посочено |
| 2020 | 3042 | не е посочено |

25.  Според годишните доклади на Националното бюро броят на случаите, в които органите са използвали СРС спрямо обекти с цел установяване на самоличността на лица (вж. параграф 23, буква в) по-горе), е следният:

| **Година** | **Брой на случаите, в които СРС за използвани спрямо обекти с цел установяване на самоличността на лица** |
| --- | --- |
| 2014 | 645 |
| 2015 | 299 |
| 2016 | 340 |
| 2017 | 261 |
| 2018 | 279 |
| 2019 | 259 |
| 2020 | 172 |

*2. Правила относно кореспонденцията между адвокат и клиент*

26.  Съгласно чл. 33, ал. 1 от Закона за адвокатурата от 2004 г. адвокатските книжа, досиета, електронни документи, компютърна техника и други носители на информация са „неприкосновени“ и не подлежат на преглеждане, копиране, проверка и изземване. Съгласно чл. 33, ал. 2 кореспонденцията между адвокати и клиенти, независимо от средствата за комуникация, електронни или други, също не подлежи на преглеждане, копиране, проверка и изземване. Съгласно чл. 33, ал. 3 разговорите между адвокат и клиент не могат да бъдат подслушвани и записвани, а всички евентуални записи на такива разговори не могат да бъдат използвани като доказателствени средства и подлежат на незабавно унищожаване. С чл. 136, ал. 2 от Наказателно-процесуалния кодекс използването на специални разузнавателни средства по отношение на адвокати се урежда от Закона за адвокатурата от 2004 г. Върховният касационен съд е постановил, че въпреки изричните условия на чл. 33, ал. 3 от Закона за адвокатурата забраната, която той постановява, не е непременно абсолютна във всички случаи, с оглед, наред с другото, на обществения интерес за разкриване на престъпления, извършени от адвокати (вж. решение № 211 от 08.04.2019 г. по н. д. № 1009/2018 г., ВКС, III н. о.). ЗСРС не съдържа разпоредби, които да се отнасят конкретно до използването на СРС по отношение на адвокати или подслушване на тяхната кореспонденция в резултат на използването на СРС по отношение на техни клиенти.

27.  Въпросът изглежда е засегнат единствено в инструкция, издадена от главния прокурор на 11 април 2011 г. при упражняване на правомощията му по член 138, ал. 4 (от август 2016 г. член 138, т. 6) от Закона за съдебната власт от 2007 г. за изготвяне на инструкции, относно дейността на прокуратурата . В преамбюла на инструкцията се посочва, че издаването ѝ е необходимо, за да се спрат непоследователните практики и да се предотвратят нарушенията на чл. 33 от Закона за адвокатурата (вж. параграф 26 по-горе).

28.  Точка 12 от инструкцията гласи, че СРС могат да бъдат използвани по отношение на адвокати само ако има достатъчно данни, от които може да се направи обосновано предположение, че те са извършили престъпление самостоятелно или в съучастие с други лица. В искането за използване на СРС трябва изрично да се посочи, че ще бъдат приложени спрямо адвокат.

29.  Точка 13 от инструкцията гласи, че ако в хода на прилагане на СРС органите запишат разговора на адвокат с клиент или с друг адвокат и този разговор засяга защитата на клиента, не трябва да се изготвя веществено доказателствено средство на тази база, освен ако при използването на СРС не се разкрие, че адвокатът е съпричастен с престъпна дейност.

30.  Изглежда, че инструкцията не е публикувана от прокуратурата. На 13 април 2011 г. обаче главният прокурор изпраща копие от нея на Висшия адвокатски съвет, а през м. юни 2011 г. Висшият адвокатски съвет я публикува в брой 5-6/2011 на своето издание „Адвокатски преглед“ ([връзка](https://www.vas.bg/p/A/d/Adv5-6_2011_5-2252.pdf)).

**Д. Процедури за издаване на разрешение**

*1. Органи, оправомощени да искат използване на СРС*

31.  Само ограничен брой органи могат да искат използването на специални разузнавателни средства и да се ползват от получената по този начин информация в рамките на съответните им компетенции.

32.  Извън рамките на висящо наказателно производство използването на такива средства може да се иска само от: а) редица дирекции на Министерството на вътрешните работи (Главна дирекция "Национална полиция", Главна дирекция "Борба с организираната престъпност", Главна дирекция "Гранична полиция", дирекция "Вътрешна сигурност", областните дирекции на Министерството на вътрешните работи, специализираните дирекции, ); б) териториалните дирекции и самостоятелните териториални отдели на Държавна агенция "Национална сигурност; в) службите "Военно разузнаване" и "Военна полиция" към министъра на отбраната; г) Държавна агенция "Разузнаване"; д) окръжните прокуратури (само във връзка със сериозни изборни нарушения); и е) специализираната дирекция за противодействие на корупцията[[3]](#footnote-3) (чл. 13, ал. 1 от ЗСРС).

33.  В хода на наказателното производство това може да направи прокурорът, отговарящ за надзора на досъдебното производство (чл. 13, ал. 2 от ЗСРС и чл. 173, ал. 1 от НПК).

34.  За предотвратяване на терористични престъпления (включително подготовка за такива) искането може да бъде отправено от главния прокурор, председателя на Държавна агенция „Национална сигурност“, Държавна агенция "Разузнаване", директора на Служба "Военно разузнаване" (или надлежно упълномощените от тях заместници) или главния секретар на Министерството на вътрешните работи (член 13, ал. 4 от ЗСРС).

35.  Специални правила уреждат престъпленията, за които има основание да се смята, че са извършени от председатели на съдилища, съдии, прокурори или следователи (чл. 13, ал. 3 от ЗСРС и чл. 174, ал. 5 от Наказателно-процесуалния кодекс).

36.  Други органи не могат да искат използването на специални разузнавателни средства (чл. 13, ал. 6 от ЗСРС).

37.  Искането трябва да произхожда от ръководителя на съответния орган; ако е подадено от прокурор, той трябва да уведоми административния ръководителя на съответната прокуратура (чл. 13, ал. 5 и чл. 14, ал. 1 от ЗСРС. и чл. 173, ал. 1 *in fine* от Наказателно-процесуалния кодекс).

38.  Според годишните доклади на Националното бюро съответният дял на исканията за използване на СРС е следният:

| **Година** | **Министерство на вътрешните работи** | **Държавна агенция „Национална сигурност“** | **Прокуратура** | **Други органи** |
| --- | --- | --- | --- | --- |
| 2014 | 43,40% | 31,50% | 24,90% | 0,20% |
| 2015 | 50,29% | 19,16% | 30,05% | 0,51% |
| 2016 | 56,22% | 10,08% | 33,39% | 0,32% |
| 2017 | 56,50% | 6,41% | 36,94% | 0,15% |
| 2018 | 60,78% | 4,82% | 34,27% | 0,66% |
| 2019 | 53,73% | 5,69% | 37,95% | 2,63% |
| 2020 | 51,12% | 7,28% | 36,98% | 3,70% |

*2. Съдържание на искането за използване на СРС*

**(а) Самото искане**

39.  Исканията за използване на СРС, направени извън рамките на висящи наказателни производства, трябва да бъдат обосновани и да съдържат: а) пълно и изчерпателно посочване на фактите и обстоятелствата, даващи основание да се предполага, че се подготвя, извършва или е извършено съответното престъпление, включително когато става въпрос за национална сигурност по смисъла на чл. 4 от ЗСРС (вж. параграф 22 по-горе); б) пълно описание на вече предприетите стъпки и резултатите от предишни предварителни проверки или разследвания; в) данни, позволяващи идентифицирането на целта (лицето или обекта); г) срокът, за който се иска използването на СРС и мотиви, които да обосноват необходимостта му; д) предвидените оперативни способи; е) мотиви, поради които информацията не може да бъде събрана по друг начин, или описанието на изключителните трудности, до които би довело това; и ж) длъжностното лице, което да бъде уведомявано за резултатите от използването на СРС (чл. 14, ал. 1 от ЗСРС).

40.  Исканията за използване на СРС, подадени в хода на наказателно производство, също трябва да бъдат обосновани и да посочват: а) информация за разследваното престъпление; б) описание на извършените до момента действия по разследването и резултатите от тях; в) данни, позволяващи идентифицирането на целта (лице или обект); г) предвидените оперативни способи; д) срока, за който се иска ползването, и мотиви, които да обосновават продължителността му; и е) мотиви за невъзможността необходимите данни да бъдат събрани по друг начин или описание на изключителните трудности, с които е свързано събирането им (чл. 173, ал. 2 от Наказателно-процесуалния кодекс).

41.  В исканията за използване на СРС, свързани с терористични престъпления (включително приготовление за такива), трябва да се посочат: а) фактите и обстоятелствата, които дават основание да се предполага, че се подготвя или се извършва, или е било извършено съответното престъпление; б) ако има такива, данни, позволяващи идентифицирането на целта (лице или предмет); в) предвидения срок на използване на СРС; г) предвидените оперативни способи; и д) длъжностното лице, което да бъде уведомявано за резултатите от използването на СРС (чл. 14, ал 3 от ЗСРС).

42.  Исканията за удължаване на срока трябва да съдържат и пълно и изчерпателно посочване на резултатите от използването на СРС до момента (чл. 21, ал. 3 от ЗСРС и чл. 173, ал. 6 от Наказателно-процесуалния кодекс).

43.  Исканията, отнасящи се до използването на СРС спрямо лица в тяхна защита, или до свидетелите (вж. параграф 23, букви г) и д) по-горе), трябва да бъдат придружени от писменото им съгласие (чл. 14, ал. 2 от ЗСРС и чл. 175, ал. 5 от Наказателно-процесуалния кодекс).

**(б) Материали в подкрепа на искането**

44.  За искания, подадени извън рамките на наказателно производство, правилото е, че искащият орган трябва да приложи всички материали, на които се основава искането му (чл. 15, ал. 3 от ЗСРС).[[4]](#footnote-4) За искания, подадени в хода на наказателно производство, правилото е, че съдията, компетентен да издаде разпореждането за разрешаване използването на СРС, може да поиска тези материали (чл. 174, ал. 4 от Наказателно-процесуалния кодекс).[[5]](#footnote-5) Не е ясно дали на практика има различия.

45.  В годишния доклад на Националното бюро за 2017 г. – единственият, в който се засяга този въпрос – се казва (на стр. 19), че през тази година 2% от подадените от МВР искания, 4% от подадените от прокуратурата искания и 4% от подадените от ДАНС искания са отхвърлени, тъй като не са представени всички материали, на които се основават тези искания. Според същия доклад процентът на отказаните искания поради тази причина през предходните две години е 2,5% за министерството и 5% за Агенцията през 2015 г., и 6% за Агенцията през 2016 г.

*3. Органи, оправомощени да разрешат използване на СРС*

46.  По правило разрешения за СРС могат да се издават само от председателите на Софийския градски съд, на съответните окръжни или военни съдилища и на специализирания наказателен съд (който е създаден през 2011 г. и започва работа в началото на 2012 г.), или от изрично упълномощен заместник (чл. 15, ал. 1 и 2 от ЗСРС и чл. 174, ал. 1 - 3 от Наказателно-процесуалния кодекс). Думата „съответни“ – специално добавена към член 15, ал. 1 от Закона от 1997 г. през 2013 г., за да се предотврати рискът от търсене на най-благоприятна юрисдикция от страна на органите – е тълкувана от съдилищата като означаваща съда, който би бил компетентен *ratione materiae*, *personae* и *loci* да разгледа делото за предполагаемото престъпление, във връзка с което се иска използване на СРС (вж. реш. № 262304 от 07.04.2021 г. по гр. д. № 8701/2019 г., СГС, не е ясно дали е влязло в сила).

47.  Специални правила уреждат престъпленията, за които има основания да се смята, че са извършени от съдии, прокурори или следователи: в тези случаи разрешението може да бъде издадено от председателите на Софийския апелативен съд, Военно-апелативния съд или Апелативния специализиран наказателен съд, или от надлежно упълномощен заместник, в зависимост от това кой съд е компетентен да гледа наказателното дело (чл. 15, ал. 4, точка 1 от ЗСРС и член 174, ал. 5 от Наказателно - процесуалния кодекс). Ако има основания да се смята, че престъплението е извършено от някой от тези председатели или заместници, разрешението може да бъде издадено от заместник‑председателя на Върховния касационен съд, ръководещ Наказателната колегия (чл. 15, ал. 4, т. 2 от ЗСРС и чл. 174, ал. 6 от Наказателно - процесуалния кодекс).

48.  Спазването на тези правила за подсъдност се счита за основна гаранция срещу незаконосъобразно използване на СРС (вж. реш. № 365 от 14.02.2014 г. по в. н. о. х. д. № 653/2013 г., САС, потвърдено от реш. № 189 от 03.02.2015 г. по н. д. № 515/2014 г., ВКС, II н. о.).

49.  Според годишните доклади на Националното бюро (и годишните доклади на съответните съдилища за периода 2011 - 2014 г.) разрешенията за използване на СРС, издадени от председателите или заместник-председателите на четирите съдилища, издали най-голям брой от тях през 2015 г., са следните:

| **Година** | **Софийски градски съд** | **Специализиран наказателен съд** | **Окръжен съд Пловдив** | **Окръжен съд Стара Загора** |
| --- | --- | --- | --- | --- |
| 2011 | 6008 (44,10%) | не е приложимо[[6]](#footnote-6) | не е посочено | 872 (6,40%) |
| 2012 | 5556[[7]](#footnote-7) | 550 | не е посочено | 498 |
| 2013 | 4324 | 687 | не е посочено | 332 |
| 2014 | 2298 (41,01%) | 1011 (18,04%) | не е посочено | не е посочено |
| 2015 | 837 (21,38%) | 1049 (26,79%) | 461 (11,78%) | 240 (6,13%) |
| 2016 | 90 (1,91%) | 2179 (46,25%) | 485 (10,30%) | 385 (8,17%) |
| 2017 | 196 (4,24%) | 1808 (39,10%) | 339 (7,33%) | 320 (6,92%) |
| 2018 | 190 (3,57%) | 2524 (47,71%) | 333 (6,25%) | 258 (4,84%) |
| 2019 | 146 (2,71%) | 3006 (55,71%) | 355 (6,58%) | 271 (5,02%) |
| 2020 | 120 (2,40%) | 2798 (55,93%) | 422 (8,43%) | 206 (4,12%) |

50.  В годишния си доклад за 2016 г. (на стр. 13) Националното бюро отбелязва, че въпреки че получава най-голям брой искания за използване на СРС в страната, Специализираният наказателен съд не разполага с достатъчно персонал и ресурси, за да ги обработи правилно. Проверка на Бюрото установява, че този съд не е в състояние да обработи правилно огромния обем документи, свързани с подобни искания. Бюрото обръща внимание на този проблем и в доклада си за 2017 г. (на стр. 16). В доклада за 2019 г. Бюрото отбеляза (на стр. 16), че големият брой искания за използване на СРС, получени от Специализирания наказателен съд, от една страна, е дал възможност на съответните съдии да натрупат повече опит, но от друга страна е довел до прекомерно натоварване, което е причина за грешки. Тази констатация е повторена в доклада за 2020 г. (на стр. 27).

*4. Ред разглеждане на исканията за използване на СРС*

**(а) Съответни законови разпоредби и съдебна практика**

51.  Исканията за използване на СРС, подадени извън рамките на текущи наказателни производства, трябва да бъдат разгледани от компетентния председател или заместник-председател на съда на хартиен носител в рамките на четиридесет и осем часа,[[8]](#footnote-8) като председателят или заместник-председателят може да издаде разрешение или да откаже искането и трябва да мотивира решението си (чл. 15, ал. 1 *in fine* от ЗСРС). За терористични престъпления срокът за вземане на решение е двадесет и четири часа (чл. 15, ал. 2 от ЗСРС). Когато искането е подадено в хода на наказателно производство, законът не определя срок за произнасяне по него,[[9]](#footnote-9) но по същия начин изисква мотивирано решение (чл. 174, ал. 4 от НПК).

52.  Разрешенията и отказите за даване на разрешение за използване на СРС не могат да бъдат обжалвани пред административните съдилища (вж. опр. № 11281 от 28.10.2015 г. по адм. д. № 10354/2015 г., ВАС, V о.).

**(б) Информация за практиката на съдилищата във връзка с разглеждането на искания за използване на СРС, получена на базата на годишните доклади на Националното бюро**

53.  От годишните доклади на Националното бюро за 2015 г. (на стр. 16 и 25), 2016 г. (на стр. 15 - 16 и 26), 2017 г. (на стр. 17 и 27) и 2020 г. (на стр. 29) става ясно, че на практика понякога исканията за използване на СРС се уважават частично и се отхвърлят частично: само по отношение на някои оперативни способи или по отношение на някои престъпления, ако искането се отнася до няколко престъпления, или за по-кратък срок от предлагания.

54.  От годишните доклади на Националното бюро за 2015 г. (на стр. 16), 2016 г. (на стр. 16), 2017 г. (на стр. 17 -19), 2018 г. (на стр. 15 -16), 2019 г. (на стр. 17) и 2020 г. (на стр. 22 -34 и 29) става ясно също, че когато отказват да дадат разрешение, съдиите обясняват конкретно причините за това: че искането не е подадено от компетентен орган; че не е адресирано до компетентен съд; че няма връзка с релевантно престъпление; че не съдържа достатъчно информация, за да обоснове предположение, че обекта на прилагане на СРС е замесен в престъпление, или достатъчно причини защо трябва да бъде дадено разрешение; че не разяснява защо е необходим определен оперативен способ; че не са посочени вече получените резултати (във връзка с искане за удължаване на срока); или че се търси разрешение за използване на СРС извън законоустановените срокове. Според годишния доклад на Бюрото за 2020 г. (стр. 9) най-големият брой откази през тази година се е основавал на липсата на достатъчно информация в искането за използване на СРС, че лицето, по отношение на което се иска прилагането на СРС, са е съпричастно към описаната престъпна дейност.

55.  Според годишните доклади на Националното бюро съдебните решения за разрешаване или отхвърляне на искания за издаване на разрешение за използване на СРС всяка година от 2014 г. насам са следните:

| **Година** | **Издадени разрешения** | **Откази** |
| --- | --- | --- |
| 2014 | 7604 (98,07%)[[10]](#footnote-10) | 150 (1,93%) |
| 2015 | 4034 (85,52%) | 683 (14,48%) |
| 2016 | 4885 (80,16%) | 1209 (19,84%) |
| 2017 | 4624 (77,86%) | 1315 (22,14%) |
| 2018 | 5328 (87,36%) | 771 (12,64%) |
| 2019 | 5396 (89,35%) | 643 (10,65%) |
| 2020 | 5003 (93,20%) | 365 (6,80%) |

**(в) Други официални данни за практиката на съдилищата**

*(i) В Софийски градски съд през 2013 - 2017 г.*

(1) Наказателно и дисциплинарно производство срещу председателя на СГС

56.  В началото на 2015 г. председателят на Софийски градски съд, която встъпва в длъжност през 2011 г., е обвинена в умишлено издаване на разрешения за използване на СРС при липса на законовите предпоставки. Тя е отстранена от поста си на председател на съда и от длъжността съдия, а през м. март 2015 г. подава оставка като председател. В началото на 2016 г. е осъдена за умишлено разрешаване на използване на СРС по отношение на Автоматизирана информационна система „Централен полицейски регистър“ на Министерството на вътрешните работи, използвана от отдела за вътрешна сигурност на министерството за период, надхвърлящ законоустановения максимален срок, в нарушение на член 284в от Наказателния кодекс (вж. параграф 145 по-долу). Тя обаче е оправдана по допълнителното обвинение, че въпросната полицейска информационна система не е била реален „обект“ на прилагане на СРС по смисъла на член 12, ал. 1 от ЗСРС (вж. точка 23, буква в) по-горе). Присъдата на първоинстанционния съд, която е класифицирана (прис. № 1 от 15.01.2016 г. по н. о. х. д. № С-61/2015 г., СГС), се отнася до разрешение, което тя е издала през м. март 2014 г. Тя е потвърдена изцяло при обжалването (вижте реш. № 42 от 10.01.2017 г. по в. н. о. х. д. № 50/2016 г., САС (непубликувано) и реш. № 57 от 19.04.2017 г. по н. д. № 161/2017 г., ВКС, I н. о.).

57.  Успоредно с това през м. март 2015 г. министърът на правосъдието иска от Висшия съдебен съвет да образува дисциплинарно производство срещу (тогавашния) председател на Софийски градски съд и да я освободи от поста ѝ на съдия въз основа на твърдения, че е направила неефективна системата за предварително съдебно разрешение за използване на СРС в Софийски градски съд. Висшият съдебен съвет първоначално отказва да образува такова производство, но по жалба на министъра през м. август 2015 г. Върховният административен съд отменя този отказ (вижте опр. № 9195 от 03.08.2015 г. по адм. д. № 5340/2015 г., ВАС, VI о.) и Висшият съдебен съвет образува производство. Впоследствие то е спряно, за да се изчака произнасянето по наказателните обвинения срещу (вече бившия) председател на съда (вж. параграф 56 по-горе). През м. май 2017 г., след като присъдата ѝ става окончателна, Висшият съдебен съвет я освобождава и от поста ѝ на съдия.

58.  Съгласно декларация, съставена от председателя на Националното бюро за периода 2013-18 г. (вж. параграфи 109 и 112 по-долу) през м. февруари 2020 г. за целите на текущото производство и представена от жалбоподателите, заместниците на този председател на СГС са извършили „четири пъти повече“ нарушения от същото естество, но не са били привлечени към отговорност за нито едно от тях.

(2) Доклад от м. април 2017 г. на заместник-председателите на Софийски градски съд

59.  В *ad hoc* доклад, публикуван през м. април 2017 г., двама заместник-председатели на Софийски градски съд отбелязват редица недостатъци в начина, по който съдът е разглеждал подадените искания за използване на СРС до средата на 2015 г. Някои от тези недостатъци са: а) между 2009 г. и средата на 2014 г. съответните регистри са водени по начин, който не позволява да се установи кой съдия кое искане е разгледал; б) воденето на документацията, свързана с такива искания, е крайно незадоволително; в) по много искания е дадено разрешение, въпреки че не съдържат никакви фактически данни, позволяващи преценка на тяхната обоснованост; г) има много случаи на дублиране на искания и разрешения, издадени по отношение на едно и също лице в един и същи ден; д) много пъти е разрешавано използване на СРС по отношение на чуждестранни посолства в нарушение на международното дипломатическо право; е) по много искания, в които не се посочва престъпление, или касаят престъпления, които не са релевантни, са издавани разрешения; ж) разрешение получават много искания, които е трябвало да бъдат адресирани до други съдилища; з) до м. април 2015 г. всички разрешения по искания за използване на СРС не съдържат никакви мотиви; и) между м. април и м. август 2015 г. разрешенията съдържат, с някои изключения, само бланкетни и общи мотиви; й) в много случаи разрешенията за използване на СРС не са изготвени от съдиите, а от заявителя, като съдиите просто са ги подписали; к) до м. април 2015 г. докладите с резултатите от използването на СРС, които е трябвало да бъдат представени от органите, прилагащи СРС (вж. параграф 106 по-долу), не са били представени на вниманието на съдиите и те не са предприели никакви стъпки за тяхното преглеждане; и (л) компетентните съдии, в нарушение на своите задължения, не са упражнявали какъвто и да е контрол върху унищожаването на неотносима информация, получена чрез СРС.

60.  В доклада се описват стъпките, предприети след м. август 2015 г., за да се отстранят тези недостатъци и да се гарантира ефективното разглеждане на всички искания за използване на СРС, като например: подобряване на съхраняването на документацията; настояване във всички случаи заявителят да предостави всички материали в подкрепа на искането си, както и действителното преглеждане на тези материали от съдия; излагане на пълни мотиви както при разрешаване, така и при отказ на искания, включително за това дали информацията в подкрепящите материали е позволила да се заключи, че лицето, спрямо което се иска прилагане на СРС е съпричастно към извършването на някое от престъпленията, посочени в закона; и пълен контрол върху докладите с резултатите от използването на СРС и унищожаването на неотносимите материали, получени чрез СРС.

(3) Примери за разрешения за използване на СРС, издадени от Софийски градски съд през 2012 -13 г.

61.  Като пример жалбоподателите представят две разрешения за използване на СРС, издадени от (тогавашния) председател на СГС през м. декември 2012 г. и м. февруари 2013 г. И двете са бланки, в които не се споменават никакви данни за конкретния случай или за лицата, които ще бъдат поставени под наблюдение, а само са посочени номерът и датата на искането за използване на СРС, и двете разрешават използването на няколко оперативни способа (наблюдение, подслушване и проследяване), като всички те са за максималния законоустановен срок от шестдесет дни.[[11]](#footnote-11)

*(ii) В Специализирания наказателен съд през 2015 - 2019 г.*

62.  В годишния си доклад за 2015 г. председателят на Специализирания наказателен съд посочва (на стр. 1 - 2), че в средата на годината броят на постъпилите искания за използване на СРС се е увеличил драстично – според него поради промяната на подсъдността за разглеждане на престъпления срещу Републиката (вж. параграф 18 по-горе) от Софийски градски съд към този съд през м. юни 2015 г. По този начин той и неговият заместник са изправени пред значително увеличаване на работното натоварване (вж. таблицата в параграф 49 по-горе). Затова той отправя искане до Висшия съдебен съвет за назначаване на втори заместник-председател на съда.

63.  В годишния си доклад за 2018 г. *временно изпълняващият длъжността* председател на Специализирания наказателен съд заявява (на стр. 7 - 8), че тя и нейните двама заместници отново са изправени пред огромна натовареност, свързана с исканията за използване на СРС, която се е увеличила още повече през тази година (вж. таблицата в параграф 49 по-горе). Годишният доклад за 2019 г. съдържа подобни констатации (на стр. 5).

64.  В присъда от м. юни 2019 г. (прис. № 34 от 24.06.2019 г. по н. о. х. д. № 1907/2014 г., СпНС, не е ясно дали е влязла в сила) Специализираният наказателен съд описва подробно съдържанието на единадесет разрешения, издадени от заместник-председателя на Софийски градски съд и председателя или заместник-председателя на Специализирания наказателен съд през 2011 - 2012 г. Той отбеляза, че всички те са готови формуляри с изцяло бланкетно съдържание и без посочване на конкретния случай, за който се отнасят, с изключение на номера на искането за използване на СРС. Освен това съдът установява, че всички тези разрешения всъщност са съставени от други лица и просто са подписани от съответните съдии, и заключава, че няма основание да се приеме, че тези съдии реално са проверили законовите предпоставки за издаване на разрешенията.

65.  В присъда от м. декември 2019 г. (прис. № 55 от 09.12.2019 г. по н. о. х. д. № 1590/2019 г., СпНС) Специализираният наказателен съд прави подобни констатации за деветнадесет разрешения за използване на СРС, издадени от председателя и двамата заместник-председатели на съда през 2017 - 2018 г. Съдът отбеляза, че всички искания за използване на СРС, на базата на които са издадени разрешенията, съдържат подробни мотиви защо трябва да бъде дадено разрешение. От друга страна, всички разрешения представляват документи от една страница, които не съдържат препратка (с изключение на препратка към номера на искането) към отделните случаи, за които се отнасят, и които в общи линии са формулирани еднакво в достатъчна степен, че да могат да се отнасят до искане за използване на всяко възможно СРС по Закона от 1997 г. или Наказателно - процесуалния кодекс. Единствено в диспозитива на всяко от разрешенията е посочено, че случаят се отнася до предполагаемо престъпление по чл. 321 от Наказателния кодекс (вж. параграф 19 по-горе). Всички, с изключение на едно, разрешават използване на СРС за максималния законоустановен срок от два месеца и всички разрешават използването на няколко оперативни способа: наблюдение; подслушване; проследяване; и белязване и проверка на кореспонденцията или компютризираната информация (вж. параграф 11 по-горе). По този начин е невъзможно да се спекулира дали съдиите, които са издали разрешенията, всъщност са разгледали исканията за тях (въпреки че отсъствието на преглеждане не може да се презюмира). Съдът също така отбеляза, че неговата статистика за 2017 - 2018 г. показва, че е получавал средно по дванадесет или тринадесет искания на ден през 2017 г. и тринадесет или четиринадесет искания на ден през 2018 г., и че практиката да не се посочват конкретни мотиви е обща. Въз основа на констатациите си за липса на мотиви в разрешенията, съдът изключва получените доказателствени средства.

66.  През м. февруари 2021 г. Апелативният специализиран наказателен съд отменя посочената присъда. Наред с другото, той постановява, че не може да се очаква, че при вземане на решение за издаване на разрешение за използване на СРС съдията ще коментира доказателствата. Нито ЗСРС, нито Наказателно-процесуалният кодекс изискват това. Всичко, което съдията, разглеждащ искане за използване на СРС, е трябвало да провери, е дали са налице формалните изисквания за разрешаването му (вижте реш. № 260002 от 10.02.2021 г. по в. н. о. х. д. № 245/2020 г., АСпНС, окончателно).

67.  Според изтекла информация, появила се през първата половина на 2021 г., между м. юли 2020 г. и м. февруари 2021 г. по отношение на много опозиционни политици и журналисти, както и на стотици участници в анти-правителствените протести в България през 2020 г., са били неправомерно използвани СРС въз основа на разрешения, издадени от Специализирания наказателен съд във връзка с твърдения, че ще се опитат да извършат държавен преврат. Когато разглежда въпроса в Парламента на 28 юли 2021 г., министърът на вътрешните работи заявява, наред с другото, че разполага с документи, които показват, че спрямо най-малко 123 протестиращи са били прилагани СРС въз основа на разрешения, издадени от Специализирания наказателен съд, и изразява сериозни опасения относно законността на това прилагане на СРС, което според него е било разрешено безкритично от този съд. През м. юли 2021 г. Парламентът създава *ad hoc* комисия, която да разследва въпроса. Комисията приема доклада си на 13 септември 2021 г.; той и досега остава класифициран. На 15 септември 2021 г. Парламентът одобрява доклада на закрито пленарно заседание.

*(iii) В обобщение*

68.  С решение от м. февруари 2014 г. Софийският апелативен съд постановява, че използването на шаблони за издаване на разрешения за използване на СРС може да бъде прието, тъй като, за разлика от основанията за отказ на искане за използване на СРС, причините за разрешаване на такова на практика не се различават (вижте реш. № 365 от 14.02.2014 г. по в. н. о. х. д. № 653/2013 г., САС, потвърдено с реш. № 189 от 03.02.2015 г. по н. д. № 515/2014 г., ВКС, II н. о.).

**(г) Изисквания за публично оповестяване**

69.  Председателите на окръжните и апелативните съдилища и председателят на Върховния касационен съд трябва да включат в годишните доклади на съдилищата данни за броя на а) издадените разрешения и б) веществените доказателствени средства, изготвени въз основа на прилагането на СРС (чл. 29, ал. 8 от ЗСРС).

*5. Допълнителен контрол от страна на органите, използващи специални разузнавателни средства*

70.  Единствените органи, които имат правомощия да използват специални разузнавателни средства, са: а) Държавна агенция „Технически операции“ към Министерския съвет, б) специализирана дирекция „Технически операции“ на Държавна агенция „Национална сигурност“, в) Държавна агенция „Разузнаване“ и разузнавателните служби на Министерството на отбраната (в рамките на конкретната им компетентност), и г) (но само по отношение на служители под прикритие, контролирани доставки и доверителни сделки) Министерството на вътрешните работи (чл. 20, ал. 1 и 2 от ЗСРС и чл. 175, ал. 1 от Наказателно - процесуалния кодекс). В мотивите към законопроекта от 2013 г. (№ [354 -01-19](https://parliament.bg/bills/42/354-01-19.pdf)) за изменение на ЗСРС, което довежда до това положение, се посочва, че причината повечето операции по използване на СРС да бъдат поверени на специализирана структура, отделна от Министерството на вътрешните работи, е да се гарантира, че тези, които прилагат СРС, ще бъдат отделени от тези, които отправят искания за използване на СРС, и ще действат независимо и като допълнителна гаранция срещу злоупотреби.

71.  Когато получат разрешение за използване на СРС, ръководителят на Държавна агенция „Технически операции“, ръководителят на Държавна агенция „Национална сигурност“, главният секретар на Министерството на вътрешните работи или надлежно упълномощен заместник, според случая, трябва да издадат последващо разпореждане за прилагане на СРС (чл. 16, ал. 1 и 2 от ЗСРС и чл. 175, ал. 2 от Наказателно - процесуалния кодекс). Тази допълнителна стъпка може да бъде пропусната в неотложни случаи, но ръководителят на съответния орган или надлежно упълномощеният заместник трябва да бъде информиран незабавно (чл. 17 от ЗСРС).

72.  Според годишните доклади на Националното бюро тази допълнителна стъпка е била пропусната в следните случаи:

| **Година** | **Пропуснато последващо разпореждане от ръководителя на съответния орган** |
| --- | --- |
| 2014 | 742 (17,70%) |
| 2015 | 604 (22,09%) |
| 2016 | 685 (25,28%) |
| 2017 | 640 (23,29%) |
| 2018 | 607 (19,93%) |
| 2019 | 548 (16,56%) |
| 2020 | 435 (14,38%) |

73.  Тези структури не трябва да започват прилагането на СРС или да го прекратят, ако а) разрешението за използване на СРС е издадено за престъпление, извън посочените в чл. 3, ал. 1 от ЗСРС., или ако б) искането или разрешението за използване на СРС съдържат явни грешки (член 22, ал. 3, т. 1 и ал. 3, т. 2 от ЗСРС). В такива случаи органът трябва да уведоми заявителя и съдията, издал разрешението за използване на СРС. След това съдията трябва да отмени, измени или да потвърди разрешението, според случая, да изпрати решението си на прилагащия СРС орган и да информира заявителя. Ако съдията промени или потвърди разрешението, операцията по прилагане на СРС трябва да продължи (чл. 22, ал. 5 от ЗСРС).

74.  В годишния си доклад за 2015 г. Националното бюро посочва (на стр. 17), че дори преди измененията на ЗСРС, влезли в сила през м. юни и септември 2015 г., с които е въведена тази допълнителна гаранция, то е дало задължителни указания на компетентните органи да не започват прилагането на СРС, ако забележат такива грешки в исканията или разрешенията за използване на СРС.

75.  Според годишните доклади на Националното бюро за 2016 г. (стр. 17), 2018 г. (стр. 17) и 2019 г. (стр. 18 -19) органите по СРС са задействали тази допълнителна гаранция в следните случаи:

| **Година** | **Сезирания съгласно чл. 22, ал. 3 от Закона от 1997 г.** |
| --- | --- |
| 2016 | 9 |
| 2018 | 3 |
| 2019 | 4 |

76.  Годишните доклади на Бюрото за 2014, 2015, 2017 и 2020 г. не съдържат такава информация.

*6. Последващо разрешение в неотложни случаи*

77.  В случаите на непосредствена опасност от извършване на тежко умишлено престъпление (от изброените в чл. 3, ал. 1 от ЗСРС - вж параграф 18 по-горе) или при непосредствена заплаха за националната сигурност специалните разузнавателни средства могат да се използват и без разрешение на съда въз основа на разпореждане на председателя на Държавна агенция "Технически операции", председателя на Държавна агенция "Национална сигурност" или главния секретар на МВР (чл. 18, ал. 1 от Закона от 1997 г.). Използването се прекратява, ако компетентният съдия не издаде разрешение в рамките на двадесет и четири часа; този съдия трябва също да реши дали вече получената информация трябва да бъде съхранена или унищожена (член 18, ал. 2). Ако бъде издадено, разрешението потвърждава със задна дата извършените действия, предприети преди издаването му (чл. 18, ал. 3).

78.  Според годишните доклади на Националното бюро всяка година тази неотложна процедура е използвана по отношение на следния брой лица:

| **Година** | **Лица, спрямо които се прилагат СРС без предварително разрешение** |
| --- | --- |
| 2014 | 125 (3,00%) |
| 2015 | 29 (1,10%) |
| 2016 | 49 (1,78%) |
| 2017 | 28 (1,02%) |
| 2018 | 7 (0,23%) |
| 2019 | 15 (0,45%) |
| 2020 | 4 (0,13%) |

**Е. Максимален срок на прилагането на СРС**

79.  Съгласно чл. 21, ал. 1 и 2 от ЗСРС и чл. 175, ал. 3 и 4 от Наказателно-процесуалния кодекс максималният срок, през който могат да се прилагат специални разузнавателни средства, е:

а)  до двадесет дни, когато се прилагат за идентифициране на лица (вж. параграф 23, буква в) по-горе); този срок може да бъде удължен с искания за удължаване до общо шестдесет дни;

б)  до две години, когато се прилагат във връзка с дейности, свързани с националната сигурност (вж. параграф 23, буква б) по-горе), за предотвратяване на тежки умишлени престъпления срещу Републиката; този срок може да бъде удължен с искания за удължаване до общо три години;

в)  до два месеца във всички останали случаи (вж. параграф 23, букви а), г) и д) по-горе); този срок може да бъде удължен с искания за удължаване до общо шест месеца.[[12]](#footnote-12)

80.  В годишния си доклад за 2018 г. Националното бюро посочва, че двугодишният срок за прилагане на СРС при риск за националната сигурност (вж. параграф 79, буква б) по-горе) е една от възможните причини за намаляване броя искания за използване на СРС, подадени от Държавната агенция „Национална сигурност“ от 2015 г. насам (вж. таблицата в параграф 38 по-горе).

81.  Срокът започва да тече от датата, определена с разрешението за използване на СРС (чл. 21, ал. 4 от ЗСРС).

**Ж. Ситуации, при които прилагането на СРС трябва да бъде прекратено**

82.  Съгласно чл. 22, ал. 1, 2 и 3 от ЗСРС и чл. 175, ал. 6 от Наказателно-процесуалния кодекс, с изключение на (специалните) случаи, в които органът по СРС трябва да прекрати прилагането на СРС, ако установи, че се отнася до нерелевантно престъпление, или че искането или разрешението за използване на СРС са опорочени поради явна грешка (вж. параграф 73 по-горе), прилагането на СРС трябва да бъде прекратено, ако а) разрешеният срок е изтекъл; б) целите са постигнати; в) прилагането не дава резултати; г) съществува опасност от разкриване на използваните оперативни способи или д) когато прилагането е невъзможно.

83.  Във всеки от тези случаи органът по СРС трябва да уведоми съдията, издал разрешението (чл. 22, ал. 4 от ЗСРС и чл. 175, ал. 7 от Наказателно-процесуалния кодекс). Член 22, ал. 4 изисква и уведомяване на запитващия орган. В член 175, ал. 7 се изисква в уведомлението да се изложат мотивите във всички възможни случаи, докато по чл.22, ал. 4 се изискват мотиви само ако прилагането е било прекратено, тъй като а) е съществувал риск използваните оперативни способи да бъдат разкрити или б) прилагането е станало невъзможно.

**З. Обработка на информация, получена чрез прилагане на специални разузнавателни средства**

*1. Цели, за които може да се използва информацията*

84.  Общото правило е, че информацията, получена чрез специални разузнавателни средства, може да се използва само за предотвратяване, разкриване или доказване на престъпления или за защита на националната сигурност (чл. 32 от ЗСРС).

85.  Използването на такава информация за друга цел е престъпление, което се утежнява, ако е извършено от длъжностно лице, което е получило достъп до информацията в кръга на службата си (чл. 145а, ал. 1 и 2 от Наказателния кодекс). Изглежда, че до момента е имало само една присъда по тази разпоредба, тази на високопоставен полицейски служител, който е предавал данни от прилагането на СРС на журналисти и други лица (вижте прис. № 58 от 11.06.2014 г. по н. о. х. д. № 457/2012 г., ОС-Велико Търново, потвърдено в съответната част от реш. № 149 от 31.07.2015 г. по в. н. о. х. д. № 389/2014 г., АС-Варна, оттеглено обжалване: вижте Р-12 от 19.01.2016 г. по н. д. № 1372/2015 г., ВКС, III н. о.).

*2. Средства за прихващане на електронни съобщения*

86.  По отношение на електронните съобщения всички доставчици на съобщителни услуги в страната са длъжни да осигурят на двата основни органа за СРС (Държавна агенция "Технически операции" и Дирекция „Технически операции“ на Държавна агенция „Национална сигурност“ – вж. параграф 70 по-горе) достъп в реално време до всички комуникации, преминаващи през техните мрежи, за да могат да бъдат прихванати в съответствие със ЗСРС (чл. 304 от Закона за електронните съобщения от 2007 г.). Доставчиците на съобщителни услуги имат същото задължение към съдилищата и разследващите органи (чл.172, ал. 3 от Наказателно - процесуалния кодекс). Те трябва за своя сметка да инсталират и експлоатират интерфейси, които могат автоматично да прихващат и да предават сигурно съобщения на органите по СРС (чл. 305, ал. 1, 308 и 309 от Закона от 2007 г.).

*3. Етапи на обработка*

**(а) „Материален носител“ и „производен носител на данни“**

87.  Всеки оперативен способ за СРС (с изключение на използването на служители под прикритие – вижте реш. № 112 от 02.06.2016 г. по в. н. о. х. д. № 81/2016 г., ВтАС, потвърдено от реш. № 198 от 05.12.2016 г. по н. д. № 766/2016 г., ВКС, I н. о.) трябва да има за резултат записване на получената чрез него информация: фотографиране, видеозаписване, звукозаписване и филмиране (чл. 11 и 24 от ЗСРС.).

88.  Органът по СРС трябва да съхранява „материалния носител“ за срока, през който е в ход операцията по прилагане на СРС (чл. 25, ал. 6 от Закона от 1997 г.). Този „материален носител“ се използва за създаване на „производен носител на данни“, който органът по СРС трябва да изпрати на запитващия орган заедно с (при поискване от последния) всички снимки, записи, скици или планове (чл. 25, ал. 1, 4 и 5).

89.  „Производният носител на данни“ може да бъде в писмена или друга (на практика електронна) форма (чл. 25, ал. 1 от ЗСРС). Ако е технически осъществимо, той трябва да бъде предоставен на запитващия орган чрез автоматизирана мрежа (чл. 25, ал. 2). Съдържанието му трябва напълно да съответства на това на „материалния носител“ (чл. 25, ал. 3).

**(б) Веществено доказателствено средство**

90.  Ако въз основа на този „производен носител на данни“ запитващият орган установи, че прилагането на СРС е осигурило полезна информация, той трябва незабавно (и във всеки случай не повече от десет дни след приключването на прилагането на СРС) да уведоми органа по СРС да изготви веществено доказателствено средство въз основа на „материалния носител“ (чл. 26 и чл. 27, ал. 2 от ЗСРС). Въпреки че ЗСРС не уточнява какво точно представлява това веществено доказателствено средство, от съдебната практика на наказателните съдилища става ясно, че това са компютърни файлове, съдържащи аудио- или видеозаписи, в зависимост от случая (вж. например прис. № 50 от 03.06.2011 г. по н. о. х. д. № 424/2011 г., ОС-Варна, потвърдена в съответната част от реш. № 157 от 21.11.2011 г. по в. н. о. х. д. № 313/2011 г., ВнАС, и след това от реш. № 83 от 19.06.2012 г. по н. д. № 3135/2011 г., ВКС, II н. о.; реш. № 172 от 18.04.2012 г. по н. д. № 398/2012 г., ВКС, I н. о.; прис. № 56 от 16.11.2016 г. по н. о. х. д. № 379/2014 г., ОС-Плевен, потвърдена от реш. № 124 от 03.05.2017 г. по в. н. о. х. д. № 69/2017 г., ВтАС, необжалвано; и реш. № 1 от 17.02.2017 г. по н. д. № 1143/2016 г., ВКС, III н. о.). Вещественото доказателствено средство не трябва да се бърка с веществените доказателства и поради това съдът, който гледа наказателно дело, не може законно да разпореди неговото унищожаване (вижте опр. № 145 от 17.06.2016 г. по в. ч. н. д. № 156/2016 г., ОС-Видин). Когато органът по СРС изготвя това веществено доказателствено средство, той трябва да състави протокол, в който се посочват времето, мястото и физическите условия на прилагането на СРС, използваното оборудване и способи, получените данни за целта и текстовото възпроизвеждане на вещественото доказателствено средство (чл. 27, ал. 1 и чл. 29, ал. 4 от ЗСРС и чл. 132, ал. 2 от Наказателно-процесуалния кодекс). В този протокол той трябва също така да посочи искането за използване на СРС, разрешението за използване на СРС и последващото разпореждане (както и на съгласието на лицата, ако СРС се прилага с цел защита на лице или по отношение на свидетел) (чл. 29, ал. 3 от Закона от 1997 г. и чл. 132, ал. 3 от Наказателно-процесуалния кодекс). Въпреки че Законът от 1997 г. не го посочва изрично, на практика това веществено доказателствено средство не може да възпроизвежда всички части на „материалния носител“ (вж. например реш. № 384 от 08.07.2017 г. по в. н. о. х. д. № 1182/2016 г., САС, потвърдено с реш. № 314 от 25.01.2018 г. по н. д. № 1118/2017 г., ВКС, I н. о.). Изглежда това следва и от правилото, че всички части от „материалния носител“, които не се използват за изготвянето му, трябва да бъдат унищожени (вж. точка 94 по-долу).

91.  Вещественото доказателствено средство трябва да бъде изготвено в два екземпляра, единият от които трябва да бъде изпратен запечатан на запитващия орган, а другият, отново запечатан, на съдията, издал разрешението за използване на СРС. Това трябва да се случи не повече от двадесет и четири часа след изготвянето им (чл. 29, ал. 1 от ЗСРС и чл. 176, ал. 1 от Наказателно - процесуалния кодекс). Запитващият орган може да изиска допълнителни копия от вещественото доказателствено средство (чл. 29, ал. 1 *in fine* и чл. 176, ал. 2).

92.  Веществените доказателствени средства, получени от запитващия орган, трябва да бъдат съхранявани от него до образуване на наказателно производство във връзка с тях; когато такова производство бъде образувано, средствата се съхраняват от прокуратурата и съда, който разглежда делото (чл. 31, ал. 1 и 2 от Закона от 1997 г.). Законът не определя правила как да се съхранява това средство. Според правителството въпросът е уреден във вътрешните правила на съответния орган, с изключение на случаите, в които по някаква причина средството се счита за класифицирано, като в този случай съхранението му е уредено от съответните разпоредби на Закона за защита на класифицираната информация от 2002 г. (вж. параграфи 102 и 103 по-долу). Според правителството след образуване на наказателното производство вещественото доказателствено средство се съхранява в съответствие с правилата за съхраняване на доказателства от органите на прокуратурата и съдилищата. В чл. 125, ал. 3 от Наказателно - процесуалния кодекс се предвижда към наказателното дело да се прилагат веществени доказателствени средства, изготвени на основание прилагането на СРС. Нито Правилникът за администрацията в съдилищата, издаден от Висшия съдебен съвет през 2017 г., нито Правилникът за администрацията на Прокуратурата на Република България, издаден от Висшия съдебен съвет през 2013 г., които уреждат съхранението на дела съответно от съдилищата и прокурорските органи, съдържат разпоредби, които се отнасят конкретно до съхранението или унищожаването на веществени доказателствени средства, изготвени на базата на прилагане на СРС.

93.  Според годишните доклади на Националното бюро броят на веществените доказателствени средства, изготвени въз основа на информацията, получена чрез прилагане на СРС, и съотношението между тези веществени доказателствени средства и броя на лицата, по отношение на които се прилагат СРС всяка година, са следните:

| **Година** | **Брой веществени доказателствени средства** | **Съотношение спрямо броя на лицата, по отношение на които се прилагат СРС** |
| --- | --- | --- |
| 2010 | 3461 | 60,06% |
| 2011 | 3603 | 44,02% |
| 2012 | 3347 | 56,71% |
| 2013 | 1602 | 48,38% |
| 2014 | 1084 | 24,46% |
| 2015 | 1677 | 57,10% |
| 2016 | 1431 | 46,33% |
| 2017 | 1670 | 55,52% |
| 2018 | 1714 | 56,27% |
| 2019 | 1124 | 33,96% |
| 2020 | 1089 | 36,01% |

**(в) Унищожаване на информация, която не е от значение**

94.  Ако е изготвено веществено доказателствено средство, а) всички части от „материалния носител“, които не се използват за изготвянето му, и б) „производният носител на данни“ трябва да бъдат унищожени от органа по СРС и от запитващия орган в срок от десет дни след края на прилагането на СРС. Това трябва да бъде направено и протоколирано от тричленни комисии, назначени от ръководителите на съответните органи (чл. 31, ал. 3 от ЗСРС).

95.  Ако, обратно, прилагането на СРС не е осигурило полезна информация, органът по СРС не е длъжен да изготвя веществено доказателствено средство и трябва да унищожи всяка получена информация в срок от десет дни по същия начин, както описания в параграф 94 по-горе (чл. 28 във връзка с чл. 31, ал. 3 от ЗСРС).

96.  Има три докладвани случая, в които на полицейски служители са наложени дисциплинарни наказания за това, че не са осигурили навременното унищожаване на информацията от прилагането на СРС (вижте реш. № 2466 от 11.10.2013 г. по адм. д. № 1804/2013 г., АдмС-Варна; реш. № 100 от 20.03.2019 г. по адм. д. № 708/2018 г., АдмС-Добрич; и реш. № 101 от 20.03.2019 г. по адм. д. № 709/2018 г., АдмС-Добрич).

97.  Във всички случаи, в които унищожаването на информацията от прилагането на СРС се изисква от закона, органът по СРС трябва в срок от седем дни да изпрати на запитващия орган протокола, удостоверяващ унищожаването, заедно с искането и разрешението за използване на СРС (чл. 31, ал. 4 от ЗСРС). След това запитващият орган трябва да запази тези документи (чл. 31, ал. 5).

98.  По изключение от общите правила за унищожаване, всяка информация, получена чрез прилагане на СРС по съображения за национална сигурност, трябва да се съхранява от съответния запитващ орган (съответната дирекция на Държавната агенция „Национална сигурност“, Служба "Военно разузнаване" към министъра на отбраната и Държавна агенция „Разузнаване“) в продължение на петнадесет години след края на прилагането на СРС (чл. 31, ал. 6 от Закона от 1997 г.). След това тя трябва да бъде унищожена от специална тричленна комисия, назначена от ръководителя на съответния орган (чл. 31, ал. 7).

99.  Всички горепосочени правила за унищожаване на информация очевидно са приложими само когато прилагането на СРС е извършено извън рамките на текущо наказателно производство. Когато то е извършено в хода на наказателно производство, правилото е, че при преустановяване прилагането на СРС, съдията, издал разрешението, трябва да бъде информиран за резултатите от него. Ако информация, получена в резултат от прилагането на СРС, не се използва за изготвяне на веществено доказателствено средство, съдията трябва да разпореди нейното унищожаване (чл. 175, ал. 7 от Наказателно - процесуалния кодекс). В докладите си за 2015 г. (стр. 23), 2016 г. (стр. 21), 2019 г. (стр. 20) и 2020 г. (стр. 36) Националното бюро отбелязва, че несъответствието между двата режима понякога става причина за забавяне на унищожаването.

*4. Правила за разрешеното използване на резултати, получени извън направеното искане*

100.  Ако при прилагането на СРС се получат резултати, които надхвърлят първоначално търсената цел, председателят на Държавна агенция "Технически операции" или на Държавна агенция „Национална сигурност“ (в зависимост от това кой е извършил прилагането на СРС) трябва да информира заявителя за тези допълнителни резултати в рамките на двадесет и четири часа (чл. 30, ал. 1 от ЗСРС). На свой ред заявителят трябва да информира съответния орган в рамките на още двадесет и четири часа (чл. 30, ал. 2). Специално правило урежда ситуацията, при която допълнителните резултати се отнасят до служителя, който е поискал използването на СРС, или до по-висшестоящ от него служител: в този случай председателят (или изрично упълномощен заместник) на съответния орган по СРС (Държавна агенция „Технически операции, Държавна агенция „Национална сигурност“ или Министерството на вътрешните работи) трябва незабавно да изпрати допълнителните резултати на главния прокурор или на изрично упълномощен заместник (чл. 30, ал. 3).

101.  Тези допълнителни резултати могат да се използват като доказателства в наказателното производство само ако се отнасят до друго тежко умишлено престъпление (чл. 177, ал. 2 и 3 от Наказателно - процесуалния кодекс).

* + - 1. Релевантни разпоредби от Закона за защита на класифицираната информация от 2002 г.

102.  Информацията за специалните разузнавателни средства (технически устройства и/или способите за тяхното прилагане), използвани по предвидения от закона начин, е държавна тайна (точка 6 от част II от Приложение № 1 към Закона за защита на класифицираната информация от 2002 г.). До 2013 г. такава е и информацията, получена в резултат на използването на такива средства (точка 8 от част II на Приложение № 1). През 2013 г. точка 8 е отменена.

103.  В тълкувателно решение от 2014 г., което засяга главно въпроса дали може да бъде изключена публичността на съдебните заседания по наказателни дела, по които се представят доказателства, получени чрез специални разузнавателни средства (тълк. реш. № 4 от 03.12.2014 г. по т. д. № 4/2014 г., ВКС, ОСНК), Върховният касационен съд отбелязва, наред с другото, че ефектът от отмяната на точка 8 е, че изготвянето на вещественото доказателствено средство на базата на информация, получена чрез специални разузнавателни средства, само по себе си вече не е достатъчно за третирането на това веществено доказателствено средство като класифицирана информация, дори и да се споменава видът на способа (наблюдение, подслушване, проследяване и т.н.), използван за получаване на информацията.

104.  В изявление, приложено към становището на правителството, Държавна агенция „Технически операции“ (вж. параграф 70, буква а) по-горе) посочва, че според нейното тълкуване ефектът от точка 6 на част II от Приложение № 1 към Закона за защита на класифицираната информация от 2002 г. е, че както „материалният носител“, получен в резултат на прилагането на СРС, така и „производният носител на данни“ са класифицирана информация (вж. параграфи 87 и 88 по-горе).

И. Органи, които упражняват контрол върху използването на специални разузнавателни средства

* + - 1. Съдии, издали разрешение за използване на СРС

105.  Както е отбелязано в параграф 83 по-горе, когато прилагането на СРС приключи поради каквато и да е причина, органът по СРС трябва да уведоми съдията, издал разрешението за неговото използване.

106.  В срок от един месец след края на операцията по прилагане на СРС заявителят трябва да представи доклад на съдията. Докладът трябва да посочва вида на използваните СРС, началото и края на прилагането им, както и дали в резултат от прилагането е изготвено веществено доказателствено средство или дали получената информация е била унищожена (чл. 29, ал. 7 от ЗСРС). Ако въз основа на информацията, получена в резултат на прилагането на СРС е изготвено веществено доказателствено средство (вж. точка 90 по-горе), копие от него и от придружаващите го документи трябва да се изпратят запечатани на съдията (вж. параграф 91 по-горе).

107.  Както е отбелязано в параграф 99 по-горе, за прилагането на СРС в хода на наказателното производство съдията, издал разрешението, трябва да бъде информиран незабавно след края на прилагането и ако получената по този начин информация не се използва за изготвяне на веществено доказателствено средство, той трябва да разпореди нейното унищожаване. Съдията трябва също така да получи запечатано копие на всяко веществено доказателствено средство в резултат от прилагане на СРС, в рамките на двадесет и четири часа от неговото изготвяне (вж. параграф 91 по-горе).

* + - 1. Национално бюро

108.  Националното бюро, което е възстановено като „независим държавен орган“ през 2013 г., е избрано за първи път през м. декември 2013 г. и започва своята работа в началото на 2014 г. (вж. параграф 16 по–горе), има за задача а) да упражнява наблюдение на процедурите по разрешаване, прилагане и използване на специални разузнавателни средства, както и по съхраняването и унищожаването на информацията, получена чрез такива средства, и б) да защитава правата на лицата, засегнати от незаконното използване на такива средства (чл. 34б, ал. 1 от ЗСРС). То е постоянен орган, подпомаган от собствена администрация (чл. 34б, ал. 4). Според годишните доклади на Бюрото през 2014 - 2015 г. администрацията му се състои от петнадесет служители; през периода 2016 - 2020 г. този брой е намален на четиринадесет; всички те имат необходимото разрешение за достъп до класифицирана информация с ниво на класификация „Строго секретно“. Бюрото ежегодно представя доклад на Парламента (чл. 34б, ал. 7).

* + - * 1. Начин на избиране и мандат на членовете на Националното бюро

Законови разпоредби

109.  Националното бюро има председател, заместник-председател и трима членове, всички избрани от Парламента за петгодишен мандат (чл. 34в, ал. 1 от ЗСРС). Те трябва да имат най-малко осем години юридически стаж или професионален стаж в службите за сигурност или в службите за обществен ред и да са получили възможно най-високо ниво на достъп до класифицирана информация – ниво на класификация „строго секретно“ (чл. 34в, ал. 2 от ЗСРС). Разрешенията за достъп до това най-високо ниво на класификация се издават след специална процедура за проверка, която трябва да се извърши от Държавна агенция „Национална сигурност“ (чл. 49, ал. 1 и 2 от Закона за защита на класифицираната информация от 2002 г.).[[13]](#footnote-13)

110.  След като предложенията за членове на Националното бюро бъдат получени от Парламента (ЗСРС не посочва кой може да направи тези предложения, но както през 2013 г., така и през 2018 г. всяко от предложенията се прави от различна парламентарна група въз основа на специални процедурни правила, приети от Парламента във всеки от тези случаи), ръководителят на специализираната парламентарна комисия изпраща всички материали за кандидатите на Държавна агенция „Национална сигурност“ за извършване на проучване за надеждност, което трябва да приключи в рамките на един месец. След това парламентарната комисия разглежда предложенията в рамките на седем дни, след което провежда изслушвания на кандидатите, които отговарят на изискванията, и в рамките на още седем дни представя доклад. След това Парламентът гласува за всеки от кандидатите поотделно и избира кои от тях ще станат председател и заместник-председател. След това всички те полагат клетва (чл. 34г от ЗСРС).

111.  След края на мандата си членовете на Националното бюро трябва да бъдат възстановени на предишните си длъжности (чл. 34в, ал. 4). Техният мандат може да бъде прекратен преждевременно от Парламента, ако: а) подадат оставка, б) реално не са били в състояние да изпълняват задълженията си в продължение на три последователни месеца, в) са престанали да отговарят на условията за заемане на длъжността или г) е открит конфликт на интереси след официална процедура съгласно специалното законодателство за противодействие на корупцията (чл. 34в, ал. 6).

Членове на Националното бюро за периода 2013 - 2018 г. и след 2018 г.

112.  Трима от петимата първоначални членове на Националното бюро, избрани през 2013 г., включително неговият председател и заместник-председателят му, са с юридическо образование и юридически стаж. Само един от членовете, избрани през м. декември 2018 г. (който е член и в периода 2013 - 2018 г.), е с юридическо образование и стаж (като адвокат). Според официалния уебсайт на Бюрото[[14]](#footnote-14) непосредствено преди избирането му на поста през м. декември 2018 г. настоящият председател е работил десет години (2008 - 2018) в Държавна агенция „Национална сигурност“; избраният през 2018 г. заместник-председател също е работил в продължение на двадесет и шест години (1981 - 2007 г.) в службите за сигурност; а един от редовните членове е работил дълги години (1983 - 2009 г.) в Министерството на вътрешните работи.

113.  За тримата редовни членове на Националното бюро настоящият мандат (2018 - 2023 г.) е вторият им мандат, като и тримата са били членове и през 2013 - 2018 г.

114.  Мандатът на първия заместник-председател на Националното бюро, избран през 2013 г., е предсрочно прекратен от Парламента през м. март 2018 г. с мотива, че вече не отговаря на условията да бъде член на Бюрото (вж. точка 111, буква в) по-горе), тъй като през м. юли 2017 г. Държавна агенция “Национална сигурност“ е отнела разрешението му за достъп (по-късно стана ясно, че цитираната причина за отнемането е била, че той е разкрил на няколко души информация за използването на специални разузнавателни средства в нарушение на законовото изискване за запазване на тази информация в тайна) и през м. януари 2018 г. Върховният административен съд потвърждава отнемането на разрешението.[[15]](#footnote-15)

115.  В началото на м. юни 2021 г. заместник-председателят на Националното бюро, избран през 2018 г., е поставен под различни санкции от органите на Съединените американски щати съгласно член 1, буква а), подточка ii), буква Б, точка 1 от Изпълнителна заповед 13818 (Блокиране на имуществото на лица, замесени в тежки нарушения на правата на човека или корупция), издадена през 2017 г., и съгласно член 7031, буква в) (Антиклептокрация и права на човека) на Закона за Държавния департамент, външните операции и свързани с тях програми, което се дължи съответно на това, че той е „отговорен или съучастник в или пряко или косвено замесен в корупционни дейности“, както и на това, че е „участва(л) в сериозни корупционни дейности“. В средата на м. юни 2021 г. той подава оставка, а на 28 юли 2021 г. парламентът единодушно я приема.

(б) Правомощия на Националното бюро

* + - * 1. *За достъп до материали*

116.  При изпълнение на своите задължения Националното бюро може а) да изисква съответната информация от органите, оправомощени да искат използване на СРС, съдиите, които разглеждат искания за използване на СРС, и органите по СРС, и б) да инспектира материалите (искания и разрешения за използване на СРС и последващи разпореждания и протоколи, свързани с унищожаването на информацията, получена от прилагане на СРС), както и регистрите, водени от тези органи (чл. 34е, ал. 1, т. 1 и т. 2 от ЗСРС.).

117.  Членовете на Националното бюро и неговите служители имат достъп до (а) всички документи, свързани с използването или прилагането на специални разузнавателни средства, (б) всички документи, свързани със съхраняването или унищожаването на информацията, придобита чрез такива средства, и (в) всяко помещение, в което се съхраняват такива документи (чл. 34е, ал. 4 от ЗСРС).

118.  В доклада си за 2017 г. Националното бюро посочва (на стр. 23), че Държавна агенция „Национална сигурност“ не му позволява да инспектира материалите, на които се основават изготвените от агенцията искания за използване на СРС. По този начин агенцията възпрепятства ефективния надзор от страна на Бюрото, тъй като един от аспектите на този надзор е дали исканията за използване на СРС се основават на реални предположения за престъпно поведение. Бюрото също така посочва (на стр. 24), че поради многобройните случаи на предоставяне на неточна информация от страна на Държавна агенция „Технически операции“ през периода 2014 - 2017 г. то е трябвало да отправя нови искания за информация в около 200 отделни случая. За Бюрото е трудно да установи дали това е умишлено възпрепятстване с цел прикриване на нередности.

119.  През м. ноември 2015 г. главният прокурор издава инструкция до всички прокурори за начина, по който на Националното бюро да бъде предоставен достъп до материалите, съхранявани от прокуратурите, в хода на неговите проверки. Съгласно точка 7 от посочената инструкция (частично изменена през м. април 2019 г.) на членовете на Бюрото и на неговите служители следва да се предостави достъп до: искания за използване на СРС, приложени към тях информационни бележки, разрешения за използване на СРС (или откази от издаване на такива разрешения), последващи разпореждания за прилагане на СРС, искания за прекратяване на употребата на СРС, доклади от прилагането на СРС, документи, удостоверяващи, че материалите от прилагането на СРС са унищожени или на тяхна база са изготвени веществени доказателствени средства, съответните регистри, вътрешни организационни материали и други относими документи, издадени от органите, които искат използване на СРС, съдиите, които го разрешават, или органите, прилагащи СРС. Съгласно точка 8 от инструкцията (частично изменена през м. април 2019 г.) членовете на Бюрото и неговите служители не получават достъп до материалите по делата, които попадат извън пределите на компетентността на Бюрото, т.е. материали, които не са сред изчерпателно изброените в точка 7. По този начин те не могат да видят в цялост прокурорските преписки или досъдебните производства, провеждани от прокурорите, нито да оценят материалите, които са в подкрепа на искания за използване на СРС, или резултатите, или доказателствата, получени чрез прилагане на СРС (точки 8.1 и 8.2 от инструкцията). Всички искания от тяхна страна за достъп до веществени доказателствени средства в хода на проверка подлежат на одобрение от компетентния прокурор (точка 8.3 от инструкцията).

Даване на указания и определяне на образци

120.  Националното бюро може да дава задължителни указания на съответните органи (чл. 34е, ал. 1, т. 3). То може също така да определя стандарти и образци за съответните регистри и за работата със съответните материали (чл. 34е, ал. 2 и 3).

121.  Според годишните си доклади през цялото си съществуване Националното бюро е дало следните указания:

| **Година** | **Брой указания** |
| --- | --- |
| 2014 | 3 |
| 2015 | 49 |
| 2016 | 3 |
| 2017 | 3 |
| 2018 | 1 |
| 2019 | 7 |
| 2020 | 2 |

Сезиране на компетентните органи за нередности

122.  Ако Националното бюро установи, че неправомерно са използвани или приложени специални разузнавателни средства, или че получените чрез тях материали са били съхранявани или унищожени неправомерно, то трябва да уведоми за това прокуратурата и да информира ръководителите на съответните запитващи органи и органи по СРС (чл. 34е, ал. 5 от ЗСРС).

123.  Ако Националното бюро установи, че съдия е разрешил неправомерно използването на специални разузнавателни средства, то трябва да сезира прокуратурата и да информира Висшия съдебен съвет и министъра на правосъдието (чл. 34е, ал. 6 от ЗСРС).

Брой проверки на Националното бюро

124.  Според годишните доклади на Националното бюро всяка година от 2014 г. насам то е извършвало следния брой проверки:

| **Година** | **Брой инспекции** |
| --- | --- |
| 2014 | „повече от“ 200 |
| 2015 | 242 |
| 2016 | 287 |
| 2017 | 323 |
| 2018 | 133 |
| 2019 | 230 |
| 2020 | 240 |

* + - 1. Парламентарна комисия

125.  Другият орган, който има за задача да контролира процедурите за разрешаване, прилагане и използване на специални разузнавателни средства, както и съхраняването и унищожаването на получената чрез тях информация, е постоянна парламентарна комисия – Парламентарна комисия за контрол над службите за сигурност, прилагането и използването на СРС и достъпа до данните по Закона за електронните съобщения (чл. 34з, ал. 1 от ЗСРС, чл.18, ал. 1, точка 4, буква а) от Правилника за дейността на Народното събрание 2017 - 2021 г. (заменен с чл. 21, ал. 7 от Правилника за дейността за 2021 г.) и чл.17, параграф 1, точка 9, буква а) от Правилника за дейността на комисията). Комисията трябва да докладва на Парламента по тези въпроси всяка година (чл. 18, ал. 2, точка 1 от Правилника за дейността на Народното събрание 2017 - 2021 г. и чл. 17, ал. 1, т. 10, буква а) от Правилника за дейността на комисията). Тя има правомощието да призовава длъжностни лица (чл. 34з, ал. 2 от ЗСРС). Тя също така участва и в избора на членовете на Националното бюро (вж. параграф 110 по-горе) и упражнява наблюдение върху самото Бюро (чл. 5, т. 7 от Правилника за дейността на комисията).

* + - * 1. Начин на избиране на членовете на комисията

126.  Комисията се състои от девет членове, които са от всички парламентарни групи, пропорционално на броя на техните членове (чл. 4 от Правилника за дейността на комисията).

* + - * 1. Правомощия на комисията

127.  Комисията може а) да разглежда жалби на физически и юридически лица относно нередности в работата на службите за сигурност и б) да сезира прокуратурата, ако установи противозаконни действия в резултат на своите проверки или въз основа на индивидуални жалби (чл. 17, ал. 1, т. 11 и 12 от Правилника за дейността на комисията).

128.  Според годишните ѝ доклади в комисията са постъпили три жалби през 2014 г., шест жалби през 2015 г., четири жалби през 2016 г., седем жалби през 2017 г. и четири жалби през 2018 г. Само в доклада за 2018 г. става ясно колко от тези жалби са свързани конкретно с използване на СРС (комисията има и други правомощия – вж. параграфи 205 - 221 по-долу). В годишните доклади на комисията за 2016, 2017, 2018 и 2019 г. не се споменават проверки, извършени от нея. В годишния доклад на Специализирания наказателен съд за 2016 г. се споменава (на стр. 2), че през м. юли същата година комисията е извършила рутинна проверка там и не е установила нередности.

Й. Уведомяване на лица, по отношение на които се използват СРС

129.  Общото правило е, че всички лица, които са научили за използването на специални разузнавателни средства, не трябва да разкриват тази информация (чл. 33 от ЗСРС).

130.  Националното бюро обаче трябва служебно да уведоми лицата, спрямо които са били прилагани неправомерно СРС (член 34ж, ал. 1 от ЗСРС). Не се изисква уведомяване, ако а) то може да създаде опасност за постигане на целите на прилагането на СРС, б) за разкриване на оперативните способи или техническите средства, използвани за прилагането на СРС, или в) да доведе до риск за живота на служител под прикритие или на негови роднини или приятели (чл. 34ж, ал. 2). Законът не определя никакви изисквания относно формулировката или съдържанието на уведомлението. В становище, изготвено за целите на настоящото производство, Националното бюро посочва, че съгласно неговия вътрешен правилник в уведомлението се посочва: а) номерът на искането за използване на СРС; б) запитващият орган; в) номерът на разрешението за използване на СРС; г) органът, издал това разрешение; и д) периодът, през който е имало неправомерно прилагане на СРС.

131.  В три примера, предоставени от жалбоподателите, и очевидно свързани с хипотезите по чл. 34ж, ал. 2 от ЗСРС., в уведомленията на Националното бюро се посочва следното:

„[Националното бюро] извърши проверка съгласно Ваша жалба №... и стигна до решение, и затова Ви информирам, съгласно чл. 34ж, ал. 1 от [Закона от 1997 г.], че спрямо Вас не са били използвани неправомерно специални разузнавателни средства.“

132.  В един от тези случаи по-късно се установява, че реално са били използвани СРС и са допуснати нередности, въз основа на което съответният съд изключва получените доказателства от наказателното дело срещу лицата, спрямо които са използвани СРС (вижте прис. № 13 от 09.03.2018 г., н. о. х. д. № 727/2015 г., ОС-Хасково, не е ясно дали е влязла в сила; според правителството все още е висящо производството по обжалване).

133.  В две решения, постановени през 2016 г. (непубликувани, тъй като и двете дела са класифицирани; копия са предоставени от жалбоподателите: опр. № 18 от 26.04.2016 г. по адм. д. № С-2/2016 г., ВАС, VII о., и опр. № 28 от 09.06.2016 г. по адм. д. № С-14/2016 г.), Върховният административен съд приема, че тези уведомления на Националното бюро не подлежат на съдебен контрол.

134.  ЗСРС не изисква от Националното бюро да отговаря на жалби на физически лица, но на практика неизменно извършва проверка по тях и е задължено да го прави съгласно чл. 8, ал. 1, т. 9, буква а) от вътрешния си правилник, при условие че жалбите са „мотивирани“.

135.  Според годишните доклади на Националното бюро то е получило следния брой жалби и е изготвило следния брой уведомления на основание чл. 34ж от ЗСРС:

| **Година** | **Жалби** | **Уведомления** |
| --- | --- | --- |
| 2014 | 27 | 4 |
| 2015 | 108 | 10 |
| 2016 | 86 | 5 |
| 2017 | 133 | 2 (към едно и също лице) |
| 2018 | 110 | – |
| 2019 | 46 (10 от които невалидни и оставени без разглеждане) | 2 |
| 2020 | 45 (14 от които невалидни и оставени без разглеждане) | – |

К. Гражданска отговорност на органите за неправомерно използване на СРС

136.  Член 2, ал. 1, т. 7 от Закона за отговорността на държавата и общините за вреди от 1988 г., добавен през м. март 2009 г., предвижда, че държавата носи отговорност за вреди, които разследващите органи и прокуратурата или съдилищата са причинили на граждани чрез неправомерно използване на специални разузнавателни средства.

137.  По тази разпоредба вече е натрупана известна съдебна практика.

138.  До момента съдилищата са приели, че:

а) чл. 2, ал. 1, точка 7 се прилага само занапред за използване на СРС, което е извършено след влизането му в сила (вижте реш. № 61 от 05.03.2012 г. по гр. д. № 536/2011 г., ВтАС, не е допуснато до обжалване с опр. № 1435 от 15.12.2012 г. по гр. д. № 815/2012 г., ВКС, III г. о.);

б) иск за обезщетение за вреди съгласно чл. 2, ал. 1, т. 7 не може да бъде предявен срещу съда, издал разрешението за използване на СРС, но, според случая, срещу i) органа, който е подал искане за разрешение, ако такова е издадено; ii) органа, който е приложил СРС, ако не е подадено искане за разрешение или то е било отказано, или органа, който е пристъпил към прилагане без разрешение (съгласно разпоредбите на ЗСРС, чл. 18, който разрешава това в неотложни случаи – вж. параграф 77 по-горе); или iii) органа, който е използвал материалите, получени от прилагането на СРС (вижте опр. № 3658 от 10.08.2015 г. по гр. д. № 126/2015 г., ОС‑Благоевград, потвърдено с опр. № 2987 от 28.10.2015 г. по в. ч. гр. д. № 3999/2015 г., САС, не е допуснато до обжалване с опр. № 89 от 01.04.2016 г. по ч. гр. д. № 240/2016 г., ВКС, I г. о.; опр. № 240 от 28.03.2016 г. по в. ч. гр. д. № 171/2016 г., ОС‑Перник, не е допуснато до обжалване с опр. № 344 от 19.09.2016 г. по ч. гр. д. № 3228/2016 г., ВКС, III г. о.; опр. от 06.01.2017 г. по гр. д. № 5567/2016 г., СГС, потвърдено с опр. № 1284 от 12.04.2017 г. по в. ч. гр. д. № 1349/2017 г., САС, не е допуснато до обжалване с опр. № 303 от 22.08.2017 г. по ч. гр. д. № 2731/2017 г., ВКС, III г. о.; и реш. № 203 от 27.02.2019 г. по гр. д. № 5061/2017 г., ВКС, III г. о.);

в) ищецът трябва да посочи в исковата молба кой орган е използвал специални разузнавателни средства по отношение на него и да насочи иска срещу този орган (вижте опр. № 778 от 06.03.2018 г. по в. гр. д. № 1063/2018 г., САС, не е ясно дали е влязло в сила);

г) граждански съд, разглеждащ иск за обезщетение за вреди по чл. 2, ал. 1, т. 7, може да се позове на фактическите констатации на Националното бюро, но не е обвързан от преценката на Бюрото дали използването на СРС е било незаконосъобразно (вж. № 166 от 03.08.2018 г. по гр. д. № 4454/2017 г., ВКС, IV г. о.);

д)  самото разрешение за използване на СРС може да бъде основание за възникване на отговорност по чл. 2, ал. 1, т. 7; последващото им прилагане се отнася само до размера на обезщетението (вж. № 166 от 03.08.2018 г. по гр. д. № 4454/2017 г., ВКС, IV г. о.);

е)  отговорност по член 2, ал. 1, т. 7 може да възникне, ако разрешението за използване на СРС е издадено във връзка с престъпление, което по закон не може да бъде предотвратено или разследвано чрез такива средства, или ако искането за издаване на разрешение е подадено от некомпетентен орган или е непълно, но не и ако искането е надлежно подадено, тъй като гражданските съдилища, разглеждащи искове за обезщетение по тази разпоредба, не могат да проверяват дали съдиите, които са издали разрешение за използване на СРС, са преценили правилно необходимостта от използване на СРС по отношение на фактите (пак там, и реш. № 203 от 27.02.2019 г. по гр. д. № 5061/2017 г., ВКС, III г. о.);

ж)  неспазването на правилата, уреждащи своевременното унищожаване на информацията, получена от прилагането на СРС (вж. точки 94 и 95 по-горе), само по себе си не е основание за пораждане на отговорност по чл. 2, ал. 1, точка 7 (вижте реш. № 6303 от 10.10.2018 г. по гр. д. № 11689/2016 г., СГС (окончателно), допусната поправка на ОФГ с реш. № 3 от 02.01.2019 г. по гр. д. № 11689/2016 г., СГС); и

(з) давностният срок за предявяване на иск по чл. 2, ал. 1, т. 7 (пет години – чл. 110 от Закона за задълженията и договорите от 1950 г.; вж. също *Харизанов срещу България* (решение по допустимост.), № 53626/14, § 52, 5 декември 2017 г.) започва да тече, когато съответното лице бъде уведомено от Националното бюро, че спрямо него неправомерно са използвани СРС (вж. параграф 130 по-горе), тъй като без такова уведомление това лице няма възможност да защити правата си (вижте реш. № 166 от 03.08.2018 г. по гр. д. № 4454/2017 г., ВКС, IV г. о.).

139.  Единствената форма на обезщетение, предвидена в производствата по ЗОДОВ, са паричните обезщетения (чл. 4, ал. 1 и чл. 8, ал. 1). По дела по чл. 2, ал. 1, т. 7 до момента съдилищата са присъждали обезщетения в размер от 2000 до 27 000 лева (1023 до 13 805 евро) за различни случаи на неправомерно използване на специални разузнавателни средства:

а)  използване на такива средства по отношение на престъпления, за които това не е разрешено от закона, и при липса на достатъчна фактическа обосновка в искането за използване на СРС (вижте реш. № 1811 от 21.07.2017 г. по в. гр. д. № 615/2017 г., САС, потвърдено от реш. № 166 от 03.08.2018 г. по гр. д. № 4454/2017 г., ВКС, IV г. о., и реш. № 1960 от 30.07.2019 г. по гр. д. № 2052/2018 г., САС, не е допуснато до обжалване с опр. № 424 от 15.05.2020 г. по гр. д. № 4684/2019 г., ВКС, III г. о.);

б)  издаване на разрешение за удължаване на срока на прилагане на СРС без нова обосновка и прилагане на СРС извън сроковете (вижте реш. № 2808 от 04.05.2018 г. по гр. д. № 11366/2016 г., СГС, потвърдено с реш. № 1034 от 01.05.2019 г. по в. гр. д. № 5808/2018 г., САС, не е ясно дали е влязло в сила);

в)  издаване на разрешение за използване на СРС от некомпетентен съдия и без да се предостави достатъчна обосновка в искането за използване на СРС (вижте реш. № 12538 от 22.12.2020 г. по в. гр. д. № 1690/2020 г., САС, не е допуснато до обжалване с опр. № 60753 от 04.11.2021 г. по гр. д. № 1845/2021 г., ВКС, III г. о.);

г)  издаване на разрешение за използване на СРС от некомпетентен съд и прилагане на СРС извън съответния срок (вижте реш. № 312 от 16.10.2020 г. по гр. д. № 238/2020 г., ОС-Бургас, потвърдено с реш. № 13 от 19.02.2021 г. по в. гр. д. № 474/2020 г., АС-Бургас, не е допуснато до обжалване с опр. № 60653 от 12.10.2021 г. по гр. д. № 1872/2021 г., ВКС, IV г. о.), и реш. № 262304 от 07.04.2021 г. по гр. д. № 8701/2019 г., СГС, не е ясно дали е влязло в сила);

д)  издаване на разрешение за използване на СРС, без да са предоставени достатъчно фактически данни в първоначалното искане (и в искането за удължаване на срока) и без да се разполага с достатъчно информация, че лицето, спрямо което е поискано прилагане на СРС, всъщност може да бъде заподозряно в извършването на престъпление (вижте реш. № 6303 от 10.10.2018 г. по гр. д. № 11689/2016 г., СГС (окончателно), допусната поправка на ОФГ с реш. № 3 от 02.01.2019 г. по гр. д. № 11689/2016 г., СГС);

е)  издаване на разрешение за използване на СРС единствено въз основа на анонимен сигнал и без подробно описание на предходните, ако има такива, действия по разследване (вижте реш. № 7225 от 20.11.2018 г. по в. гр. д. № 16408/2017 г., СГС (окончателно), с което е отменено реш. № 192358 от 11.08.2017 г., по гр. д. № 13365/2016 г., СРС);

ж)  прилагане на СРС извън съответния срок (вижте реш. № 8690 от 21.12.2017 г. по гр. д. № 6213/2017 г., СГС, потвърдено с реш. № 1536 от 01.06.2018 г. по в. гр. д. № 1509/2018 г., САС, потвърдено с реш. № 293 от 17.03.2020 г. по гр. д. № 3963/2018 г., ВКС, IV г. о.).

з)  прилагане на СРС с цел проследяване на беглец, което не е сред хипотезите, предвидени в ЗСРС (вижте реш. № 1360 от 12.01.2017 г. по гр. д. № 781/2015 г., РС-Перник, потвърдено от реш. № 173 от 23.06.2017 г. по в. гр. д. № 237/2017 г., ОС-Перник, потвърдено, с увеличение на обезщетението, с реш. № 203 от 27.02.2019 г. по гр. д. № 5061/2017 г., ВКС, III г. о.).

140.  Във всички тези случаи ищците са уведомени от Националното бюро, че спрямо тях неправомерно са приложени СРС и съдилищата са разполагали с информация от Бюрото, а в някои случаи и с материали от прилагането на СРС, включени като доказателства в наказателното производство срещу съответните лица. В годишния си доклад за 2016 г. Бюрото посочва (на стр. 25), че е предоставило на гражданските съдилища материали от своите проверки по искания, отправени от тях в такива случаи.

141.  С решение от м. март 2018 г. Софийският апелативен съд постановява, наред с другото, че съгласно общото правило за *affirmanti incumbit probatio* в производството по чл. 2, ал. 1, т. 7 от Закона от 1988 г. тежестта е върху ищците да докажат кой орган е използвал незаконно специални разузнавателни средства по отношение на тях и поради това е надлежният ответник по иска им (вижте опр. № 778 от 06.03.2018 г. по в. гр. д. № 1063/2018 г., САС, не е ясно дали е влязло в сила).

142.  В скорошен случай, при който използването на специални разузнавателни средства не е видно от материалите в наказателното производство срещу ищеца, съдилищата отхвърлят иска по чл. 2, ал. 1, точка 7 от ЗОДОВ като недоказан, като отбелязват, че ищецът трябва да изложи твърдението си, че такива средства са били използвани по отношение на него (вижте реш. oт 31.12.2019 г. по гр. д. 31075/2015 г., СРС, потвърдено с реш. № 260651 от 29.01.2021 г. по в. гр. д. № 6434/2020 г., СГС, производството по обжалване е висящо).

143.  С решение от м. юни 2020 г. Бургаският окръжен съд постановява, че иск по чл. 2, ал. 1, т. 7 от ЗОДОВ може да бъде предявен само ако използването на специални разузнавателни средства по отношение на ищеца е видно от представените доказателствени средства по наказателното дело или от уведомлението на Националното бюро (вижте опр. № 1786 от 26.06.2020 г. по гр. д. № 1037/2020 г., ОС-Бургас, окончателно).

144.  В решение от м. април 2021 г. Софийският градски съд постановява че тъй като при уведомяването на ищеца Националното бюро не е предоставило информация за съдържанието на исканията или разрешенията за използване на СРС, не е налице основание да се смята, че използването на специални разузнавателни средства е било неправомерно. Поради това съдът отхвърля иска (вижте реш. № 262304 от 07.04.2021 г. по гр. д. № 8701/2019 г., СГС, не е ясно дали е влязло в сила).

К. Наказателна отговорност на длъжностните лица за неправомерно използване на СРС

145.  Според чл. 284в от Наказателния кодекс, приет през 2009 г., длъжностно лице, което противозаконно разреши или разпореди използването на СРС, или ги прилага, или съхранява информация, получена чрез тях, извършва престъпление. До момента има само една присъда по тази разпоредба (вж. параграф 56 по-горе).

* 1. ПРЕДСТАВЯНЕ НА ДОКУМЕНТИ В ГРАЖДАНСКОТО ПРОИЗВОДСТВО

146.  Член 190, ал. 1 от Гражданския процесуален кодекс предвижда, че дадена страна може да поиска от съда да разпореди на ответната страна да представи намиращ се у нея документ, ако обясни на съда защо този документ е от значение за случая. Ако ответната страна не представи документа, съдът може да стигне до неблагоприятни за нея изводи (чл. 190, ал. 2 във връзка с чл. 161). Ответната страна може да откаже да представи документ, ако (а) съдържанието му е свързано с личния или семейния живот на страната, или (б) представянето му би довело до опозоряване на тази страна или нейни близки или до наказателно преследване срещу тях (чл. 191, ал. 1). Ако тези основания се отнасят само до част от документа, ответната страна може да бъде задължена да представи извлечение (чл. 191, ал. 2).

147.  Член 192, ал. 1 от ГПК предвижда, че дадена страна може да поиска от съда да разпореди на неучастващо в делото лице да представи документ, с който разполага. Ако третата страна не представи документа без основание, тя може да бъде глобена от съда и носи отговорност пред страната, която е поискала документа, за вреди, произтичащи от непредставянето му (чл. 192, ал. 3).

148.  Съгласно основна практическа монография по граждански процес искането на една от страните за представяне на документ по членове 190 или 192 трябва, доколкото е практически осъществимо, да посочва неговия вид, дата, автор и други отличителни белези. Освен това е недопустимо да се изисква от ответната страна или от трето лице да представи, за целите на производството, документ, който вече не съществува (вижте *Граждански процесуален кодекс*, *Приложен коментар*, ИК „Труд и право“, 2017 г., стр. 318).

149.  В чл. 186 от същия кодекс е предвидено, че съдът, който гледа гражданско дело, може да поиска от съответното учреждение да представи официални документи или да снабди страната, която възнамерява да ползва тези документи, със съдебно удостоверение, което да представи на съответния публичен орган с оглед получаването на документите. Учреждението е длъжно да ги издаде или да посочи причините, поради които не може да направи това.

150.  Не изглежда да има съдебна практика по членове 186, 190 или 192 от Гражданския процесуален кодекс във връзка със случаи по чл. 2, ал. 1, точка 7 от ЗОДОВ (вж. параграфи 136 - 144 по-горе).

* 1. ЗАПАЗВАНЕ И ДОСТЪП ДО ТРАФИЧНИ ДАННИ
     1. Общо развитие на правния режим

151.  Режимът за запазване и последващ достъп до трафични данни за целите на правоприлагането е въведен при влизането в сила на чл. 251 от Закона за електронните съобщения от 2007 г., както и когато министърът на вътрешните работи и ръководителят на Държавната агенция за информационни технологии и съобщения издават въз основа на законоустановено делегиране по чл. 251, ал. 2, Наредба № 40 от 7 януари 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 разкриването на престъпления“.

152.  Тези разпоредби са въведени с цел транспониране на така наречената Директива относно запазването на данни (вж. параграф 232 по-долу) (точка 4 от преходните и заключителните разпоредби на наредбата).

153.  Разпоредбата на чл. 5 от Наредба № 40 от 2008 г. е отменена от Върховния административен съд през м. декември 2008 г. след оспорване от страна на четвъртия жалбоподател – Фондация „Програма за достъп до информация“ (виж реш. № 13627 от 11.12.2008 г. на ВАС по адм. д. № 11799/2008 г., ВАС, петчл. с-в, ДВ, бр. 108/2008 г.).

154.  В сила от м. март 2009 г., Парламентът изменя чл. 251 от ЗСРС, като премахва възможността за издаване на наредби. Поради това статутът на Наредба № 40 от 7 януари 2008 г., които не е отменена официално, остава неясен.

155.  В началото на 2010 г. Парламентът приема нови членове 250a -250е, 251a, 261a -261б, 327, ал. 4 - 7 и 332a към Закона от 2007 г. и изменя чл. 251. Това отново е направено с оглед на транспонирането на Директивата относно запазването на данните (параграф 10 от допълнителните разпоредби на Закона за изменение на Закона за електронните съобщения от м. февруари 2010 г).

156.  По искане на омбудсмана от м. април 2014 г., малко след решението на Съда на Европейския съюз (СЕС), с което приема Директивата за запазването на данни за невалидна (вж. параграф 233 по-долу), в средата на м. март 2015 г. Конституционният съд обявява за противоконституционни чл. 250а -250е, 251 и 251а от ЗЕС изцяло (вж. реш. № 2 от 12.03.2015 г. по к. д. № 8/2014 г., КС, обн., ДВ, бр. 23/2015 г.).

157.  В отговор на това решение в края на м. март 2015 г. Парламентът приема нови чл. 251б -251и към ЗЕС и нов член 159а към Наказателно-процесуалния кодекс. Оттогава те са изменяни няколко пъти. През 2016 г. е приет нов член 251г1.

158.  През м. март 2020 г., след избухването на пандемията от COVID-19 Парламентът изменя чл. 251б, ал. 2, 251в, ал. 2, 251г, ал. 5 и 251г1, ал. 1, 3 и 4 от ЗЕС, за да направи възможно използването на запазените данни за местоположение (идентификатор на клетките) за принудително изпълнение на поставяне под карантина или задължителна изолация на хора, които са болни или са носители на редица заразни болести, включително COVID-19.

159.  През м. ноември 2020 г. Конституционният съд обявява измененията за противоконституционни в цялост (вижте реш. № 15 от 17.11.2020 г. по к. д. № 4/2020 г., КС, обн., ДВ, бр. 101/2020 г.). Той се позова, наред с другото, на съдебната практика на СЕС в тази област (вж. параграфи 233 и 240 - 243 по-долу), че прибягването до запазване на данни за местоположението (идентификатор на клетките) в продължение на шест месеца и произтичащата от това възможност за органите да имат достъп до тях, за да прилагат мерки за предотвратяване на разпространението на инфекциозни болести, несъразмерно засяга конституционното право на неприкосновеност на личния живот.

Б. Режимът понастоящем

160.  Всички посочени по-долу законови разпоредби са изложени в редакцията им към 7 декември 2021 г.

* + - 1. Видове к данни, подлежащи на запазване

161.  Всички доставчици на електронни комуникационни услуги в България трябва да запазят за срок от шест месеца следните видове комуникационни данни за всички свои потребители: а) данни, необходими за проследяване и идентифициране на източника на връзката; б) данни, необходими за идентифициране на направлението на връзката; в) данни, необходими за идентифициране на датата, часа и продължителността на връзката; г) данни, необходими за идентифициране на типа на връзката; д) данни, необходими за идентифициране на крайното устройство на потребителя или на това, което се представя за негово крайно устройство; и е) идентификатор на клетките за мобилното комуникационно оборудване (чл. 251б, ал. 1 от ЗЕС). Член 251и дефинира подробно в какво се състои всеки от тези видове данни за стационарна и мобилна телефония и достъп до интернет, електронна поща и интернет телефония. Тези разпоредби възпроизвеждат почти дословно текста на член 5 от Директивата относно запазването на данни (вж. параграф 232 по-долу). Доставчиците на комуникационни услуги, които не спазват това задължение за запазване на данни, подлежат на имуществена санкция в размер от 3000 до 25 000 лв. (чл. 327, ал. 4 от ЗЕС).

162.  Съгласно годишните доклади на Комисията за защита на личните данни (вж. параграфи 198 - 203 по-долу) общият брой на доставчиците на комуникационни услуги в България и броят на доставчиците, които докладват на комисията във връзка със запазването на данни всяка година от 2015 г. насам,[[16]](#footnote-16) е следният:

| **Година** | **Общ брой доставчици на комуникационни услуги** | **Доставчици на комуникационни услуги, които докладват на комисията** |
| --- | --- | --- |
| 2015 | 1160 | 77[[17]](#footnote-17) |
| 2016 | 1143 | 104 |
| 2017 | не е посочено | 93 |
| 2018 | не е посочено | 117 |
| 2019 | не е посочено | 99 |

* + - 1. Цели, за които се запазват тези данни

163.  Тези данни се съхраняват за целите на а) националната сигурност; б) предотвратяването, разкриването или разследването на „тежки“ престъпления[[18]](#footnote-18) (включително, след изменение от м. януари 2018 г., предотвратяването на „тежки престъпления“ на корупция от специална комисия); в) проследяването на хора, които са осъдени с влязла в сила присъда на лишаване от свобода за тежко престъпление или които са попаднали или биха могли да попаднат в ситуация, която излага на риск живота или здравето им; и г) (това се отнася единствено за идентификатора на клетки) извършването на операции по търсене и спасяване на хора в беда (чл. 251б, ал. 2 от ЗЕС и чл. 159, ал. 2 от Наказателно - процесуалния кодекс).

* + - 1. Правила за обработване на запазените данни от доставчиците на комуникационни услуги

164.  Запазените данни трябва да бъдат обработвани и съхранявани от доставчиците на комуникационни услуги в съответствие с изискванията за защита на личните данни (чл. 251б, ал. 4 от ЗЕС).

165.  Доставчиците на комуникационни услуги трябва да гарантират, че запазените данни: а) са със същото качество и са предмет на същата сигурност и защита като данните в техните мрежи; б) с подходящи технически и организационни мерки, за да бъдат защитени от случайно или незаконно унищожаване, случайна загуба или промяна, или от непозволено или незаконно съхраняване, обработване, достъп или разкриване; в) с подходящи технически и организационни мерки, за да се гарантира, че до данните може да има достъп само специално упълномощен персонал; и г) се унищожават в края на периода на съхранение, освен в случаите, предвидени в закона (чл. 261а, ал. 2 от ЗЕС).

* + - 1. Унищожаване на запазени данни, до които органите не са осъществили достъп

166.  Доставчиците на комуникационни услуги трябва да унищожат запазените данни незабавно след изтичането на шестмесечния срок за съхраняването им и да изпратят протокол, удостоверяващ това унищожаване, на Комисията за защита на личните данни (вж. параграфи 198 - 203 по-долу) не по-късно от пето число на съответния месец (чл. 251ж, ал. 1 от ЗЕС). Комисията може да контролира дали това задължение е било спазено (вж. параграф 204, буква б) по-долу).

* + - 1. Процедура за получаване на разрешение
         1. Органи, оправомощени да поискат достъп

167.  Само ограничен брой органи могат да поискат достъп до запазените данни в рамките на компетентността си.

168.  Извън рамките на висящо наказателно производство такъв достъп може да се търси само от: а) специализираните дирекции и териториалните дирекции и звена на Държавна агенция „Национална сигурност“; б) различните дирекции на Министерството на вътрешните работи (Главна дирекция "Национална полиция", Главна дирекция "Борба с организираната престъпност" и териториалните и звена, Главна дирекция "Гранична полиция" и териториалните и звена, дирекция "Вътрешна сигурност", и областните дирекции на Министерството на вътрешните работи); в) службите "Военно разузнаване" и "Военна полиция" при министъра на отбраната; г) Държавна агенцията “Разузнаване“; д) специализираната дирекция за противодействие на корупцията;[[19]](#footnote-19) и е) (по отношение на идентификационните данни на клетките, необходими за операции по издирване и спасяване – вж. параграф 161, буква е) и параграф 163, буква г) по-горе) Главна дирекция "Пожарна безопасност и защита на населението" на Министерството на вътрешните работи, включително нейните териториални единици (чл. 251в, ал. 1 и ал. 2 от Закона от 2007 г.). Ако чуждестранен орган иска достъп, искането трябва да бъде направено чрез главна или специализирана дирекция на Държавна агенция „Национална сигурност“ или Министерството на вътрешните работи (чл. 251з, ал. 2).

169.  В рамките на наказателно производство съдът, разглеждащ делото, може да поиска достъп (ако то вече е в съдебна фаза или обжалване) или от наблюдаващия прокурор в досъдебното производство (чл. 159а, ал. 1 от НПК).

170.  Според годишните доклади на парламентарната комисия, контролираща системата (вж. параграфи 205 до 221 по-долу), броят на исканията за достъп за периода 2015 - 2019 г. е следният:

| **Година** | **Заявления за достъп извън рамките на наказателно производство** | **Заявления за достъп от прокурори** |
| --- | --- | --- |
| 2015 | 12948 | 13354 |
| 2016 | 15805 | 24758 |
| 2017 | 13233 | 25252 |
| 2018 | 10603 | 22563 |
| 2019 | 13108 | 18883 |

(б) Съдържание на заявлението искането за достъп

171.  Исканията за достъп, подадени извън контекста на висящи наказателни производства, трябва да бъдат мотивирани и да съдържат а) правното основание и целта, за която се иска достъп; б) регистрационния номер на преписката, по която е необходимо извършване на справката,; в) ако е налична, информация за потребителя (потребителите), чиито данни се търсят; г) данните, които трябва да се отразят в справката; д) периодът от време, за който се търсят данни, който трябва да бъде „разумен“ и „необходим за постигане на целта“, за която се прави искането за достъп; е) пълно и изчерпателно посочване на фактите, които показват, че данните са необходими за постигане на съответната цел; и ж) длъжностното лице, на което трябва да се предоставят данните (чл. 251в, ал. 3 от ЗЕС).

172.  Исканията за достъп, подадени от прокурор в хода на наказателно производство, също трябва да бъдат мотивирани и да съдържат: а) информация за предполагаемото престъпление, във връзка с което се иска достъп; б) описание на обстоятелствата, на които се основава искането за достъп; в) информация за ползвателя (ползвателите), чиито данни се търсят; г) „разумен“ период от време, за който се търсят данни; и д) разследващия орган, на който трябва да се предоставят данните (чл. 159а, ал. 3 от Наказателно - процесуалния кодекс).

(в) Органи с правомощия да издават разрешения за достъп

173.  Извън рамките на висящо наказателно производство разрешението може да бъде издадено от председателя на районния съд, който е териториално компетентен по отношение на мястото, където е седалището на запитващия орган, или от съдия, на когото председателят е делегирал това правомощие (чл. 251г, ал. 1 от ЗЕС).

174.  Ако искането за достъп се отнася до предполагаеми терористични престъпления (включително подготовка за такива), разрешението може да бъде издадено само от председателя на Специализирания наказателен съд или от съдия, на когото той е делегирал това правомощие (чл. 251г, ал. 2 от ЗЕС).

175.  Ако искането за достъп е подадено по молба на чуждестранен орган, разрешението трябва да бъде издадено от председателя на Софийски градски съд или съдия, на когото той е делегирал това правомощие (чл. 251з, ал. 2 от ЗЕС).

176.  Специални правила уреждат достъпа до запазени комуникационни данни, свързани с председателите на районни съдилища или техни близки, или председателя на Специализирания наказателен съд или негови близки (освен ако се иска достъп до данните за операция по търсене и спасяване): в тези случаи разрешението може да бъде издадено от съответния председател на окръжния съд или от председателя на Апелативния специализиран наказателен съд (чл. 251г, ал. 4 от ЗЕС).

177.  Ако искането за достъп е подадено от прокурор в хода на наказателно производство, разрешението може да бъде издадено от съдия от компетентния първоинстанционен съд (чл. 159а, ал. 1 от НПК).

(г) Ред за разглеждане на искането за достъп

178.  Когато се иска достъп във връзка с предполагаемо терористично престъпление, разрешението трябва да бъде издадено в рамките на двадесет и четири часа от получаването на искането (чл. 251г, ал. 3 от ЗЕС). Нито ЗЕС, нито чл. 159а от Наказателно-процесуалния кодекс предвиждат изрични срокове за разглеждане на исканията за достъп в други случаи.

179.  Когато се отнася до искане за достъп, подадено извън рамките на висящо наказателно производство, разпореждането за издаване на разрешение трябва да бъде мотивирано и да съдържа а) данните, които трябва да бъдат предоставени; б) срокът, за който трябва да се предоставят данните, който трябва да бъде „разумен“ и „необходим за постигане на целта“, за която е подадено искането за достъп; и в) длъжностното лице, на което трябва да се предоставят данните (чл. 251г, ал. 6 от ЗЕС).

180.  Когато се отнася до заявление за достъп, подадено в хода на наказателно производство, разпореждането за издаване на разрешение също трябва да бъде мотивирано и да съдържа: а) данните, които трябва да се предоставят; б) срокът, за който трябва да се предоставят данните, който трябва да бъде „разумен“; и в) разследващият орган, на когото трябва да се предоставят данните (чл. 159а, ал. 1 и 4 от Наказателно-процесуалния кодекс).

181.  Всички районни съдилища, Специализираният наказателен съд и Софийският градски съд трябва да впишат дадените мотивирани разрешения или откази за достъп в регистри, които не са публични (чл. 251г, ал. 7 и чл.251з, ал. 2 *in fine* от ЗЕС).

182.  Съгласно годишните доклади на парламентарната комисия, която осъществява наблюдение на системата (вж. параграфи 205 до 221 по-долу), съдебните разпореждания за уважаване или отказ на искания за достъп всяка година през периода 2015 - 2019 г. са, както следва:

| **Година** | **Издадени разрешения за достъп** | **Откази за достъп** |
| --- | --- | --- |
| 2015 | 25303[[20]](#footnote-20) | 2911 |
| 2016 | 39990 | 3479 |
| 2017 | 38492 | 2762 |
| 2018 | 33835 | 2287 |
| 2019 | 29325 | 2666 |

(д) Последващо разрешение в неотложни случаи

183.  В случаите на непосредствена опасност от извършване на терористично престъпление (включително приготовление за такова престъпление), достъпът може да бъде осигурен без предварително разрешение на съда (чл. 251г1, ал. 1 от ЗЕС). В тези случаи в искането за (незабавен) достъп трябва да се посочат: а) правното основание за достъпа; б) данните, които трябва да бъдат предоставени; в) „разумен“ период от време, за който трябва да бъдат предоставени данни; и г) длъжностното лице, на което трябва да бъдат предоставени данните (чл. 251г1, ал. 2).

184.  Впоследствие ръководителят на запитващия орган трябва незабавно да информира съответния съдия за достъпа, да му изпрати искането за достъп и да изложи мотиви, обосноваващи необходимостта от незабавен достъп. Мотивите трябва да включват пълно описание на обстоятелствата, поради които органът е счел, че предстои извършването на терористично престъпление (чл. 251г1, ал. 3 от Закона от 2007 г.).

185.  Ако съдията не одобри искането за достъп в рамките на двадесет и четири часа, всички данни, предоставени съгласно искането за незабавен достъп, трябва да бъдат унищожени от органа, който ги е получил, и доставчикът на комуникационни услуги трябва да бъде уведомен за това (чл. 251г1, ал. 4 от ЗЕС). Ако съдията одобри искането за достъп, с разпореждането се потвърждават извършените действия до момента.(член 251г1, ал. 5).

186.  В годишния доклад на парламентарната комисия, която осъществява наблюдение на системата (вж. параграфи 205 до 221 по-долу) за 2019 г. – единственият, в който се споменава този въпрос – се посочва (на стр. 11), че през тази година съдилищата са одобрили 317 искания за незабавен достъп, отправени в неотложни случаи.

* + - 1. Процедура за достъп до запазените данни

187.  Доставчиците на комуникационни услуги трябва да осигурят възможност за постъпване на искания за достъп, включително искания за незабавен достъп, по всяко време (чл. 251д, ал. 1 от ЗЕС). Те трябва да информират съответните органи за длъжностните лица, оправомощени да получават разпореждания и искания за достъп (чл. 251д, ал. 1). Неспазването на това задължение може да доведе до налагане на имуществена санкция в размер от 2000 до 12 000 лв. (чл. 327, ал. 5).

188.  В обичайните хипотези доставчиците на комуникационни услуги трябва да предоставят данните във възможно най-кратък срок и във всеки случай в рамките на седемдесет и два часа от получаване на искането за достъп. Въпреки това министърът на вътрешните работи или ръководителят на Държавна агенция „Национална сигурност“, или надлежно упълномощени от тях заместници, могат да определят по-кратък срок в конкретния случай. В случаите, свързани с предполагаеми терористични престъпления, данните трябва да бъдат предоставени незабавно (чл. 251е, ал. 2 от ЗЕС). Неспазването на това задължение може да доведе до налагане на имуществена санкция от 10 000 до 25 000 лв., а при повторни случаи от 15 000 до 50 000 лв. (чл. 327, ал. 6 и 7). При спасителни операции, достъпът трябва да бъде осигурен незабавно и във всеки случай не по-късно от два часа след получаване на искането за достъп; ако животът или здравето на засегнатите лица са изложени на сериозен риск, министърът на вътрешните работи или надлежно упълномощено длъжностно лице могат да определят по-кратък срок (чл. 251е, ал. 3).

189.  Всички искания за достъп трябва да бъдат записани от доставчиците на комуникационни услуги в специален регистър, който не е публичен (чл. 251е, ал. 1 *in fine* от ЗЕС). Само надлежно оправомощени служители могат да разглеждат искания за достъп (чл. 251е, ал. 4). Документът, в който се посочват данните, търсени от органите, трябва да бъде подписан от ръководителя на доставчика на комуникационни услуги или от надлежно упълномощен служител, записан в специален регистър и изпратен директно на определеното длъжностно лице (чл. 251е, ал. 5).

190.  Ако е технически осъществимо, целият обмен на документи между органите и доставчиците на комуникационни услуги трябва да се извършва по електронен път (чл. 251е, ал. 6 от ЗЕС).

191.  Ако съответният орган поиска и получи разрешение от компетентния съдия, запазените данни, до които е получил достъп, могат да бъдат съхранявани от доставчика на комуникационни услуги най-много три месеца от датата, на която са предоставени на органа. (чл. 251е, ал. 7 от ЗЕС).

192.  Съгласно годишните доклади на Комисията за защита на личните данни (вж. параграфи 198 до 203 по-долу) броят на случаите, в които запазени комуникационни данни са предоставени на органите, и броят на исканията за достъп, които не са удовлетворени, всяка година от 2010 г. насам[[21]](#footnote-21) е следният:

| **Година** | **Случаи на предоставен достъп** | **Неудовлетворени искания за достъп** |
| --- | --- | --- |
| 2010 | 38861 | 920 |
| 2011 | 74296 | 1376 |
| 2012 | 91159 | 1083 |
| 2013 | 96652 | 1606 |
| 2014 | 107769 | 705 |
| 2015 | 70543 | 2783 |
| 2016 | 64959 | 546 |
| 2017 | 65073 | 347 |
| 2018 | 56527 | 416 |
| 2019 | 47553 | 291 |

* + - 1. Съхранение на запазените данни, до които органите имат достъп

193.  Нито ЗЕС, нито Наказателно-процесуалният кодекс съдържат разпоредби, в които се посочва начинът, по който запазените комуникационни данни, до които органите са получили достъп, трябва да се съхраняват от тях. Преглед на съдебните решения, в които се споменават такива данни, предполага, че когато се използват в хода на наказателно производство, те се съхраняват по съответното дело (вижте, например, прис. № 4 от 19.01.2018 г. по н. о. х. д. № 234/2017 г., ОС-Хасково; прис. № 32 от 10.09.2019 г. по н. о. х. д. № 475/2018 г., ОС-Стара Загора; и прис. № 34 от 11.12.2019 г. по н. о. х. д. № 650/2019 г., ОС-София). Нито Правилникът за администрацията в съдилищата, издаден от Висшия съдебен съвет през 2017 г., нито Правилникът за администрацията в прокуратурата, издаден от Висшия съдебен съвет през 2013 г., които уреждат съхранението на преписки по дела съответно от съдилищата и прокуратурата, съдържат специални правила за съхраняване на комуникационни данни, съдържащи се в делата.

* + - 1. Унищожаване на запазените данни, до които органите имат достъп

194.  Ако не ги използват за образуване на наказателно производство, органите трябва да унищожат комуникационните данни, до които имат достъп, в срок от три месеца от получаването им. Унищожаването се извършва от тричленна комисия, назначена от ръководителя на съответния орган. Комисията трябва да изготви протокол, удостоверяващ унищожаването, и да го изпрати незабавно на съдията, издал разрешението за достъп. Този протокол трябва да бъде вписан в регистъра на разрешенията, воден от съответния съд (вж. параграф 181 по-горе) (чл. 251ж, ал. 2 от ЗЕС).

195.  Ако компетентният съдия не утвърди достъпа до запазените данни, до които органите са получили достъп без предварително разрешение по неотложната процедура (вж. параграфи 183 до 185 по-горе), тези данни трябва да бъдат незабавно унищожени по същия начин (чл. 251ж, ал. 3 от ЗЕС).

196.  Комуникационните данни, до които е осъществен достъп в хода на наказателното производство и които се оказват неотносими или не допринасят за установяване на фактите по случая, също трябва да бъдат унищожени. Това се прави по разпореждане на съдията, издал разрешението за достъп (по предложение на прокурора по делото), в съответствие с правилата, установени от главния прокурор (тези правила не са публично достъпни). В седемдневен срок от унищожаването доставчиците на комуникационни услуги и прокурорът по делото трябва да изпратят на съдията, издал разрешението за достъп, протокола, удостоверяващи унищожаването(чл. 159а, ал. 6 от НПК).

* + - 1. Органи, които осъществяват надзор върху запазването и достъпа до комуникационни данни

(а) Съдии, издали съответните разрешения за достъп

197.  Както е отбелязано в параграфи 194, 195 и 196 *in fine* по-горе, съдията, издал разрешението за достъп, трябва да бъде уведомен за унищожаването от съответния правоприлагащ орган на всички комуникационни данни, които са неотносими или безполезни.

(б) Комисия за защита на личните данни

198.  Комисията за защита на личните данни наблюдава запазването на комуникационни данни за целите на правоприлагането от доставчиците на комуникационни услуги (чл. 261а, ал. 1 и 2 от ЗЕС). Съгласно чл. 262 от ЗЕС, изменен през м. февруари 2019 г., надзорът на Комисията върху обработката на лични данни, свързана със съхраняването и достъпа до комуникационни данни, трябва да се извършва в съответствие с изискванията на Общия регламент за защита на данните („GDPR“ – вж. параграфи 234 - 237 по–долу) и Закона за защита на личните данни от 2002 г. (вж. параграфи 218 и 225 по-долу).

199.  По принцип същата Комисия е компетентна да наблюдава обработването на лични данни от несъдебни органи за целите на правоприлагането (вж. параграф 225 по-долу).

Начин на избиране и мандат на членовете на Комисията

200.  Комисията, която е „независим надзорен орган“, се състои от председател и четирима членове, избирани от Парламента по предложение на Министерския съвет за срок от пет години, който може да бъде подновен еднократно (чл. 6, ал. 1 и чл. 7, ал. 1 и 2 от Закона за защита на личните данни от 2002 г.). Те трябва да имат висше образование по информатика, по информационни технологии или по право (чл. 8, ал. 1, точка 1). Председателят трябва да бъде правоспособен юрист (чл. 8, ал. 3). Парламентът може да прекрати мандата на председателя преждевременно само в ограничен брой случаи: осъдителна присъда, грубо нарушение, невъзможност да изпълнява задълженията си за повече от шест месеца или надлежно установен конфликт на интереси (чл. 8, ал. 4, т. 2).

Правомощия на Комисията съгласно ЗЕС

Да получава информация

201.  Комисията може да поиска от доставчиците на комуникационни услуги да ѝ предоставят всякаква информация, свързана с компетентността ѝ в тази област (чл. 261а, ал. 3, т. 1 от ЗЕС). Доставчиците на комуникационни услуги трябва също така да ѝ предоставят ежегодно статистическа информация за: а) броя на случаите, в които компетентните органи са получили достъп до запазени комуникационни данни; б) времето, изтекло от датата, на която данните са били запазени, до датата, на която компетентният орган е поискал достъп до тях; и в) броя на случаите, в които исканията за достъп са били невъзможни за изпълнение (чл. 261а, ал. 4). Комисията трябва да съобщава тази статистическа информация ежегодно на Парламента и на Европейската комисия[[22]](#footnote-22) (чл. 261а, ал. 5).

202.  Комисията може също така да проверява как доставчиците на комуникационни услуги изпълняват задълженията си да съобщават на потребителите за нарушения на сигурността на личните данни (вж. параграф 214 по-долу) (чл. 261г, ал. 2 от ЗЕС) и да проверява техническите и организационните мерки, предприети от доставчиците на комуникационни услуги за съхраняване на запазените комуникационни данни (чл. 261г, ал. 3).

Да дава указания и препоръки

203.  Комисията може да даде задължителни указания, които трябва да бъдат изпълнени незабавно (чл. 261а, ал. 3, т. 2 от ЗЕС). Тези указания могат по-специално да бъдат за това кога и как доставчиците на комуникационни услуги трябва да съобщават на засегнатите лица за нарушенията на сигурността на личните им данни (чл. 261г, ал. 1). Тя може също така да издава препоръки относно най-добри практики за нивото на сигурност при съхраняване на запазените комуникационни данни (чл. 261г, ал. 3 *in fine*).

Да налага санкции

204.  Комисията може да налага санкции на доставчиците на комуникационни услуги, които не са изпълнили задълженията си да: а) съобщят на засегнатите лица за нарушение на сигурността на личните им данни (вж. параграф 214 по-долу) или б) унищожат запазените комуникационни данни в рамките на законоустановения срок (вж. параграф 166 по-горе) (чл. 261г, ал. 2 *in fine* и чл. 323а от ЗЕС).

(б) Парламентарна комисия

205.  Същата постоянна парламентарна комисия, която осъществява наблюдение на използването на СРС – Парламентарната комисия за контрол над службите за сигурност, прилагането и използването на СРС и достъпа до данните по Закона за електронните съобщения (вж. параграф 125 по-горе) – също има за задача да осъществява надзор по отношение запазването и достъпа до комуникационни данни. Тя наблюдава не само доставчиците на комуникационни услуги, но и органите, които имат право на достъп до данните и процедурите, чрез които искат и получават достъп до тях, и трябва да гарантира, че индивидуалните права и свободи са защитени срещу незаконен достъп (чл. 261б, ал. 1 от ЗЕС и чл. 18, ал. 1, т. 4, буква б) и ал. 2, т. 2 от Правилника за дейността на Народното събрание за 2017 - 2021 г.). Комисията трябва да докладва ежегодно за всички извършени от нея проверки (чл. 261б, ал. 2, т. 4).

Ред за избор на членовете на Комисията

206.  Той е посочен в параграф 126 по-горе.

Правомощия на Комисията по ЗЕС

Да получава на информация

207.  Комисията може: а) да поиска от доставчиците на комуникационни услуги, органите, които имат право на достъп до запазените данни (вж. параграфи 168 и 169 по-горе), и Комисията за защита на личните данни да ѝ предоставят всяка информация, свързана с нейната компетентност; б) да проверява начина, по който се съхраняват запазените данни, исканията за достъп и разрешенията за достъп, и начина, по който се унищожават запазените данни; и в) има достъп до помещенията на съответните органи или доставчици на комуникационни услуги (чл. 261б, ал. 2, т. 1 до ал. 2, т. 3 от ЗЕС). Министерството на вътрешните работи, Държавна агенция “Национална сигурност“, Държавна агенция „Разузнаване“ и главният прокурор трябва да предоставят на Комисията статистическа информация за годишния брой на исканията за достъп, разрешенията за достъп и случаите на достъп и унищожаване на данни (чл. 261б, ал. 3).

208.  В годишния си доклад за 2017 г. Комисията отбеляза, че нейни експерти са извършили 302 проверки в съдилища и правоприлагащи органи. Тези проверки разкриват а) разнопосочни практики в съдилищата по отношение на исканията за достъп и б) неизпълнение от страна на прокурорите, които отговарят за съответните наказателни дела, на задължението им по чл. 159а, ал. 6 от Наказателно-процесуалния кодекс да предложат на компетентните съдии да разпоредят унищожаването на достъпните комуникационни данни, които са се оказали неотносими или не допринасят за изясняване на обстоятелствата по делото (вж. параграф 196 по-горе). В доклада се отбелязват и различни случаи, при които не са спазени законовите изисквания за достъп.

209.  В годишния си доклад за 2018 г. Комисията отбеляза, че нейни експерти са извършили 229 проверки и отново са станали свидетели на разнопосочни практики, както и пропуски от страна на прокуратурата да унищожи комуникационни данни, които не са от значение, въз основа на това, че тези данни могат да се окажат полезни на по-късен етап от разследването. Докладът отново отбелязва различни случаи, при които законовите изисквания за достъп не са спазени.

210.  В годишния си доклад за 2019 г. Комисията отбеляза, че нейни експерти са извършили 136 проверки и отново са станали свидетели на разнопосочни практики, както и пропуски от страна на прокурорите да предложат на компетентните съдии да разпоредят унищожаването на комуникационни данни, които не са от значение (вж. параграф 208, буква б) по-горе). Докладът отново отбелязва различни случаи, при които законовите изисквания за достъп не са спазени.

Да дава указания

211.  Комисията може да дава указания, насочени към подобряване на процедурите за обработване и унищожаване на запазените данни (чл. 261б, ал. 2, т. 4 *in fine* от ЗЕС).

Сезиране на компетентните органи за нередности

212.  Ако Комисията установи, че запазените комуникационни данни са били използвани, съхранявани или унищожени неправомерно, тя трябва да уведоми прокуратурата и да информира ръководителите на съответните органи, търсещи достъп, и доставчиците на комуникационни услуги. Тези ръководители трябва да докладват на Комисията за предприетите стъпки за отстраняване на нередностите (чл. 261б, ал. 4 от ЗЕС).

* + - 1. Изискване за уведомяване
         1. В случай на незаконен достъп или опит за достъп

213.  Ако Комисията установи, че до запазените за дадено лице комуникационни данни неправомерно е осъществен или поискан достъп, тя трябва да го уведоми (чл. 261б, ал. 5 от ЗЕС). Такова уведомяване не се изисква, ако съществува риск за постигане на целта(ите) по чл. 251б, ал. 2 от ЗЕС, заради която (които) е поискан или осъществен достъп до данните (вж. параграф 163 по-горе).

(б) В случай на нарушение на сигурността на личните данни

214.  Ако доставчик на комуникационни услуги узнае за нарушение на сигурността на личните данни, той трябва да уведоми Комисията за защита на личните данни в рамките на три дни (чл. 261в, ал. 1 от ЗЕС). Ако нарушението може да повлияе неблагоприятно на личните данни или личния живот на потребител или друго лице, доставчикът трябва да им съобщи за него (чл. 261в, ал. 2), но може да пропусне да направи това, ако убеди Комисията, че е въвел подходящи технологични и организационни мерки за защита на личните данни, засегнати от нарушението – като например технологични мерки, които правят данните неразбираеми за всеки, който няма разрешение за достъп до тях (чл. 261в, ал. 3). Ако доставчикът сам не е съобщил за нарушението, Комисията, след като е разгледала възможните му неблагоприятни последици, може да изиска от доставчика да съобщи за нарушението на засегнатите лица (чл. 261в, ал. 4). В чл. 261в, ал. 5 посочено минималното съдържание на съобщението.

* 1. РЕЛЕВАНТНИ РАЗПОРЕДБИ ЗА ЗАЩИТА НА ДАННИТЕ

215.  Всички законови разпоредби цитирани по-долу, които са в сила от м. февруари 2019 г., са посочени в редакцията им към 7 декември 2021 г.

* + 1. Приложно поле

216.  Разпоредбите на Закона за защита на личните данни от 2002 г. се прилагат само за физически лица, независимо дали се отнасят до обработването на лични данни, попадащи в обхвата на GDPR (вж. параграф 234 по-долу), или до обработването на такива данни от органите за целите на правоприлагането (чл. 1, ал. 1 и 2). Те не се прилагат за обработването на такива данни за целите на отбраната на страната и националната сигурност, доколкото в специален закон не е предвидено друг (чл. 1, ал. 5).

Б. Относно обработването на лични данни от частни лица

* + - 1. Ограничения на правата на субектите на данни

217.  Администраторът или обработващият лични данни може да ограничи изцяло или частично достъпа, коригирането, заличаването и другите права на субекта на данни, предвидени в членове 12 - 22 от GDPR, или да премахне задължението по член 34 от GDPR за съобщаване на субекта на лични данни за нарушение на сигурността на личните данни, ако упражняването на тези права или изпълнението на това задължение би създало риск за, наред с другото, а) националната сигурност, б) обществения ред и сигурност или в) предотвратяването, разследването, разкриването или наказателното преследване на престъпления (чл. 37а, ал. 1 от Закона за защита на личните данни от 2002 г., който възпроизвежда член 23, параграф 1 от GDPR – вж. параграф 234 по-долу).

* + - 1. Средства за правна защита

218.  Субектите на данни, които считат, че правата им съгласно GDPR или Закона за защита на личните данни от 2002 г. са нарушени, могат да подадат жалба до Комисията за защита на личните данни и да обжалват нейното решение (чл. 38, ал. 1 и 7 от Закона за защита на личните данни, който възпроизвежда член 77, параграф 1 и член 78, параграф 1 и 2 от GDPR – вж. параграф 236 по-долу). Субектите на данни могат също така да обжалват действията или решенията на администратора на данни или обработващия лични данни, или обезщетение за вреди от тях, в случай че са обработили незаконно личните им данни (чл. 39, ал. 1 и 2 от Закона за защита на личните данни, който възпроизвежда член 79, параграф 1 и член 82, параграф 1 от GDPR – вж. точки 237 и 238 по-долу).

* + 1. Относно обработването на лични данни от компетентните органи за целите на правоприлагането
       1. Условия, при които обработването е законосъобразно

219.  Обработването на лични данни от компетентните правоприлагащи органи е законосъобразно, ако е: а) необходимо за предотвратяването, разследването, разкриването или наказателното преследване на престъпление и б) предвидено в правото на Европейския съюз или в нормативен акт, в който са определени целите на обработването и категориите лични данни, които се обработват. (чл. 49 от Закона за защита на личните данни, с който се транспонира член 8 от Директива (ЕС) 2016/680 – вж. параграф 239 по-долу). Тези данни трябва, наред с другото, а) да бъдат обработвани по начин, гарантиращ тяхната сигурност, включително защита срещу неразрешено или незаконно обработване и срещу случайна загуба, унищожаване или повреждане, б) да не бъдат обработвани по начин, несъвместим с изричните законови цели, за които са събрани, и в) да се съхраняват във форма, която позволява идентифицирането на субектите на данни за не по-дълго време от необходимото за целите, за които се обработват (член 45, ал. 1, т. 2, ал. 1, т. 5 и ал. 1, т. 6, транспониращ член 4, параграф 1, букви б), д) и е) от Директивата).

* + - 1. Възможни ограничения на правата на субектите на данни

220.  Администраторът на данни може да забави или да откаже (изцяло или частично) да предостави на субекта на данни информация относно обработването на данни за целите на правоприлагането и правата на субекта на данни във връзка с това обработване, ако това е необходимо, наред с другото, за да се избегне възпрепятстването на служебни или законово регламентирани проверки, разследвания или процедури; б) да се избегнат пречки пред предотвратяването, разкриването, разследването или наказателното преследване на престъпления; в) да се защити обществения ред и сигурност; или г) да се защити националната сигурност (чл. 54, ал. 3 от Закона от 2002 г., с който се транспонира член 13, параграф 3 от Директива (ЕС) 2016/680). Когато пречката престане да съществува, администраторът на данни трябва да предостави исканата информация в срок от два месеца (чл. 54, ал. 4 от Закона от 2002 г.).

221.  Правата на субекта на данни на достъп до, коригиране, заличаване и ограничаване на обработването на неговите лични данни могат да бъдат ограничени на същите основания (член 55, ал. 3 и член 56, ал. 6 от Закона от 2002 г., с който се транспонират членове 14, 15, параграф 1 и 2 и член 16, параграф 4 от Директива (ЕС) 2016/680). Когато пречката престане да съществува, администраторът на данни трябва да предостави исканата информация в срок от два месеца (чл. 55, ал. 3 *in fine* и член 56, ал. 6 *in fine* във връзка с чл. 54, ал. 4 от Закона от 2002 г.). Във всеки случай администраторът трябва да ограничи обработването на лични данни, вместо изцяло да ги заличава, ако тези данни трябва да бъдат запазени за доказателствени цели (член 56, ал. 4, т. 2, с който се транспонира член 16, параграф 3, буква б) от Директивата).

222.  Ако достъпът до лични данни е ограничен съгласно тези разпоредби, администраторът трябва да информира субекта на данните за ограничението и причините за него в срок от два месеца, но може да не го уведоми, ако това би нарушило целта на ограничението (чл. 55, ал. 4 от Закона от 2002 г., с който се транспонира член 15, параграф 3 от Директива (ЕС) 2016/680). В този случай администраторът трябва да документира фактическите или правните основания, на които се основава това решение, и да ги предостави на надзорните органи (Комисията за защита на личните данни или Инспектората към Висшия съдебен съвет (член 55, ал. 5, с който се транспонира член 15, параграф 4 от Директивата).

223.  Ако поправката, заличаването или ограничаването на обработването на лични данни бъде отказано съгласно горните разпоредби, администраторът трябва да информира субекта на данните за ограничението и причините за него в срок от два месеца, но може да не направи това, ако това би обезсмислило целта на отказа. В този случай администраторът на данни трябва да представи причините за отказа на субекта на данните в срок от два месеца, след като пречката престане да съществува (чл. 56, ал. 7 от Закона за защита на личните данни, с който се транспонира член 16, параграф 4 от Директива (ЕС) 2016/680).

224.  Във всички тези случаи на ограничаване на правата на субектите на данни те могат да упражняват своите права непряко чрез Комисията за защита на личните данни или Инспектората към Висшия съдебен съвет (в зависимост от това дали данните се обработват от съдебен или несъдебен орган – вж. параграф 225 по-долу). Ако получат такава жалба, посочените органи трябва да проверят дали ограничението е законосъобразно (чл. 57, ал. 1 от Закона за защита на личните данни, с който се транспонира член 17, параграф 1 от Директива (ЕС) 2016/680). Те трябва да уведомят субекта на данните най-малко за това, че са извършени всички необходими проверки, както и за правото му да търси съдебна защита (чл. 57, ал. 2, транспониращ член 17, параграф 3 от Директивата).

* + - 1. Надзорни органи

225.  Комисията за защита на личните данни осъществява надзор върху обработването на лични данни за целите на правоприлагането от всички органи, с изключение на съдилищата, прокуратурата и разследващите органи. Обработването на лични данни за целите на правоприлагането от съдилищата, прокуратурата и следствените органи се контролира от Инспектората към Висшия съдебен съвет (чл. 78 от Закона за защита на личните данни, с който се транспонира член 41 от Директива (ЕС) 2016/680).

226.  При извършването на този надзор Комисията и Инспекторатът трябва, наред с другото, а) да разгледат жалбите на субектите на данни, б) да проверят законосъобразността на обработването на данни в случаите, когато правата на субекта на данни са били ограничени (вж. параграфи 220 до 223 по-горе), и в) да информират субекта на данни в срок от три месеца за резултата от проверката или за причините, поради които такава не е извършена (чл. 79, ал. 1, т. 5 и 6 от Закона за защита на личните данни, с който се транспонира член 46, параграф 1, букви е) и ж) от Директива (ЕС) 2016/680).

* + - 1. Средства за правна защита

227.  Субектите на данни имат право на същите средства за правна защита за предполагаеми нарушения на правата им от страна на правоприлагащите органи, каквито имат за предполагаеми нарушения на правата им от частни лица (вж. параграф 218 по-горе) (чл. 82, ал. 1 от Закона за защита на личните данни, с който се транспонират член 52, параграф 1 и член 54 от Директива (ЕС) 2016/680).

1. РЕЛЕВАНТНИ РЕШЕНИЯ НА КОМИТЕТА НА МИНИСТРИТЕ НА СЪВЕТА НА ЕВРОПА

228.  До момента Комитетът на министрите на Съвета на Европа е разглеждал мерките по изпълнението на решението на Съда по делото *Асоциация за европейска интеграция и права на човека и Екимджиев* (цитирано по-горе) през март 2013 г., юни 2017 г. и юни 2019 г. Комитетът наблюдава мерките по изпълнението в рамките на процедура по засилено наблюдение, като производството пред него е висящо.

229.  В трите си решения, приети досега в хода на това наблюдение (CM/Del/Dec(2013) 1164/8; CM/Del/Dec(2017)1288/H46-7; и CM/Del/ Dec(2019)1348/H46-5), Комитетът отбеляза напредъка, произтичащ от законодателните реформи, предприети от българските органи в тази област, но също така подчерта, *inter alia*, следните (нерешени) въпроси, пораждащи безпокойство или несигурност във връзка с общите мерки, необходими за изпълнението на това решение:

а) липсата на яснота относно това дали СРС може да се използват за защита на националната сигурност, ако лицата, по отношение на които ще се прилагат СРС, не са заподозрени в престъпление;

б) практическия капацитет на съдилищата, които получават голям обем искания за използване на СРС - по-специално на Специализирания наказателен съд (вж. таблицата в пар. 49 по-горе) – да ги обработят по подходящ начин;

в) максималния срок на първоначалното разрешение за използване на СРС за защита на националната сигурност (две години – вж. пар. 79, буква б) по-горе);

г) липсата на достатъчно публично достъпни детайли относно процедурите за проверка и унищожаване на информацията, получена чрез прилагане на СРС, и запазването на нейната поверителност и цялост (вж. пар. 87 - 99 по-горе);

д) професионалната квалификация на членовете на Националното бюро и тяхната независимост по отношение на органите, върху които упражняват надзор (вж. пар. 109 и 112 *in fine* по-горе); възможността Бюрото да има достъп до всички материали, от които се нуждае, за да изпълнява своите задачи, включително до материалите, на които се основават исканията за използване на СРС (вж. пар. 118 и 119 по-горе); и компетентността на Бюрото да уведомява юридическите лица, а не само физическите лица, за незаконното прилагане на СРС (вж. точка 130 по-горе); и

е) възможността гражданските съдилища да установяват фактите в производствата по член 2, ал. 1, точка 7 от ЗОДОВ в ситуации, в които ищците не са официално уведомени (или са разбрали по друг начин), че по отношение на тях са използвани СРС (вж. пар. 140 -144 по-горе) и липсата на сигурност какви са правомощията на съдилищата да разпореждат унищожаването на материалите от прилагането на СРС.

1. РЕЛЕВАНТНО ПРАВО НА ЕВРОПЕЙСКИЯ СЪЮЗ
   1. ДИРЕКТИВА ЗА ПРАВОТО НА НЕПРИКОСНОВЕНОСТ НА ЛИЧНИЯ ЖИВОТ В ЕЛЕКТРОННИТЕ КОМУНИКАЦИИ

230.  По силата на член 15, параграф 1 от Директива 2002/58/ЕО относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации („Директива за правото на неприкосновеност на личния живот в електронните комуникации“) държавите членки могат да предприемат законодателни мерки, предвиждащи съхраняването на комуникационни данни за ограничен период от време, ако това е оправдано от необходимостта да се „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“.

231.  По силата на член 15, параграф 2 от същата Директива във връзка с член 94, параграф 2 от ОРЗД всички разпоредби на ОРЗД относно съдебните средства за защита, свързани с обработката на лични данни, се прилагат по отношение на националните разпоредби, приети съгласно Директивата за правото на неприкосновеност на личния живот в електронните комуникации.

* 1. ДИРЕКТИВА ОТНОСНО ЗАПАЗВАНЕТО НА ДАННИ

232.  Член 3 във връзка с член 5 и член 6 от Директива 2006/24/ЕО за запазване на данни, създадени или обработени във връзка с предоставянето на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи („Директива относно запазването на данни“), изисква от държавите членки да приемат мерки, за да гарантират, че някои категории комуникационни данни, генерирани или обработени от доставчици на а) обществено достъпни електронни съобщителни услуги или на б) обществени съобщителни мрежи в рамките на тяхната юрисдикция, се запазват за периоди между шест месеца и две години.

233.  В решение от 8 април 2014 г. *Digital Rights Ireland and Others* (C‑293/12 и C‑594/12, EU:C:2014:238) Съдът на ЕС постанови, че Директивата е невалидна като цяло въз основа на това, че изисква непропорционална намеса в правото на зачитане на личния живот и комуникацията, защитени съгласно член 7 от Хартата на основните права на Европейския съюз, и в правото на защита на личните данни по член 8 от Хартата. Първо, Директивата изискваше запазване на всички данни за трафика и се прилагаше за всички средства за електронна комуникация. На второ място, Директивата не определяше материалноправните и процесуалноправните предпоставки, уреждащи достъпа на органите до запазените данни или тяхното последващо използване, и не обвързваше този достъп с предварителен контрол от съд или независим административен орган, чието решение би могло да ограничи достъпа до данните и използването им до строго необходимото. На трето място, Директивата изискваше всички данни да се съхраняват за период от най-малко шест месеца, без да прави разграничение между категориите данни въз основа на тяхната полезност или на засегнатите лица. На последно място, Директивата не предвиждаше достатъчно гаранции за ефективната защита на съхраняваните данни срещу риск от злоупотреба или от незаконен достъп и използване.

* 1. ОБЩ РЕГЛАМЕНТ ОТНОСНО ЗАЩИТАТА НА ДАННИТЕ

234.  Регламент (ЕС) 2016/679 относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни („Общ регламент относно защитата на данните – ОРЗД“) се прилага за „физически лица“ и не обхваща обработването на лични данни, което се отнася до юридически лица (съображение 14). По силата на член 23, параграф 1 законодателна мярка на държавите членки може да ограничи обхвата на задълженията и правата, предвидени в членове 12 - 22 и член 34, „когато подобно ограничение е съобразено със същността на основните права и свободи и представлява необходима и пропорционална мярка в едно демократично общество с цел да се гарантира“, наред с другото, а) националната сигурност, б) обществената сигурност и в) предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наложените наказания, включително предпазването от и предотвратяването на заплахи за обществената сигурност.

235.  Ако е приложимо, всяка такава законодателна мярка трябва, наред с други неща, да съдържа разпоредба за правото на субектите на данни да бъдат информирани за ограничаването, освен ако това би било в разрез с целта на ограничаването (член 23, параграф 2, буква з) от ОРЗД).

236.  Всеки субект на данни има право да подаде жалба до надзорен орган, ако „счита, че обработването на лични данни, отнасящи се до него, нарушава [ОРЗД]“ (член 77, параграф 1 от ОРЗД).

237.  Всеки субект на данни също така има право, при същите обстоятелства, на ефективна правна защита (член 79, параграф 1 от ОРЗД).

238.  Всяко лице, което е претърпяло материални или неимуществени вреди в резултат на нарушение на ОРЗД, има право да получи обезщетение от администратора или обработващия лични данни (член 82, параграф 1 от ОРЗД). Членове 82 §§ 2 до 4 уреждат условията, при които може да се иска такова обезщетение.

* 1. ДИРЕКТИВА ОТНОСНО ПРАВОПРИЛАГАНЕТО

239.  Директива (ЕС) 2016/680 относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни урежда обработването на лични данни на „физически лица“ от компетентните органи за целите на „предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазването и предотвратяването на заплахи за обществената сигурност“ (член 1, параграф 1 и член 2, параграф 1). Тя трябваше да бъде транспонирана до май 2018 г. (член 63, параграф 1). България направи това чрез изменение на Закона от 2002 г. през март 2019 г. (вж. точки 219 - 227 по-горе).

* 1. ПРАКТИКА НА СЪДА НА ЕС ПО ЧЛЕН 15, ПАРАГРАФ 1 ОТ ДИРЕКТИВАТА ЗА ПРАВОТО НА НЕПРИКОСНОВЕНОСТ НА ЛИЧНИЯ ЖИВОТ В ЕЛЕКТРОННИТЕ КОМУНИКАЦИИ

240.  С решение от 21 декември 2016 г. (*Tele2 Sverige and Watson and Others*, C‑203/15 и C‑698/15, EU:C:2016:970), постановено въз основа на преюдициални запитвания от Апелативния административен съд на Стокхолм, Швеция, и от Апелативния съд на Англия и Уелс, Съдът на ЕС постанови, че националното законодателство, предвиждащо общо запазване на всички данни за трафика и местоположението с цел борба с престъпността, е недопустимо съгласно член 15, параграф 1 от Директивата за правото на неприкосновеност на личния живот в електронните комуникации (вж. пар. 230 по-горе). Член 15, параграф 1 също така не допуска законодателство, което позволява на органите да имат достъп до съхраняваните данни, ако, доколкото това е от значение за целите на настоящия случай, а) целта не е била ограничена до борбата с тежката престъпност и б) този достъп не е бил предмет на предварителен преглед от съд или независим орган. Съдът на ЕС основава тези заключения, наред с другото, на общата структура на Директивата за правото на неприкосновеност на личния живот, включително на общия принцип на поверителност на съобщенията, установен от него, и на изискването за стриктна необходимост съгласно правото на Европейския съюз от всякакви ограничения на защитата на личните данни. На последно място, Съдът на ЕС отказа да отговори на въпрос дали защитата, предоставена от членове 7 и 8 от Хартата, както се тълкува от нея, е по - широка от защитата, предоставена съгласно член 8 от Конвенцията. Той отбеляза, наред с другото, че правото на Европейския съюз би могло да предостави по - широка защита от Конвенцията и че член 8 от Хартата се отнася до право (защита на личните данни), което няма еквивалент в Конвенцията.

241.  В решение от 2 октомври 2018 г. (*Ministerio Fiscal*, C-207/16, EU:C:2018:788), постановено въз основа на предварително запитване от Провинциалния съд на Тарагона, Испания, Съдът на ЕС постанови, че намесата, свързана с достъпа до запазени имена и адреси за идентифициране на собствениците на SIM карти, активирани с откраднат мобилен телефон, не е достатъчно сериозна и следователно е допустима съгласно член 15, параграф 1 от Директивата за правото на неприкосновеност на личния живот в електронните комуникации, дори и да не е оправдана от необходимостта от борба с „тежката“ престъпност.

242.  С решение от 6 октомври 2020 г. (*La Quadrature du Net and Others*, C‑511/18, C‑512/18 и C‑520/18, EU:C:2020:791), постановено въз основа на предварителни позовавания от страна на Държавния съвет на Франция и белгийския Конституционен съд, Съдът на ЕС, наред с другото, потвърди позицията си в *Tele2 Sverige and Watson and Others* (вж. точка 240 по-горе), че член 15, параграф 1 от Директивата за правото на неприкосновеност на личния живот в електронните комуникации не допуска общото запазване на данни за трафика и местонахождението с цел борба с тежката престъпност и счете, че тази разпоредба позволява единствено целенасочено съхраняване на такива данни, ограничено въз основа на обективни и недискриминационни фактори. За разлика от това член 15, параграф 1 не изключва общото запазване на а) IP адресите на източника на интернет връзка и б) данните, свързани с гражданската идентичност на потребителите на комуникационни системи. Всеобщото запазване на данни за трафика и местоположението – за период, ограничен до строго необходимото – е допустимо, ако дадена държава е изправена пред реална и сериозна заплаха за националната сигурност, която е налице или e предвидима. Решението обаче, което се позовава на такава заплаха, за да обоснове общо задържане, трябва да бъде предмет на ефективен контрол или от съд, или от независим административен орган, чието решение е задължително. Този контрол трябва да обхваща и спазването на предварително определени условия и гаранции.

243.  В друго решение от 6 октомври 2020 г. (*Privacy International*, C‑623/17, EU:C:2020:790), постановено въз основа на предварително запитване от Трибунала на Обединеното кралство за разследващите правомощия, СЕС постанови, наред с другото, че член 15, параграф 1 от Директивата за правото на неприкосновеност на личния живот в електронните комуникации не допуска законодателство, което дава възможност на даден орган да изисква от доставчиците на съобщителни услуги да извършват общо предаване на данни за трафика и местоположението на агенциите за сигурност и разузнаване с цел защита на националната сигурност.

244.  В решение от 2 март 2021 г. (*Prokuratuur*, C‑746/18, EU:C:2021:152), постановено въз основа на предварително запитване от страна на Върховния съд на Естония, Съдът на ЕС потвърди, че член 15, параграф 1 от Директивата за правото на неприкосновеност на личния живот в електронните комуникации позволява достъп до запазен трафик или данни за местонахождението с цел борба с престъпността, само когато става въпрос за тежко престъпление или сериозни заплахи за обществената сигурност, независимо от продължителността на периода, за който се иска достъп, и от количеството или естеството на наличните данни за този период. Освен това Съдът на ЕС счита, че правомощието за разглеждане на исканията за достъп не може да бъде предоставено на прокуратурата, тъй като нейните правомощия по водене на досъдебното производство и повдигане и поддържане на обвинение в съдебната фаза засягат нейната независимост по отношение на страните в наказателното производство.

245.  Разглеждането на три предварителни запитвания относно съвместимостта на германското и ирландското законодателство, които изискват общо запазване на комуникационните данни с член 15, параграф 1 от Директивата за правото на неприкосновеност на личния живот в електронните комуникации, направени съответно от германския федерален административен съд през октомври 2019 г. и от Върховния съд на Ирландия през март 2020 г. (*SpaceNet*, C-793/19; *Telekom Deutschland*, C-794/19; и *Commissioner of the Garda Síochána and Others*, № C-140/20) все още предстои.

1. ПРАВОТО
   1. ТАЙНО НАБЛЮДЕНИЕ

246.  Жалбоподателите се оплакват, че системата за прилагане на СРС в България не отговаря на изискванията на член 8 от Конвенцията и че в това отношение те не разполагат с ефективни средства за защита в нарушение на член 13 от Конвенцията.

247.  С оглед на практиката на Съда (вж. *Roman Zakharov срещу Russia* [GC], № 47143/06, § 307, ЕСПЧ 2015) жалбата подлежи на разглеждане единствено по член 8 от Конвенцията, който предвижда, доколкото е приложимо:

„1.  Βсеки има право на неприкосновеност на личния ... си живот, на жилището и на тайната на кореспонденцията.

2.  Намесата на държавните власти в ползването на това право е недопустима освен в случаите, предвидени в закона и необходими в едно демократично общество в интерес на националната и обществената сигурност или на икономическото благосъстояние на страната, за предотвратяване на безредици или престъпления, за защита на здравето и морала или на правата и свободите на другите.“

* + 1. Допустимост
       1. Твърденията на страните
          1. Статус на жертва на жалбоподателите

Правителството

248.  Правителството твърди, че жалбоподателите не могат да твърдят, че са жертва на нарушение на правото им на зачитане на личния живот или кореспонденция. Това е така, защото по българското законодателство само хора, заподозрени в тежки престъпления, могат да бъдат поставени под наблюдение, дори когато става дума за национална сигурност. Нищо не подсказва, че в настоящото дело някой от жалбоподателите попада в тази категория. Тази възможност по принцип е немислима за двете организации-жалбоподатели, тъй като в България юридическите лица не носят наказателна отговорност.

249.  Освен това никой от жалбоподателите, въпреки експертния си опит, не е подал искане до Националното бюро с въпрос дали по отношение на тях са използвани специални средства за наблюдение. Също така никой от жалбоподателите-физически лица не се е опитал да предяви иск съгласно член 2, ал. 1, точка 7 от ЗОДОВ, който може да бъде предявен дори без уведомление от Бюрото, че срещу тях са били използвани специални разузнавателни средства. И двете процедури представляват ефективни средства за защита. От това следва, че жалбоподателите е следвало да докажат, че са изложени на риск от наблюдение поради личното си положение – нещо, което не са направили. Това не е и много вероятно, тъй като нищо не предполага, че те могат да бъдат заподозрени в някое от престъпленията, за които е позволено използване на тайно наблюдение в България.

Жалбоподателите

250.  В отговор жалбоподателите посочват, че съгласно начина, по който е устроена системата за тайно наблюдение в България, комуникациите на всеки в страната могат да бъдат прихванати по няколко причини. Първо, законите, позволяващи наблюдение, са разписани с общи и неясни термини, особено що се отнася до понятието за национална сигурност. Второ, много държавни органи имат право да поискат наблюдение, а органите на прокуратурата имат неконтролируемо правомощие да започнат наказателно производство срещу всеки. Трето, процедурите за издаване на разрешения са рутинно пренебрегвани. На последно място, на практика контролът от страна на Националното бюро е неефективен, което прави безсмислено жалбоподателите да се оплакват пред него, особено като се има предвид, че те могат да бъдат подлагани на непряко наблюдение чрез поставянето на техни контакти под наблюдение. Жалбоподателите не са предявили иск по член 2, ал. 1, точка 7 от ЗОДОВ, тъй като той би бил неефективен в тяхното положение и освен това не е на разположение на двете организации-жалбоподатели, тъй като е на разположение само на физически лица. Следователно не е необходимо някой от тях да доказва, че е изложен на риск да бъде подложен на наблюдение поради личното си положение.

(б) Изчерпване на вътрешноправните средства за защита

251.  Въз основа на съображенията, обобщени в пар. 249 по-горе, правителството също така изтъква, че заявителите не са изчерпали националните средства за защита.

252.  Жалбоподателите опонират, че поради причините, обобщени в пар. 250 по-горе, средствата за правна защита, предложени от правителството, не са ефективни в тяхната ситуация.

* + - 1. Оценката на Съда
         1. Дали жалбата е „по същество същата“

253.  Първият въпрос, който възниква, е дали настоящата жалба е „по същество същата“ като разглежданата в *Асоциацията за европейска интеграция и права на човека и Екимджиев срещу България* (№ 62540/00, 28 юни 2007 г.). Съдът трябва да разгледа въпроса по своя собствена инициатива, с оглед очертаване границите на своята компетентност (вж. *Harkins/Обединено кралство* (dec.) [GC], № 71537/14, § 55, 15 юни 2017 г.).

254.  Съдът счита, че това не е така по следните причини.

255.  Вярно е, че двама от жалбоподателите – г-н Екимджиев и Асоциацията за европейска интеграция и права на човека – са същите като в предишното дело и че същността на тяхното оплакване по настоящата жалба, както е формулирано от тях, е идентично със същността на разглежданото оплакване в първата жалба. Настоящата жалба обаче не се основава на същите факти. По това по-ранно дело Съдът разгледа внимателно системата за тайно наблюдение в България към средата на 2007 г., докато по настоящото дело той трябва да направи анализ на тази система в сегашния ѝ вид (вж. пар. 293 по - долу). Съответните законови и подзаконови разпоредби в България претърпяха значително развитие от 2007 г. насам, а също и начинът на тяхното прилагане (вж. по-специално пар. 13 - 16 по-горе). Всичко това е „релевантна нова информация“ по смисъла на член 35, параграф 2, буква б) от Конвенцията (вж., *mutatis mutandis*, *Verein gegen Tierfabriken Schweiz (VgT) v. Switzerland (№ 2)* [GC], № 32772/02, § 64 -65, ЕСПЧ 2009 г. и *Ivanśoc nd Others v. Moldova and Russia*, № 23687/05, § 93, 15 ноември 2011 г.). Разбира се, този израз трябва да се тълкува като значима нова *фактическа* информация (вижте *Harkins*, цитирано по-горе, § 50). Но в случаи като разглеждания, когато жалбата се основава по-скоро на състоянието на вътрешното право, отколкото на прилагането му спрямо конкретен случай, основният факт, предмет на разглеждане, е вътрешното право и начинът, по който то се прилага като цяло.

* + - * 1. Дали Съдът е възпрепятстван да разгледа жалбата по член 46 от Конвенцията

256.  Вторият въпрос, който възниква, е дали Съдът е възпрепятстван да разгледа жалбата в съответствие с член 46 от Конвенцията. Този въпрос касае компетентността на Съда и също трябва да бъде разгледана по негова инициатива. Тя е тясно свързана с въпроса, разгледан в пар. 253 - 255 по-горе.

257.  Текущото наблюдение на българските закони и практика, свързани с тайното наблюдение, от страна на Комитета на министрите при осъществяване на неговата задача по контрол на изпълнението на *Асоциация за европейска интеграция и права на човека и* *Екимджиев* (цитирано по-горе) (вж. пар. 228 и 229 по-горе) не е пречка за допустимостта на жалбата. Задачата на Съда по настоящото дело не е да прецени дали общите мерки, предприети от българските органи, са достатъчни за изпълнение на задължението им по член 46, ал. 1 от Конвенцията да се съобразят с това решение; Съдът не е компетентен да направи това (вж. *Ivanţoc and Others*, цитирано по-горе, точка 91). Неговата задача тук е по - скоро да проучи дали оплакването, че системата за тайно наблюдение в България в сегашния си вид – отчасти резултат на общи мерки, предприети за изпълнение на решението *Асоциация за европейска интеграция и права на човека и* *Екимджиев* (цитирано по-горе) (вж. точка 14 по – горе) – не отговаря на изискванията на член 8 от Конвенцията, е допустимо и обосновано. Въпреки че тази проверка може на практика да се припокрива или дори частично да съвпада с контрола, осъществяван от Комитета на министрите, това не поставя жалбата извън компетентността на Съда. Ролята на Комитета на министрите в изпълнението на решенията на Съда не означава, че мерките, предприети от ответната държава за отстраняване на нарушението, установено от Съда, не могат да повдигнат нов въпрос, нерешен от по - ранното решение, и като такъв представляват предмет на нова жалба, с която Съдът може да се занимава (вж. *Verein gegen Tierfabriken Schweiz (VgT) (№ 2),* цитиран по-горе, § 62; Bochan/*Ukraine (№ 2)* [GC], № 22251/08, § 33, ECHR 2015; и *Moreira Ferreira/Portugal (№ 2)* [GC], № 19867/12, § 47, буква б), 11 юли 2017 г.). В този контекст „нов въпрос“ предполага съществуването на „съответна нова информация“ по смисъла на член 35, параграф 2, буква б) от Конвенцията (вж. *Verein gegen Tierfabriken Schweiz (VgT) (№ 2)*, § 63; *Ivanţoc and Others*, § 85; и *Moreira Ferreira*, § 47 (d), всички цитирани по-горе). Но, както е отбелязано в точка 255 по-горе, такава „релевантна нова информация“ е налице в настоящия случай (сравнете *mutatis mutandis* с Mehemi *срещу Франция (№ 2),* № 53470/99, § 43 -44, ECHR 2003 - IV; *Wasserman срещу Русия (№ 2),* № 21071/05, § 34 -37, 10 април 2008 г.; *Liu срещу Русия (№ 2),* № 29157/09, § 62 -67, 26 юли 2011 г.; Ivanśoc *и други*, цитирани по-горе, § 89 -95; и *V.D. срещу Хърватия (№ 2),* № 1921/15, § 49 -54, 15 ноември 2018 г.).

258.  Поради това Съдът е компетентен да разгледа жалбата.

* + - * 1. Статут на жертва и изчерпване на вътрешноправните средства за защита

259.  Възраженията на правителството, че жалбоподателите не могат да претендират, че са жертви на нарушение, и че не са изчерпали вътрешните правни средства за защита, са толкова тясно свързани със съществото на жалбата на жалбоподателите, че те трябва да бъдат разгледани, заедно с въпросите по основателността й (вж. по-горе, пар. 150).

* + - * 1. Заключение относно допустимостта на жалбата

260.  Освен това жалбата не е явно неоснователна по смисъла на член 35, параграф 3, буква а) от Конвенцията или недопустима на други основания. Следователно тя трябва да бъде обявена за допустима.

* + 1. По същество на оплакванията
       1. Статус на жертва на жалбоподателите и наличие на намеса
          1. Твърденията на страните

261.  Становищата на страните по тези въпроси са обобщени в пар. 248 -250 по-горе.

* + - * 1. Оценката на Съда

Общи принципи

262.  Общите принципи за това кога жалбоподателите могат да твърдят, че са жертва на намеса в техните права съгласно член 8 от Конвенцията поради самото съществуване на национални закони или практики, позволяващи тайно наблюдение, бяха изяснени в решението по делото *Roman* Zakharov (посочено по-горе, § 171) и по-горе в решението по делото *Centrum för rättvisa/Швеция* ([GC], № 35252/08, § 167, 25 май 2021 г.).

Прилагане на тези принципи

Обхват на приложимия закон

263.  Съгласно разпоредбите на член 12 от ЗСРС специални разузнавателни средства могат да се използват по отношение, *inter alia*, на: а) лица, заподозрени, или използвани без да им е известен престъпният характер на извършваната дейност, в подготовката или извършването на едно или повече от тежките престъпления, изброени в чл. 3, ал. 1 от ЗСРС. б) лица или предмети, свързани с националната сигурност; и в) предмети, необходими за идентифицирането на такива лица (вж. параграф 23 по-горе). Следователно формулировката на член 12 предполага, че националната сигурност може да бъде самостоятелно основание за използване на тайно наблюдение; това следва също от член 4 (вж. параграф 22 по-горе). Но дори и да се приеме, че, както твърди правителството по отношение на текста на чл. 14 от ЗСРС (вж. параграф 22 по-горе), съгласно българското законодателство националната сигурност не може да бъде самостоятелно основание за прибягване до тайно наблюдение, остава хипотезата, че теоретично всяко лице в страната може да бъде заподозряно в участие, съзнателно или несъзнателно, в планирането или извършването на съответното престъпление и по този начин да бъде подложено на наблюдение. Също така е ясно, че независимо дали самите те са били поставени под наблюдение, физическитеили юридическите лица могат да бъдат прихванати непряко в резултат на наблюдението на друго лице, попадащо в една от категориите, определени в чл. 12 от ЗСРС. От това следва, че и четиримата жалбоподатели, включително двете организации, могат евентуално да бъдат засегнати от спорното законодателство. Вярно е, че някои техники за наблюдение, като визуално наблюдение и проследяване (вж. параграф 11 по-горе), не могат да се прилагат за юридически лица като такива. Изглежда обаче, че в много случаи разрешенията за прилагане на СРС включват използването на тези техники заедно с други техники за наблюдение, като например подслушване, които могат да засегнат комуникацията на юридическите лица (вж. пар. 61 и 65 по-горе).

Наличие на ефективни средства за защита

264.  Следващият въпрос е дали в България съществува ефективно средство за защита, което може да смекчи подозрението сред широката общественост, че се злоупотребява с правомощия за тайно наблюдение.

265.  През 2009 г. България въвежда специално средство за защита по отношение на тайното наблюдение под формата на иск за обезщетение за вреди съгласно член 2, ал. 1, точка 7 от ЗОДОВ (вж. параграф 136 по-горе). Съдът признава, че подобно твърдение е ефективно средство за защита за хора, които вече са научили, че са били обект на наблюдение в резултат на наказателно производство, в случаите, когато наблюдението е било извършено след влизането в сила на тази разпоредба (вж. *Харизанов срещу България* (дек.), № 53626/14, § 94 -99, 5 декември 2017 г.).

266.  Това обаче се отнася само до ситуации, в които наблюдението е дало информация, която е довела до изготвянето на веществени доказателствени средства, използвани по – късно – и следователно оповестени – в наказателното производство. През последното десетилетие случаите на наблюдение, които са довели до изготвянето на такъв доказателствен материал, варират от около 24% до около 60% (вж. таблицата в пар. 93 по-горе). И далеч не е сигурно, че във всички случаи тези доказателствени материали впоследствие са довели до повдигане на обвинения и по този начин са били разкрити на засегнатите лица в рамките на наказателното производство.

267.  Изглежда, че във всички случаи, в които това не се е случило, единственият (законосъобразен) начин, по който засегнатите лица могат да научат, че са били подложени на наблюдение, е уведомление от Националното бюро. Но ЗСРС не изисква уведомяване на всяко лице. Независимо дали проучва по своя инициатива или по искане на някой, който подозира, че е бил подложен на наблюдение, Бюрото е длъжно да уведомява само лицата, които са били подложени на наблюдение неправомерно (по смисъла на ЗСРС). Дори в тази ситуация уведомяването е възможно само ако не нарушава целта на наблюдението или не разкрива техническите или оперативните средства, с които то е било извършено (вж. параграф 130 по-горе). На практика всяка година Бюрото уведомява малък брой лица, ако изобщо има такива, , дори в сравнение с броя на исканията, които получава (вж. таблицата в пар. 135 по-горе). Изглежда, че в други случаи то просто информира лицата, които са подали заявление, че не са били подложени на незаконно наблюдение, без да уточнява дали това означава, че а) не е извършено наблюдение, че б) то е осъществено, но е законосъобразно, или в) че то наистина е било незаконно, но не следва да бъде разкривано, тъй като това би нарушило целта му или би разкрило техническите или оперативните средства, с които е извършено (вж. параграф 131 по-горе). В хипотеза в) формулировката на уведомлението на Бюрото, произтичаща от трите примера, предоставени на Съда (вж. параграф 131 по-горе), всъщност би била подвеждаща, тъй като е налице незаконосъобразно наблюдение, но има основания да се скрие, че то е извършено. Получателите на такива уведомления нямат възможност да ги оспорват и по този начин да получат повече информация (вж. параграф 133 по-горе).

268.  Освен това, противно на твърденията на правителството, не изглежда, че производството за обезщетение за вреди съгласно член 2, ал. 1, точка 7 от ЗОДОВ (вж. параграф 136 по-горе) е на разположение на лица, които не са били уведомени от Националното бюро, че са били подложени на наблюдение или са научили за това наблюдение в резултат на наказателно производство, в което са били използвани резултатите от него. Вярно е, че член 2, ал. 1, точка 7 от него не поставя такова уведомление като условие за допустимостта на такива искове. Въпреки че тази разпоредба вече е в сила повече от дванадесет години, не са представени случаи, в които исковете по нея да са били успешно предявени при липса на предварително уведомление от Бюрото или на информация относно наблюдението, което е възникнало в рамките на наказателното производство (вж. пар. 140 по-горе). Действително очевидно ограничените възможности за установяване на фактите на гражданските съдилища в производствата по член 2, ал. 1, точка 7 вече са отбелязани от Комитета на министрите в контекста на неговия контрола върху изпълнението на *Асоциация за европейска интеграция и права на човека и Екимджиев* (цитирано по-горе) (вж. пар. 229, буква е) по-горе).

269.  Начинът, по който българските съдилища прилагат правилата за доказване в такива случаи, предполага, че липсата на уведомление от Националното бюро или на информация за наблюдението, която е получена в наказателното производство, вероятно ще бъде непреодолима пречка за воденето на такива искове (вж. пар. 141, 142 и 144 по-горе). Това е признато, макар и косвено, от Върховния касационен съд, който постановява, че давностният срок за предявяване на такъв иск започва да тече, когато съответното лице бъде уведомено от Бюрото, тъй като без такова уведомяване това лице не разполага със средства за доказване на своите права (вж. пар. 138, буква з) по-горе). В скорошен случай Бургаският районен съд дори изрично постановява, че иск по чл. 2, ал. 1, т. 7 от ЗОДОВ може да бъде предявен само ако използването на специални разузнавателни средства по отношение на ищеца е видно или от представените като доказателство по наказателно дело материали, или от уведомление на Бюрото (вж. пар. 143 по-горе).

270.  При липса на представени решения от българските съдилища, този съд не е в състояние да каже дали или как в такива случаи могат да се прилагат правилата на гражданското производство в България, които уреждат разкриването на документи от възразяващата страна, от трета страна или от публичен орган (вж. пар. 146 -150 по-горе). Правителството трябваше да обясни този въпрос и доколкото е възможно, да подкрепи техните обяснения с конкретни примери (вж. *mutatis mutandis*, *Roman Zakharov*, цитирано по-горе, § 295, и *Mustafa Sezgin Tanrıkulu v. Turkey*, № 27473/06, § 28 -29, 18 юли 2017 г.). Достатъчно е да се отбележи, че в продължение на дванадесет години очевидно не е имало случаи, в които тези процедурни възможности са били използвани за преодоляване на липсата на предварително уведомление от Националното бюро или на разкрита в рамките на наказателното производство информация относно наблюдението.

271.  Друга пречка за желаещите да предявят такъв иск, без да имат предварително уведомление, е идентифицирането на правилния ответник, което трябва да бъде направено в началото на производството (вж. пар. 138, буква в) по-горе), но въпреки това може да бъде невъзможно при липса на каквато и да е информация за това кой орган е поискал наблюдението или го е извършил (вж. *mutatis mutandis*, *Ribcheva and Others v. Bulgaria*, № 37801/16 и 2 други, § 149 *in fine*, 30 март 2021 г.).

272.  Допълнително ограничение на правната защита съгласно член 2, ал. 1, точка 7 от ЗОДОВ се дължи на степента на контрол, прилагана от съдилищата при разглеждането на такива искове. Върховният касационен съд е постановил, че при вземането на решение по такива искове съдилищата не могат да проверяват дали съдиите, издали разрешение за прилагане на СРС, правилно са преценили необходимостта от това (вж. параграф 138, буква е) по-горе). Това означава, че съдилищата могат да проверяват за формални пропуски, но не могат да се задълбочат в най-важните въпроси – дали наблюдението, чиято законност се оспорва пред тях, се основава на основателно подозрение и представлява пропорционална намеса в правата на ищеца съгласно член 8 от Конвенцията. Това ограничение лишава тази гаранция от голяма част от нейната ефикасност.

273.  На последно място, както е видно от текста на разпоредбата (вж. точка 136 по-горе), такива искове не са на разположение на юридически лица.

274.  Поради всички тези ограничения средствата за правна защита, предвидени в член 2, ал. 1, точка 7 от ЗОДОВ, не могат да разсеят в достатъчна степен опасенията на обществеността относно заплахата от злоупотреба с тайно наблюдение.

275.  Тези опасения не могат да бъдат разсеяни с аргумент, че съществуват други възможни средства за защита. Правителството не посочи, а и няма данни в тази насока, че досега е имало случаи, в които някой е бил в състояние да постигне унищожаване на данни, получени чрез наблюдение, като се позовава на член 56, ал. 6 *in fine* от Закона за защита на личните данни, изменен през 2019 г., за да транспонира Директива (ЕС) 2016/680 (вж. точка 221 по-горе), да получи правна защита чрез жалба до Комисията за защита на личните данни или до Инспектората към Висшия съдебен съвет съгласно член 57 от същия закон (вж. точка 224 по-горе) или да получи защита чрез производство по член 82, ал. 1 от Закона от 2002 г., и двете добавени по начин през 2019 г. (вж. точка 227 по-горе). Вярно е, че тези разпоредби са нови и че те са част от правна материя, която се е развила сравнително наскоро. Но при липса на информация относно начина, по който те могат да действат по отношение на данните, получени чрез тайно наблюдение (за разлика от обстоятелствата в *Tretter and Others v. Austria* (дек.) [Комитет], № 3599/10, §§ 10 -14 и 43 -46, 29 септември 2020 г.), Съдът не може да спекулира по въпроса. Освен това тези средства за правна защита не са достъпни за юридическите лица (вж. пар. 216 и 239 по-горе).

Заключение

276.  С оглед на изложените по-горе съображения не е необходимо да се проверява дали жалбоподателите са изложени на риск от прихващане на техните съобщения поради личното им положение (вж. *mutatis mutandis*, *Centrum för rättvisa*, посочено по-горе, §§ 175 -76).

277.  От това следва, че разглеждането на съответните закони и практиката по прилагането им абстрактно е обосновано. Следователно възражението на правителството, че жалбоподателите не могат да твърдят, че са жертва на нарушение на член 8 от Конвенцията, за което се твърди, че е причинено от самото съществуване на закони, позволяващи тайно наблюдение, което беше присъединено към съществото на оплакването (вж. пар. 259 по-горе), трябва да бъде отхвърлено.

* + - 1. Оправдание за намесата
         1. Твърденията на страните

Жалбоподателите

278.  Жалбоподателите изтъкнаха, че законодателството, уреждащо тайното наблюдение, така както се прилага на практика, не предоставя достатъчно гаранции срещу злоупотреби с използването на СРС спрямо което и да е лице в България.

279.  Според тях понятието национална сигурност, както се разбира в България, е твърде неясно и позволява дори легитимна политическа дейност от страна на опозицията да се разглежда като достатъчно основание за наблюдение. Максималната възможна продължителност на първоначалното разрешение в такива случаи – две години – обезсмисля всички останали гаранции. Разпоредбата, която разрешава наблюдение без предварително съдебно разрешение в спешни случаи, също е особено податлива на злоупотреби. Броят на органите, които биха могли да поискат наблюдение извън рамките на висящи наказателни производства, се е увеличил през годините. От своя страна, прокурорът може чрез злоупотреба или произволно да получи разрешение за наблюдение в наказателното производство, като образува такова без достатъчно данни, тъй като наказателното производство не подлежи на контрол от съдилищата на етапа на досъдебното производство или такова образуване не може да ангажира личната отговорност на прокурорите. Сериозността на риска от подобни злоупотреби е илюстрирана от публикацията през февруари 2020 г. по инициатива на главния прокурор на прихванати разговори между президента на републиката, който се ползва с пълен имунитет срещу наказателно преследване, и командира на Военно-въздушните сили.

280.  Много от гаранциите, свързани с процедурата по издаване на разрешение, на практика не са спавани, както е записано в няколко доклада и публикации. Съдилищата често издават разрешения за наблюдение, без да проверят надлежно дали е оправдано това – практика, която е достигнала най - високата си точка в разрешението, по отношение на което председателят на СГС в периода 2011 -15 г. е осъдена наказателно. Съдебният контрол върху съхранението и унищожаването на материалите за наблюдение също е неефективен.

281.  Надзорът от страна на Националното бюро също е неефективен. Повечето от настоящите членове на Бюрото са от службите за сигурност и не притежават необходимата юридическа квалификация. Поради изискването за извършване на проверка на сигурността от Държавната агенция за национална сигурност и изискването да разполагат с разрешение за достъп до класифицирана информация през целия си мандат, членовете на Бюрото могат да загубят длъжностите си в резултат на предприетите от тази агенция стъпки, която е един от органите, които най - често подават искане за наблюдение. Този риск не е само теоретичен, както се вижда от случая с първия заместник - председател на Бюрото. Това се отразява сериозно на независимостта на Бюрото и го маргинализира, особено през последните няколко години. Няколко интервюта и декларации на първия председател на Бюрото подчертават отслабването на неговата роля и на неговия надзор върху органите на прокуратурата и Държавна агенция „Национална сигурност“. Друг проблем е незаконното ограничаване на възможността Бюрото да има достъп до материалите, съхранявани от прокурори. Накрая, Бюрото проверява единствено формалната законосъобразност на наблюдението и уведомява заинтересованите лица само ако са били подложени на него неправомерно. Това обяснява малкия брой уведомления, направени от Бюрото, който е незначителен в сравнение с броя на случаите наосъществено наблюдение.

282.  Специалното средство за защита, иск по член 2, ал. 1, точка 7 от ЗОДОВ, не може да се ползва от юридическите лица и, както е видно от съдебната практика, може да е ефективно само когато Бюрото е уведомило заинтересованите лица за незаконосъобразното наблюдение. В такива производства съдилищата не могат да получат първичните материали и трябва да разчитат на информацията, предоставена от Бюрото.

Правителството

283.  Правителството посочва, че повечето правила, уреждащи използването на специални средства за наблюдение, се съдържат в законодателни актове. Тези актове и съответните подзаконови такива са публикувани. Съществуват и вътрешни правила относно процедурите за съхраняване и унищожаване на материали, получени чрез наблюдение, и получените доказателства. Националното бюро осъществява контрол дали тези правила са в съответствие снормативната уредба.

284.  Освен това законът съдържа изчерпателен списък от престъпления, за които може да се направи искане за използване на СРС. Въпреки че законът предвижда , че скрито наблюдение може да се използва за защита на националната сигурност, в практиката на съдилищата това не е самостоятелно основание за разрешаване на наблюдението; дори когато националната сигурност е основание, разрешение се дава само за предотвратяване или разследване на едно от престъпленията, изброени в закона, което е гаранция срещу злоупотреби с тълкуването на понятието за национална сигурност. Законът също така определя категориите лица, които могат да бъдат подложени на наблюдение, както и основанията и условията, при които и целите, за които може да бъде разрешено и извършено наблюдение.

285.  Прилагането на СРС подлежи на предварително съдебно разрешение, освен в неотложни случаи – изключение, към което властите прибягват пестеливо. Дори в тези случаи наблюдението трябва да бъде потвърдено със задна дата от съдия в рамките на двадесет и четири часа и този съдия може да прецени дали е било оправдано да се прибегне до спешната процедура. За да получи разрешение, съответният орган трябва да подаде мотивирано искане, като при разглеждането на това искане съдията може да изиска всички релевантни материали. Разрешението за използване на СРС трябва да бъде обосновано и съдията проверява дали искането отговаря на всички законови изисквания – включително дали е оправдано да се прибегне до наблюдение – въз основа на всички материали в преписката по делото, а не само на тези, предоставени от запитващия орган. Това е силна защита срещу несериозни или неоснователни искания за наблюдение, основаващи се на измислени обвинения. По закон съдията разполага с до четиридесет и осем часа, за да разгледа молбата, което е достатъчно, за да позволи надлежна преценка. Това е важно за съдилищата, които получават много искания за използване на скрито наблюдение.

286.  Законът ясно определя максималната продължителност, за която може да бъде разрешено наблюдението. Въпреки че максималните законоустановени срокове за наблюдение на основания, свързани с националната сигурност, са дълги – първоначално до две години и не повече от три години – на практика съдилищата никога не издават разрешения за използване на средства за наблюдение за периоди, надвишаващи шест месеца.

287.  Съдиите, които разрешават наблюдението, могат впоследствие да осъществяват надзор на начина, по който то е извършено, тъй като запитващият орган трябва да им докладва и да предостави всички резултати от наблюдението и всички доказателства, които са изготвени на тяхна основа. Съдиите биха могли да изискат и допълнителни материали. Тази форма на текущ контрол допълва извършвания от Националното бюро.

288.  Законовите разпоредби, уреждащи проверката, обработката, съхранението и унищожаването на материалите за наблюдение, са достатъчно точни и се допълват от вътрешни правила, които се преценяват от Националното бюро. Основното положение е, че всички материали, които не се използват за изготвянето на доказателства, трябва да бъдат унищожени бързо, с изключение на материалите, свързани с престъпления срещу националната сигурност, които трябва да се съхраняват в продължение на петнадесет години. Въпреки че правилата, които се различават в зависимост от това дали материалите съдържат класифицирана информация, не са закрепени в един акт, всички те са достатъчно ясни и съдържат достатъчни гаранции срещу злоупотреби.

289.  Що се отнася до Националното бюро, неговите членове се избират от Парламента и се отчитат само пред него. Те трябва да отговарят на строги изисквания и да имат висока професионална квалификация. Дори ако някои от тези членове нямат правно образование или опит, това не означава, че не са подходящо квалифицирани. Вярно е, че при номинирането всички членове трябва да преминат проверка за сигурност от ДАНС, но това е неизбежно, когато става въпрос за чувствителна информация, а всяко отнемане на разрешението за достъп до такава информация подлежи на съдебен контрол. Бюрото разполага с широки правомощия за извършване на инспекции и може да дава указания на съответните органи, което и прави често, включително по отношение на Държавната агенция за национална сигурност. На вниманието на Парламента не бяха представени случаи, които да поставят под съмнение независимостта или почтеността на членовете на Бюрото. Допълнителен надзор на системата е осигурен от парламентарната комисия.

290.  На последно място, както процедурата за уведомяване, така и нейните ограничения са в пълно съответствие с изискванията на Съда. Юридическите лица също могат да получат такова уведомление, както е видно от случай, свързан с мобилна телефонна линия на името набанка, по който Националното бюро е проучвало жалба на ръководството на банката за предполагаемо подслушване на тази линия . Специалното средство за защита – иск по член 2, ал. 1, точка 7 от ЗОДОВ – функционира добре, когато има уведомление от Бюрото, но може да функционира правилно и при липса на такова уведомление, въпреки че досега не е имало такива случаи. Уведомлението не е формално условие за предявяване на иска и всеки може да предяви такъв въз основа на подозрение, че е бил подложен на наблюдение. Ако ищецът не може да представи доказателства за това, съдът, който разглежда случая, би могъл да поиска такива доказателства от съответните органи или да разпореди на Бюрото да разследва случая и да даде информация. Юридическите лица също биха могли да използват това средство за защита и да получат обезщетение за вреди.

* + - * 1. Оценката на Съда

Общи принципи

291.  Общите принципи, уреждащи въпроса кога тайните мерки за наблюдение, включително прихващането на съобщения, могат да бъдат обосновани съгласно член 8, параграф 2 от Конвенцията, са изложени подробно в *Roman Zakharov* (цитирано по-горе, §§ 227-34, 236, 243, 247, 250, 257-58, 275, 278 и 287-88). Много от тези принципи бяха припомнени неотдавна, макар и в малко по-различен контекст – прихващане на голямо количество информация – в *Centrum för rättvisa* (цитирано по-горе, §§ 246 -53) и *Big Brother Watch and Others v. the United Kingdom* ([GC], № 58170/13 и 2 други, §§ 332-39, 25 май 2021 г.).

292.  Тук не е необходимо да се повтарят всички принципи, а само да се подчертае, че общото изискване е, че една система за тайно наблюдение трябва да съдържа ефективни гаранции – особено механизми за преценка и надзор върху системата – които защитават срещу присъщия риск от злоупотреба и които ограничават намесата, присъща за такава система, в правата по член 8 от Конвенцията, до това, което е „необходимо в едно демократично общество“.

293.  В случаи като настоящия, в които жалбоподателите се оплакват в абстрактна форма от системата за тайно наблюдение, а не от конкретни случаи на такова наблюдение, съответните национални закони и практики трябва да бъдат преценени във вида, в който са в момента, в който Съдът разглежда допустимостта на жалбата, а не във вида, в който са били в момента на подаването ѝ (вж. по-горе *Centrum för rättvisa*, § 151 и *Big Brother Watch and Others*, § 270, и двете цитирани по-горе, точка 270). Другият въпрос от особено значение в този случай е, че оценката на това дали разглежданите закони предлагат ефективни гаранции трябва да се основава не само на законите като такива, но и на: а) действителното функциониране на режима на използване на тайно наблюдение и б) наличието или липсата на доказателства за действителна злоупотреба (вж. *Centrum för rättvisa*, § 274, и *Big Brother Watch and Others*, § 360, и двете цитирани по-горе).

Прилагане на тези принципи

294.  В *Асоциация за европейска интеграция и права на човека и Екимджиев* (цитирани по-горе, §§ 79 -84) Съдът разгледа системата за тайно наблюдение в България, действаща към средата на 2007 г. Той установи, че процедурата за разрешаване използването на СРС-та, ако се спазва стриктно, предлага достатъчна защита срещу произволно или безразборно наблюдение. Съдът констатира следните пропуски: а) липса на преглед от независим орган на прилагането на средствата за тайно наблюдение или на това дали получените чрез тези средства материали са унищожени в рамките на сроковете, ако прилагането на средствата се окаже безрезултатно; б) липса на достатъчно гаранции по отношение на наблюдение на основание национална сигурност и извън контекста на наказателното производство; в) липса на правила, определящи с подходяща степен на точност начина на проверка на материалите за наблюдение или процедурите за запазване на тяхната цялост и поверителност и процедурите за тяхното унищожаване; г) липса на независим орган, наблюдаващ функционирането на системата за тайно наблюдение; д) липса на независим контрол върху използването на материалите, попадащи извън обхвата на първоначалното искане за използване на разузнавателни средства; и е) липса на уведомяване на засегнатите лица при каквито и да било обстоятелства (пак там, § 85 -91). Въз основа на това Съдът заключи, че българското право не предоставя достатъчно гаранции срещу риска от злоупотреба, присъщ на всяка система за тайно наблюдение (пак там, § 93).

295.  От постановяването на това решение, а отчасти изглежда и в резултат на него, българското законодателство, уреждащо тайното наблюдение, се е развило значително. Същевременно Комитетът на министрите все още не е приел окончателна резолюция, в която да заключи, че неговите функции, свързани с надзора върху изпълнението на това решение, са изпълнени; той е набелязал няколко нерешени въпроса във връзка с общите мерки, предприети от българските органи за изпълнение на това решение (вж. пар. 228 и 229 по-горе). От своя страна, Съдът трябва, както вече беше отбелязано, да провери не дали българските органи са изпълнили това решение, а дали съответното българско право, в сегашния му вид, отговаря на изискванията на член 8 от Конвенцията (вж. пар. 257 по-горе).

Достъпност на закона

296.  Всички законови разпоредби, уреждащи тайното наблюдение в България, както и вътрешните правила на Националното бюро за контрол върху специалните разузнавателни средства (вж. пар. 13 по-горе), са публикувани официално и по този начин са достъпни за обществеността. За разлика от тях вътрешните правила за съхранение и унищожаване, споменати от правителството (вж. точки 283 и 288 по-горе), изглежда не са достъпни за обществеността.

297.  От своя страна, инструкцията на главния прокурор, уреждаща умишленото или случайно използване на специални разузнавателни средства по отношение на адвокатите, макар и да не е публикувано от властите, е публикувано в бюлетина на Висшия адвокатски съвет (вж. пар. 27 -30 по-горе). Може да се приеме, че това го прави достатъчно достъпен за лицата, за които се отнася – практикуващи юристи като първия и третия жалбоподател и организации, специализирани в правни въпроси, като втория и четвъртия жалбоподатели (вж. *mutatis mutandis*, *Groppera Radio AG and Others v. Switzerland*, 28 March 1990, § 68, Series A no. 173, и *Autronic AG v. Switzerland*, 22 May 1990, § 57, Series A no. 178).

Основания, на които може да се прибегне до тайно наблюдение, и лица, които могат да бъдат поставени под наблюдение

298.  Основният въпрос във връзка с основанията, на които може да се прибегне до тайно наблюдение, и лицата, които могат да бъдат поставени под наблюдение, е дали законът, разрешаващ или уреждащ разрешението за използване на тайно наблюдение, определя с достатъчна яснота а) вида престъпленията и други основания, които могат да доведат до тайно наблюдение, и б) категориите лица, които могат да бъдат поставени под тайно наблюдение.

299.  В България законът определя изчерпателно тежките умишлени престъпления, които могат да са предпоставка за използването на специални разузнавателни средства (вж. пар. 18 по-горе). Освен това в него се уточнява, че такива средства могат да се използват само ако има основания да се подозира, че такова престъпление се планира, извършва се или е извършено и само ако е малко вероятно други методи за разкриване или разследване да са успешни (вж. пар. 18 и 20 по-горе). Така законът е достатъчно ясен по този въпрос (вж. по-горе, § 244, *Роман Захаров*). Всъщност е по - ясно, отколкото когато Съдът за първи път го разгледа и го намери за адекватен в това отношение в *Асоциацията за европейска интеграция и права на човека и Екимджиев* (цитирани по-горе, §§ 10 и 79). Въпреки че видовете престъпления, попадащи в този списък, са различни, изглежда, че на практика в по - голямата част от случаите органите прибягват до наблюдение във връзка с престъпленията а) ръководене на или членство в престъпна група и б) търговия с наркотични вещества (вж. таблицата в пар. 19 по-горе).

300.  Вярно е, че законът гласи, че специалните разузнавателни средства могат да се използват и за „дейности, свързани с националната сигурност“ (вж. пар. 22 по-горе). При липсата на по - подробна информация относно практиката на съответните български съдилища и органи по този въпрос е трудно да се провери дали, както твърди правителството (вж. пар. 22 по-горе), националната сигурност никога не може да бъде самостоятелно основание за разрешаване на тайно наблюдение в България. Законовото изискване всяко искане за използване на специални разузнавателни средства да съдържа пълна информация за обстоятелствата, които дават основание да се подозира, че се подготвя, извършва или е извършено съответно престъпление, включително когато става въпрос за национална сигурност (вж. пар. 39 по-горе), и формулировката на разпоредбата, която определя срока за използване на специални средства за наблюдение за защита на националната сигурност, която изглежда свързва това с предотвратяването на престъпления срещу Републиката (вж. пар. 79, буква б) по-горе), изглежда подкрепят твърдението на правителството. Не е ясно обаче как тези разпоредби се прилагат на практика. Липсата на яснота по този въпрос вече беше констатирана от Комитета на министрите в контекста на контрола върху изпълнението на *Асоциация за европейска интеграция и права на човека и Екимджиев* (цитирано по-горе) (вж. пар. 229, буква а) по-горе).

301.  Но дори и да се приеме, че по българското законодателство защитата на националната сигурност може да бъде самостоятелно основание за тайно наблюдение, това само по себе си не противоречи на член 8 от Конвенцията (вж. *Асоциация за европейска интеграция и права на човека и* Екимджиев, § 84; *Centrum för* rättvisa, § 261; и *Big Brother Watch and Others*, § 347, всички цитирани по-горе). Това, което има значение по-скоро, е възможността всички потенциални злоупотреби, произтичащи от присъщото неясно значение и контури на понятието за национална сигурност, да могат да бъдат проверени. Във връзка с това трябва да се отбележи, че дори когато става въпрос за националната сигурност, съответните органи трябва да потърсят съдебно разрешение за прилагане на СРС, тъй като то може да ограничи тяхната свобода на преценка при тълкуването на това понятие и да гарантира наличието на достатъчно основания за поставяне на някого под наблюдение във всеки един случай (вж. по-горе, пар. 249). Това е важна предпазна мярка срещу произвола и злоупотребите. Нейната ефективност е анализирана в пар. 307 -322 по - долу.

302.  Законът също така определя изчерпателно категориите лица или предмети, които могат да бъдат поставени под наблюдение. Когато става въпрос за наблюдение, свързано с престъпления, съответните категории са ясно определени: това са или лица, за които се подозира, че са извършили престъпления, лица, които без да знаят са били използвани за тяхната подготовка или извършване, лица, които са се съгласили да бъдат наблюдавани за своя собствена защита или сътрудничат като свидетели в случаи, свързани с ограничен кръгтежки умишлени престъпления, както и предмети, които могат да доведат до идентифицирането на такива лица, ако самоличността им е неизвестна (вж. пар. 23, букви а), в), г) и д) по-горе). Вярно е, че когато става въпрос за наблюдение по съображения за национална сигурност, законът е формулиран с по - неясни термини: „лица или предмети, свързани с националната сигурност“ (вж. пар. 23, буква б) по-горе). Но съображенията в пар. 301 по-горе относно възможността за проверка на потенциални злоупотреби, произтичащи от неяснотата на понятието за национална сигурност, са също толкова важни тук.

303.  Възниква обаче проблем с липсата на достатъчна прецизност относно значението на термина „обекти“ в член 12, ал. 1 от ЗСРС (вж. пар. 23, букви б) и в) по-горе). Законът не изяснява дали „обектите “, които могат да бъдат поставени под наблюдение – или защото са свързани с националната сигурност, или защото са необходими за идентифициране на лица, които трябва да бъдат поставени под наблюдение – трябва да бъдат конкретни (например конкретни помещения, конкретно превозно средство или конкретна телефонна линия). В тази връзка трябва да се отбележи, че режимът на тайно наблюдение в България е предназначен да бъде по - скоро целенасочен режим, отколкото режим за масово прихващане на информация (bulk interception) (сравнете го с *Роман Захаров*, цитиран по-горе, § 265). Макар и краен пример, случаят с *Mustafa Sezgin Tanrıkulu* (цитиран по-горе, §§ 51 -60) илюстрира риска от неправилно тълкуване на неясни правни разпоредби, които по принцип позволяват само целенасочено наблюдение, така че да се стигне до широкомащабно наблюдение. Фактите, които са в основата на наказателната присъда на председателя на СГС от 2016 г., сочат в подобна посока (вж. пар. 56 по-горе). През 2014 г. тя е разрешила наблюдението на автоматизирана полицейска информационна система (която със сигурност е съдържала данни за много лица), очевидно считайки, че тази система е „обект“ по смисъла на член 12, ал. 1 от ЗСРС. След това е обвинена в издаване на разрешение за наблюдение на „обект “, който не попада в законоустановеното определение, но съдилищата я оправдават по това обвинение и я признават за виновна единствено по отношение на срока на издаденото разрешение,. Въпреки че в резултат на това, че съответните решения не са публични, мотивите им не са известни, има основание да се предполага, че българските съдилища не са склонни да тълкуват понятието „обекти“ в член 12, ал. 1 от ЗСРСтвърде разширително.

304.  С оглед на тези съображения може да се каже, че българското законодателство отговаря на изискванията на член 8 от Конвенцията по отношение на основанията, на които може да се прибегне до тайно наблюдение и на лицата, които могат да бъдат поставени под наблюдение, с изключение на липсата на по-ясна дефиниция на понятието „обекти“ в член 12, ал. 1 от ЗСРС (вж. пар. 23, букви б) и в) по-горе).

Срок на мерките за прилагане на СРС

305.  Българското законодателство ясно определя първоначалната и максималната продължителност на мерките за тайно наблюдение (вж. пар. 79 по-горе). Също така е ясно, че наблюдение след първоначално разрешения срок е възможно само ако е разрешено от компетентния съдия, на който трябва да бъде предоставена не само същата информация като изискваната за първоначалното разрешение, но и пълна информация за всички получени до момента резултати от наблюдението (вж. пар. 42 по-горе). Накрая, законът определя обстоятелствата, при които наблюдението трябва да бъде прекратено (вж. пар. 82 по-горе). Съществува все пак една област, която поражда безпокойство, и това е потенциалната продължителност на първоначалното разрешение за използване на СРС на основания, свързани с националната сигурност, която е до две години (вж. пар. 79, буква б) по-горе). Самата продължителност на този период, съчетана с присъщите неясни граници на понятието за национална сигурност, значително отслабва съдебния контрол, на който трябва да бъде подложено това наблюдение. Този въпрос вече е отбелязан от Комитета на министрите в контекста на контрола върху изпълнението на решението *Асоциация за европейска интеграция и права на човека и Екимджиев* (цитирано по-горе) (вж. пар. 229, буква в) по-горе). Дори ако, както твърди правителството (вж. пар. 286 по-горе), на практика съдилищата никога не издават такива заповеди за срок, по - дълъг от шест месеца, това разрешение не се основава на дефинирано в закона ограничение.

Процедури за издаване на разрешение

306.  Релевантните фактори в тази рубрика са: а) статутът на органа, който може да разреши тайно наблюдение, и б) начинът, по който този орган разглежда исканията за използване на СРС и издава разрешение за използване на СРС.

Стандартна процедура

307.  Когато през 2007 г. Съдът разглежда производството по издаване на разрешение за използване на СРС съгласно ЗСРС, Съдът установява, че ако се спазва стриктно, тази процедура предоставя съществени гаранции срещу произволно или безразборно наблюдение (вж. цитираното по-горе решение по дело *Асоциация за европейска интеграция и права на човека и* *Екимджиев*, посочено по-горе, пар. 84). Оттогава прецизността на съответните разпоредби се повишава (сравнете пар. 32 - 51 и 70 - 88 по-горе с *Асоциация за европейска интеграция и права на човека и Екимджиев*, цитирано по-горе, §§ 12 -17). Тези процедури обаче трябва да се разглеждат не само на хартия, но и на практика, доколкото това може да се установи въз основа на надеждни официални източници (в сравнение с цитираните по-горе решение по дело *Roman* *Zakharov*, посочено по-горе, точка 263 и 265).

308.  Съответното законодателство в България определя солидни гаранции, които имат за цел да гарантират, че до тайно наблюдение се прибягва само когато това е наистина оправдано. На първо място, само ограничен брой органи могат да поискат разрешение за прилагане на СРС в рамките на съответните си компетенции (вж. пар. 32-36 по-горе). Второ, изглежда, че законът предвижда форма на вътрешен контрол, предхождащ подаването на искания: тези, направени от изпълнителните органи, трябва да произхождат от ръководителя на съответния орган, а прокурорите, които възнамеряват да подадат такива искания, трябва да уведомят ръководителите си по йерархията (вж. пар. 37 по-горе). Трето и най - важно, наблюдението може да бъде разрешено само от председателя на компетентния съд или от изрично упълномощен негов заместник (вж. пар. 46 и 47 по-горе). На последно място, органът, който прилага СРС, трябва, преди да пристъпи към това, да разгледа внимателно искането за несъвместимост *ratione materiae* или явни грешки и, ако забележи проблеми в това отношение, да го върне на съдията, който е разрешил използването за преразглеждане (вж. пар. 73 по-горе).

309.  По закон исканията за използване на СРС трябва да бъдат надлежно обосновани и да посочват както основанията за исканото наблюдение, така и предвидените параметри (вж. пар. 39, 40 и 41 по-горе). Искането трябва по - специално да се отнася до а) обстоятелствата, даващи основание да се подозира, че се подготвя или извършва престъпление или е извършено такова (включително по отношение на националната сигурност), б) да посочва (освен по отношение на престъпления, свързани с тероризъм) вече предприетите действия по разследване и резултатите от предишни проверки или разследвания, в) да обяснява (освен по отношение на престъпления, свързани с тероризъм) защо търсената информация не може да бъде получена чрез други средства или защо такива други средства биха довели до изключителни трудности, и г) да обосновава (освен по отношение на престъпления, свързани с тероризъм) необходимостта от исканата продължителност на наблюдението (вж. пар. 39, букви а), б), г) и е), пар. 40, букви а), б), д) и е) и пар. 41, буква а) по-горе). Всички материали, на които се основава молбата, трябва или да бъдат приложени към нея от самото начало (за молби, подадени извън наказателното производство), или да бъдат предоставени на разположение на компетентния съдия при поискване (за молби, подадени в хода на наказателното производство) (вж. пар. 44 по-горе). При разглеждането на искането съдията трябва да провери дали са налице всички правни предпоставки и да се произнесе с мотивирано решение (вж. пар. 51 по-горе). Един от възможните недостатъци на този етап е, че макар производството по издаване на разрешение да трябва по необходимост да се води без уведомяване на лицата, които ще бъдат поставени под наблюдение, заявителят не е длъжен да разкрива пред съдията изцяло и откровено всички въпроси, свързани с основателността на неговото искане, включително такива въпроси, които могат да отслабят неговото искане.

310.  Въпреки този последен потенциален недостатък, заключението на Съда в *Асоциацията за европейска интеграция и права на човека и* *Екимджиев* (цитирано по-горе, § 84), че ако се спазва стриктно, процедурата в България по издаване на разрешение осигурява съществени гаранции срещу произволно или безразборно наблюдение, може само да бъде потвърдено. Но също така трябва да се провери дали тези гаранции се прилагат правилно на практика.

311.  Двете съдилища в България, които са издали най - голям брой разрешения за използване на СРС през последното десетилетие, са Софийският градски съд (до 2015 г.) и Специализираният наказателен съд (от 2015 г.) (вж. таблицата в пар. 49 по-горе). Според официален доклад, публикуван в началото на 2017 г., до април 2015 г. съдиите в Софийския градски съд, издаващи разрешения за наблюдение, не са посочвали мотиви за издаване на разрешения, а през април - август 2015 г. са посочили, с малки изключения, само „бланкетни и общи“ мотиви (вж. пар. 59, букви з) и и) по-горе). Това се потвърждава от двете разрешения за наблюдение от 2012 г. и 2013 г., издадени от този съд и представени от жалбоподателите (вж. пар. 61 по-горе). Вярно е, че след скандала, който избухва през 2015 г. във връзка с начина, по който Софийският градски съд обработваше исканията за наблюдение (и който по - късно доведе до уволнението и присъдата на неговия председател), компетентните съдии от този съд започнаха систематично да излагат мотивите за решенията си за предоставяне на разрешение за използване на СРС (вж. пар. 56, 57 и 60 по-горе). Същевременно обаче броят на исканията за наблюдение, адресирани до този съд, рязко намаля и най -голям брой такива молби се подават в Специализирания наказателен съд (вж. таблицата по точка 49 по-горе). Действително, от 2018 г. Специализираният наказателен съд издава приблизително половината от всички разрешения за използване на СРС в България (пак там).

312.  Както е видно от две неотдавнашни решения на Специализирания наказателен съд, около тридесет разрешения за наблюдение, издадени от неговия председател и заместник - председатели, са имали бланкетно съдържание, били са формулирани по най-общ начин така че да могат да се отнасят до всяко възможно искане за наблюдение, и не са имали никакво позоваване на конкретния случай, за който са се отнасяли, с изключение на номера на искането (вж. пар. 64 и 65 по-горе). Няма причина да се смята, че тези разрешения са по някакъв начин изключителни и представляват нещо различно от обичайната практика в този съд.

313.  Следователно може да се направи изводът, че повечето разрешения за използване на СРС в България през последното десетилетие не съдържат подходящи мотиви. Това е от особено значение, тъй като съответното предоставяне на мотиви е жизненоважна гаранция срещу злоупотреби с използването на СРС (вж. Dragojević *срещу Хърватия*, № 68955/11, §§ 88 -101, 15 януари 2015 г.; Dudchenko *срещу Русия*, № 37717/05, § 97 -98, 7 ноември 2017 г.; и Liblik *and Others срещу Естония*, №. 173/15 и 5 други, §§ 137-41, 28 май 2019 г.). Това е така, защото предоставянето на мотиви, дори и кратки, е единственият начин да се гарантира, че съдията, разглеждащ искането за използване на СРС, е прегледал надлежно искането и материалите, които го подкрепят, и наистина е насочил вниманието си към въпросите дали наблюдението би представлявало оправдана и пропорционална намеса в правата по член 8 на лицето(ата), срещу което (които) ще бъде насочено, и на всяко (всички) лице(а), което (които) има вероятност да бъде (ат) засегнато (и) от това. В България това е особено важно с оглед на твърдението на жалбоподателите, което изглежда потвърдено, наред с другото от някои неотдавнашни развития (вж. пар. 67 по-горе), че наказателното производство може да бъде образувано произволно и повърхностно, най-вече с цел да се даде възможност за поставяне на някого под наблюдение поради скрити мотиви (вж. пар. 279 по-горе). Както е видно от организацията в СГС от август 2015 г., предоставянето на мотиви, независимо дали е разрешено или отказано разрешение за използване на СРС, е постижимо на практика въпреки сравнително кратките срокове за произнасяне по такива молби (вж. пар. 60 по-горе).

314.  Вярно е, че както е отбелязано в двете горепосочени решения на Специализирания наказателен съд (вж. пар. 64 и 65 по-горе), липсата на мотиви не може автоматично да доведе до заключението, че съдиите, издаващи разрешения за използване на СРС, не са разгледали надлежно исканията. Но три фактора пораждат сериозни опасения в това отношение.

315.  Първият такъв фактор е голямата натовареност, произтичаща от подобни искания, които по закон могат да бъдат разглеждани само от председателите или заместник -‑председателите на съответните съдилища. Националното бюро многократно е обръщало внимание на недостатъчния персонал и ресурси, с които разполага Специализираният наказателен съд, за да обработи правилно всички искания за наблюдение, подадени до неговия председател и заместник - председатели (вж. пар. 50 по-горе). Самият Специализирани наказателен съд обърна внимание на нарастващото натоварване, произтичащо от големия обем искания за използване на СРС, подадени до него (вж. пар. 62 и 63 по-горе), и въпросът вече беше повдигнат от Комитета на министрите в контекста на контрола върху изпълнението на решението *Асоциация за европейска интеграция и права на човека и* *Екимджиев* (цитиран по-горе) (вж. пар. 229, буква б) по-горе).

316.  Вторият фактор е високият процент уважени искания за използване на СРС (вж. таблицата в пар. 55 по-горе).

317.  Третият фактор е изричната позиция на Апелативния специализиран наказателен съд – който има пряка надзорна компетентност над Специализирания наказателен съд – че съдия, който разглежда искане за използване на СРС, трябва само да провери дали са изпълнени формалните изисквания за уважаването му, без да разглежда материалите в подкрепа на заявлението (вж. пар. 66 по-горе).

318.  Всичко изброено по-горе не може да бъде отхвърлено като обикновена техническа подробност, която не отразява функционирането на практика на системата за тайно наблюдение в България. Съществуват доказателства, които показват, че начинът, по който компетентните съдии разглеждат исканията за използване на СРС, е довел до действителни случаи на неоправдано наблюдение.

319.  Първо, председателят на Софийския градски съд е освободена от длъжност във връзка с начина, по който е организирала разглеждането на такива искания в този съд по времето, когато именно този съд в България е издавал най -голям брой разрешения за наблюдение (вж. пар. 57 по-горе). Тя също така е осъдена за умишлено издаване на разрешение за наблюдение в нарушение на законовите изисквания (вж. пар. 56 по-горе). Въпреки че не са повдигнати такива обвинения срещу други съдии от Софийския градски съд, има доказателства, че проблемът е бил далеч по - общ (вж. пар. 58 и 59, букви в), г), д), е) и ж) по-горе).

320.  Що се отнася до Специализирания наказателен съд, заслужава да се отбележи, че през юли 2021 г. българският парламент създаде *ad hoc* комисия, която да разследва евентуално незаконното и необосновано използване на специални средства за наблюдение по отношение на опозиционни политици, журналисти и стотици участници в антиправителствените протести в България през 2020 г., въз основа на издадени от този съд разрешения. Въпреки че докладът на тази комисия, който беше финализиран през септември 2021 г., все още не е публично достъпен, изявленията на министъра на вътрешните работи, направени в Парламента по времето, когато комисията е създадена, вече показват, че проблемът с липсата на подходящ съдебен контрол е засегнал сериозно операциите по наблюдение, разрешени от Специализирания наказателен съд (вж. пар. 67 по-горе).

321.  От това следва, че Съдът не може да се увери, че процедурите за разрешаване на тайно наблюдение, както се прилагат на практика в България, ефективно гарантират, че такова наблюдение се разрешава само когато е действително необходимо и пропорционално във всеки отделен случай (сравни с цитираните по-горе *Роман Захаров*, §§ 262 -63).

322.  Допълнителният контрол, извършван от органите по прилагане след предоставянето на съдебно разрешение (вж. пар. 73 по-горе), не може да поправи липсата на подходящ съдебен контрол по две причини. Първо, проверката е ограничена до несъвместимост *ratione materiae* или очевидни грешки (пак там). На второ място, случаите, в които тази допълнителна защита е задействана, очевидно са изключително редки (вж. пар. 75 по-горе).

Неотложна процедура

323.  От друга страна, не изглежда да възниква отделен въпрос по отношение на спешната процедура, при която специални разузнавателни средства могат да бъдат използвани без предварително съдебно разрешение, ако съществува непосредствен риск от извършване на тежко умишлено престъпление или риск от непосредствена заплаха за националната сигурност (вж. пар. 77 по-горе). Когато органите прибягват до тази неотложна процедура, съответният съдия трябва в срок от двадесет и четири часа да оцени и одобри със задна дата необходимостта от това; в противен случай операцията по прилагане на СРС трябва да спре. Съдията не е длъжен само да преразгледа необходимостта от продължаване на наблюдението, но също така трябва да потвърди вече проведеното наблюдение, както и резултатите от него (за разлика от *Роман Захаров*, цитиран по-горе, § 266, и *Константин Москалев срещу Русия*, № 59589/10, § 51 -52, 7 ноември 2017 г.). Освен това тази процедура е била използвана само в няколко случая, а през 2018 -20 г. тези случаи дори са намалели до незначителен процент (вж. пар. 78 по-горе).

Процедури за съхраняване, достъп, прегледизползване, съобщаване и унищожаване на данни от наблюдението

По принцип

324.  В *Асоциация за европейска интеграция и права на човека и* *Екимджиев* (цитирано по-горе, § 86) Съдът констатира, че изглежда е налице липса на нормативна уредба, определяща с подходяща степен на точност начина на проверка на информацията, получена чрез тайно наблюдение, или процедурите за запазване на нейната цялост и конфиденциалност и нейното унищожаване.

325.  ЗСРС и Наказателно - процесуалният кодекс оттогава са изменени и сега съдържат разпоредби, които се отнасят до различни аспекти на тези въпроси. В няколко области обаче има празноти.

326.  На първо място, макар тези разпоредби да уточняват начина, по който информацията от „първичния запис“ се възпроизвежда в „производен носител на данни“, а след това и във всички доказателствени материали (вж. пар. 87 -91 по-горе), те не казват нищо за начина, по който „първичният запис“ и „производният носител на данни“ се съхраняват. Те също така не уточняват по никакъв начин длъжностните лица в рамките на съответните органи, които имат право на достъп до тях, както и не предвиждат никакви гаранции за целостта и поверителността на тези материали. Във връзка с това следва да се отбележи, че след отмяната през август 2013 г. на част II, точка 8 от Приложение № 1 към Закона за защита на класифицираната информация от 2002 г. информацията, получена чрез използване на специални разузнавателни средства, вече не е класифицирана (вж. пар. 102 по-горе). Следователно тя очевидно не е предмет на правилата, уреждащи защитата на такава информация – въпреки че Агенцията за технически операции твърди, че въпреки изменението както „първичният запис“, получен в резултат на надзора, така и „производният носител на данни“ са останали класифицирана информация (вж. пар. 104 по-горе). Както е отбелязано в точка 296 по-горе, вътрешните правила, на които се позовава правителството (вж. пар. 283 и 288 по-горе), не са публикувани. Тези правила не бяха представени в настоящото производство (сравнете с *Big Brother Watch и други*, цитирани по-горе, § 423).

327.  Освен това, освен общото правило, че съдържанието на „производния носител на данни“ трябва напълно да съответства на това на „първичния запис“ (вж. пар. 89 по-горе), не съществуват публично достъпни правила относно начина, по който „първичният запис“ и „производният носител на данни“ трябва да бъдат проучени: как органите трябва да пресеят информацията в тях и да решат кои части са от значение и трябва да се съхраняват и използват като доказателство, и кои не са от значение и трябва да се унищожат. Въпреки че в правилата, уреждащи възможното използване на материали, получени в резултат на тайно наблюдение, се посочва, че такива материали, включително излишната информация, могат да бъдат използвани само за предотвратяване, разкриване или доказване на тежки умишлени престъпления или за защита на националната сигурност (вж. пар. 18, 84, 100 и 101 по-горе), не е ясно как на практика е гарантирано спазването на това ограничение.

328.  Правилата, уреждащи унищожаването на „първичния запис“ и „производният носител на данни“, изглеждат достатъчно ясни, въпреки че съществува несъответствие между позицията по отношение на материалите, получени в резултат на наблюдение извън рамките на вече висящо наказателно производство, и позицията по отношение на материалите, получени в хода на наказателното производство. Законът предвижда автоматично унищожаване и последващ доклад до съдията, който е разрешил наблюдението в първия случай, и представяне на доклад до този съдия и унищожаване по негово разпореждане във втория случай (вж. пар. 94 -99 по-горе).

329.  Няма обаче специални правила за съхранението или унищожаването на получения доказателствен материал. Във всеки случай се създават най-малко две копия на този доказателствен материал (които изглежда се състоят от компютърни файлове, съдържащи аудио - или видеозаписи – вж. пар. 90 по-горе) и от придружаващите ги писмени записи (вж. пар. 91 по-горе). Първото копие се изпраща на съдията, издал разрешението за използване на СРС (пак там). Второто копие се съхранява първо от органа, направил искането, и след това, ако във връзка с него е образувано наказателно производство, то се прехвърля в делото– първо в преписката по досъдебното производство, а след това в делото пред наказателния съд (вж. пар. 92 по-горе). Изглежда, че и двете копия се съхраняват и унищожават заедно с делата, от които са част. Не може да се приеме, че това осигурява подходящо ниво на защита на информация, която може да засяга интимни аспекти от личния живот на някого или по друг начин да позволи непропорционална намеса в личния живот на засегнатите лица или в „кореспонденцията“ на съответните юридически лица. Случаят, при който не е образувано наказателно производство, също поражда много неясноти.

330.  Не съществуват и публично достъпни правила, уреждащи съхранението на информация, получена чрез наблюдение по съображения за национална сигурност, които трябва да се съхраняват от съответния орган, направил искането, в продължение на петнадесет години след приключване на наблюдението (вж. пар. 98 по-горе).

331.  Правителството не твърди, че всички или някои от горепосочените пропуски са били преодолени от разпоредбите, добавени през 2019 г. към Закона за защита на личните данни г. при транспониране на Директива (ЕС) 2016/680 (вж. пар. 219 по-горе) и не е ясно дали компетентните органи прилагат тези правила за защита на данните при обработването на информация, получена в резултат на тайно наблюдение. Освен това тези правила не могат да осигурят защита по отношение на информацията, свързана с юридическите лица (вж. пар. 216 и 239 по-горе).

332.  Очевидната липса на ясно регулиране във всички тези области и на подходящи гаранции дава възможност с информацията, получена в резултат на тайно наблюдение, да бъде злоупотребявано за цели, които нямат общо със законоустановената цел.

По отношение на използване на СРС, които засягат адвокатската тайна

333.  Друг въпрос в това отношение възниква от липсата на правни разпоредби, определящи с подходяща степен на точност съдбата на информацията, получена в резултат на тайно наблюдение, която може да е засегнала материали, които подлежат на опазване като професионална тайна. Може да се постави под въпрос дали инструкцията на главния прокурор по този въпрос, която е изцяло вътрешен акт, издаден по силата на неговото правомощие да дава указания, уреждащи работата на прокуратурата (вж. пар. 27 по-горе), може да се разглежда като „закон“ за целите на член 8, параграф 2 от Конвенцията (вж. *mutatis mutandis*, *Silver and Others v. the United Kingdom*, 25 март 1983 г., § 86, серия A № 61; *Malone v. the United Kingdom*, 2 август 1984 г., §§ 68 и 79, серия A № 82 и *Amann v. Switzerland* [GC], № 27798/95, § 75, ECHR 2000-II). Освен това е съмнително дали тази инструкция предвижда достатъчни гаранции по отношение на тайното наблюдение, насочено срещу адвокат, тъй като за неговото използване тя изисквасамо наличие на основателно подозрение, че те са извършили престъпление (вж. пар. 28 по-горе), което по принцип е изискване за цялото наблюдение, а не само за това, насочено срещу адвокат (вж. точки 39 и 54 по-горе). Инструкцията изглежда също така противоречи на изричните изисквания на член 33, ал. 1, 2 и 3 от Закона за адвокатурата от 2004 г., според които всички адвокатски книжа и съобщения, независимо от формата им, са неприкосновени без изключение (вж. пар. 26 по-горе). В инструкцията също така не са предвидени достатъчно гаранции по отношение на материалите, получени в резултат на случайно прихванати съобщения между адвокат и клиент (вж. *mutatis mutandis*, *R.E. срещу Обединеното кралство*, № 62498/11, § 138 -41, 27 октомври 2015 г. и Dudchenko *срещу Русия*, № 37717/05, § 107, 7 ноември 2017 г.). Единствената разпоредба, която се занимава с въпроса, точка 13, просто казва, че ако органите прихванат разговора на адвокат с клиент или с друг адвокат и този разговор засяга защитата на клиента, те не трябва да изготвят доказателствени материали въз основа на него, освен ако наблюдението не разкрие, че самият адвокат е въвлечен в престъпна дейност (вж. пар. 29 по-горе). Това оставя открит въпроса как точно трябва да бъдат унищожени такива материали, както изрично изисква член 33, ал. 3 от Закона за адвокатурата от 2004 г. (вж. пар. 26 по-горе). Изглежда също така, че инструкцията не обхваща всички видове комуникации между адвокат и клиент: по силата на тази инструкция точка 13 от инструкцията се прилага единствено за съобщения, свързани със защитата на клиента, което предполага вече висящи съдебни спорове, а може би и само наказателни производства.

Наблюдение на системата

334.  Релевантните фактори за вземане на решение дали мерките за контрол върху системата са адекватни са: а) независимостта на надзорните органи, техните компетенции и техните правомощия (както за достъп до материали, така и за отстраняване на нарушения, по - специално с цел унищожаване на материали от проведено наблюдение) и б) възможността за ефективен публичен контрол върху работата на тези органи.

335.  В България три органа могат да упражняват надзор върху използването на специални разузнавателни средства: а) съдията, издал съответното разрешение за наблюдение; б) националното бюро; и в) специална парламентарна комисия (вж. пар. 106 -135 по-горе).

336.  Тази прецизност на система се различава съществено от уредбата, критикувана от Съда в *Асоциация за европейска интеграция и права на човека и Екимджиев (*цитирани по-горе, §§ 87 -88). Въпреки това тази уредба не отговаря на съответните стандарти за ефективност в няколко отношения.

337.  Съдията, издал разрешението за наблюдение, не е в състояние да осигури ефективен надзор. Вярно е, че той трябва да бъде информиран за приключването на съответната дейност по наблюдение (вж. пар. 105 и 107 по-горе, и за разлика от *Роман Захаров*, цитиран по-горе, точка 274) и да му бъде предоставен доклад за това (вж. пар. 106 по-горе). Но във всички случаи на наблюдение извън вече висящото наказателно производство този съдия няма правомощия да разпорежда мерки за обезвреда, като например унищожаването на материалите от наблюдението. По - важното е, че той не е оправомощен или не се очаква да извършва проверки на място и изпълнява контролните си правомощия единствено въз основа на доклада, представен от органите. Освен това, с оглед на голямата натовареност на съответните съдии (вж. пар. 315 по-горе), може да се постави под съмнение дали този контрол би могъл да бъде ефективен на практика. Накратко, макар и ценна гаранция, този механизъм е недостатъчен, за да гарантира, че не се злоупотребява с правомощията за наблюдение.

338.  От своя страна, основният надзорен орган, Националното бюро, страда от редица недостатъци, подкопаващи неговата ефективност на практика.

339.  Първо, няма гаранция, че всички негови членове са достатъчно независими по отношение на органите, които трябва да контролират. По закон лицата с професионален опит в правоприлагащите органи или службите за сигурност могат да станат членове на Националното бюро (вж. пар. 109 по-горе). След изтичане на петгодишния им мандат (който, ако бъде предоставен, може да бъде подновен), те имат право да заемат предишните длъжности (вж. пар. 111 по-горе). Този потенциален механизъм „въртяща се врата“ може да породи опасения относно практическата независимост на тези членове на Бюрото и относно възможните конфликти на интереси от тяхна страна (вж. *mutatis mutandis*, *Centrum för rättvisa*, посочено по-горе, § 359). Действително настоящият председател на Бюрото идва директно от Държавната агенция за национална сигурност, а заместник - председателят, който беше избран през 2018 г. и подаде оставка в средата на 2021 г. (след като беше поставен под санкции от властите в Съединените американски щати поради сериозни обвинения в корупция), е заемал длъжности в службите за сигурност в продължение на повече от две десетилетия и половина, преди да се присъедини към Бюрото (вж. пар. 112 и 115 по-горе).

340.  Друг аспект на организацията на Националното бюро поражда допълнителни опасения в това отношение. Преди да бъдат назначени на своите длъжности, членовете на Бюрото трябва да бъдат подложени на проверка за сигурност от страна на един от органите, чиято дейност Бюрото контролира – Държавната агенция за национална сигурност (вж. пар. 109 и 110 по-горе). Това създава очевиден конфликт на интереси за тази агенция. Ако Агенцията по-късно отмени разрешението за достъп до класифицирана информация на членовете на Бюрото, те трябва да бъдат отстранени от длъжността, тъй като автоматично престават да отговарят на условията за заемането ѝ; това вече се случи веднъж през 2017 - 2018 г. (вж. пар. 111, буква в) и точка 114 по-горе). Въпреки че решението на ДАНС за отмяна на разрешение за достъп подлежи на съдебен контрол, възможността тя да оказва влияние върху състава на Бюрото може да засегне независимостта на Бюрото и обективността и задълбочеността на неговата надзорна работа, особено по отношение на тази агенция.

341.  Въпросът за независимостта на Националното бюро по отношение на органите, които то контролира, вече беше подчертан от Комитета на министрите на Съвета на Европа в контекста на неговия надзор върху изпълнението на *Асоциация за европейска интеграция и права на човека и* *Екимджиев* (цитиран по-горе) (вж. пар. 229, буква д) по-горе).

342.  Второ, възникват опасения относно квалификацията на някои от членовете на Националното бюро. Само един от настоящите петима членове има образование по право и опит (вж. пар. 112 по-горе и обратното в *Big Brother Watch и други*, цитирани по-горе, § 407). Този въпрос беше отбелязан и от Комитета на министрите (вж. пар. 229, буква д) по-горе).

343.  Трето, не изглежда, че при извършването на проверки на място членовете на Националното бюро и неговите служители могат да имат неограничен достъп до всички релевантни материали, съхранявани от органите на прокуратурата и Държавната агенция „Национална сигурност“, по - специално до материали, които да им позволят да проверят основателността на исканията за използване на СРС (основателно подозрение и пропорционалност във всеки отделен случай) (вж. пар. 118 и 119 по-горе). Бюрото се оплаква и от неколкократното предоставяне на невярна информация от страна на основния орган по прилагане на СРС в България, Агенцията за технически операции (вж. пар. 118 по-горе). Подобно възпрепятстване сериозно отслабва възможностите за надзор на Бюрото и не може да се разглежда като оправдано (сравнете, *mutatis mutandis*, с *Roman Zakharov*, цитирано по-горе, пар. 281). Предоставянето на достъп на членовете на Бюрото до всички материали по наказателно дело не може да засегне текущите разследвания, тъй като тези членове имат най - високо ниво на достъп до класифицирана информация и са обвързани с професионална тайна (вж. пар. 109, 110 и 129 по-горе). Комитетът на министрите вече обърна внимание и на този въпрос (вж. пар. 229, буква д) по-горе).

344.  На последно място, Националното бюро няма правомощия да разпорежда мерки за обезвреда, като например унищожаването на материали от наблюдение. То може да обърне внимание на ръководителите на съответните органи и на прокуратурата или на Висшия съдебен съвет за нередности, извършени от съдии (вж. пар. 122 и 123 по-горе). Правомощието на Бюрото да дава указания изглежда се отнася единствено до указания, предназначени да подобрят практиките, а не до инструкции в конкретни случаи, както се потвърждава по - специално от ограничения им брой годишно (вж. пар. 120 и 121 по-горе).

345.  Специалната парламентарна комисия също не е оправомощена да разпорежда мерки за обезвреда (вж. пар. 127 по-горе). Освен това, за разлика от Националното бюро, тя не извършва редовни инспекции (вж. пар. 128 по-горе и сравни с таблицата в пар. 124 по-горе).

346.  Правителството не твърди и няма индикации, че Комисията за защита на личните данни или Инспекторатъткъм Висшия съдебен съвет досега са играли някаква роля в надзора на системата за тайно наблюдение по силата на техните правомощия съгласно Закона за защита на личните данни от 2002 г., изменен през 2019 г. с цел транспониране на Директива (ЕС) 2016/680 (вж. пар. 225 и 226 по-горе).

347.  С оглед на описаните по-горе недостатъци, системата за прилагане на СРС в България във вида, в който е организирана понастоящем, не изглежда в състояние да осигури ефективни гаранции срещу злоупотреби.

Уведомление

348.  Съответните фактори в тази рубрика са (а) кога е възможно такова уведомяване и (б) дали това е предпоставка за използване на съществуващите средства за правна защита.

349.  Както вече беше отбелязано в пар. 267 по-горе, Националното бюро трябва да уведоми лицето, което е било поставено под тайно наблюдение, само ако това е станало неправомерно, докато съгласно съдебната практика на Съда такова уведомление се изисква във всички случаи без предварително уведомяване, веднага след като то може да бъде направено, без да се застрашава целта на наблюдението (вж. *Klass и други срещу Германия*, 6 септември 1978 г., § 58, Серия А № 28; *Weber и Saravia срещу Германия* (дек.), № 54934/00, § 135, ECHR 2006 - XI; и по - скоро *Roman* Zakharov, цитиран по-горе, § 287). В това отношение е показателно, че броят на уведомленията, осъществявани от Бюрото всяка година в сравнение с годишния брой на случаите на използване на СРС е много малък (сравни таблиците в пар. 55 и 135 по-горе). Освен това Бюрото е длъжно да уведомява само физическите лица, а не юридическите лица (вж. пар. 130 по-горе) – точка, която Комитетът на министрите вече отбеляза в контекста на своя надзор върху изпълнението на *Асоциация за европейска интеграция и права на човека и Екимджиев* (цитирано по-горе) (вж. пар. 229, буква д) *in fine* по-горе).

350.  Правителството не изтъква, а и няма данни за това, че досега е имало случаи, в които такова уведомление е направено по силата на член 54, ал. 4 от Закона за защита на личните данни, изменен през 2019 г., за да транспонира Директива (ЕС) 2016/680 (вж. пар. 220 по-горе). Също така не изглежда досега да е имало случаи, в които хората да са получили информация относно тайното наблюдение по член 55, ал. 3 *in fine*, чл. 56, ал. 6 *in fine* или чл. 57, ал. 1 и 2 от същия закон, в редакцията след изменението от 2019 г. (вж. пар. 221 и 224 по-горе).

351.  Същевременно, както вече беше отбелязано в пар. 266 - 271 по-горе, уведомяването от страна на Националното бюро обикновено е предпоставка за предявяване на иск за обезщетение по член 2, ал. 1, точка 7 от ЗОДОВ; единствената друга ситуация, при която може да се проведе такъв иск, е, когато тайното наблюдение е било разкрито, тъй като материалите от него са били използвани в наказателното производство.

Средства за правна защита

352.  През 2009 г. България въведе специално средство за правна защита по отношение на тайното наблюдение: иск за обезщетение по член 2, ал. 1, точка 7 от ЗОДОВ (вж. пар. 136 по-горе). Това средство за правна защита обаче, макар и ефективно в някои ситуации, страда от три сериозни недостатъка, посочени в пар. 266 -273 по-горе: а) до този момент искът не може да бъде проведен успешно при липса на предварително уведомление от Националното бюро, че някой е поставен под наблюдение, б) не води до проверка на необходимостта от наблюдение във всеки отделен случай и в) не е достъпен за юридически лица.

353.  Освен това единствената форма на обезвреда, налична в такива производства, е парично обезщетение (вж. пар. 139 по-горе); съдилищата нямат правомощия да разпореждат унищожаването на материалите, получени в резултат на използването на СРС(например *Big Brother Watch и други*, цитирани по-горе, § 413). Комитетът на министрите вече подчерта тази точка в контекста на наблюдението върху изпълнението на *Асоциация за европейска интеграция и права на човека и* *Екимджиев* (цитирано по-горе) (вж. пар. 229, буква е) *по-горе*).

354.  Както е отбелязано в пар. 275 по-горе, новите средства за правна защита, които са на разположение съгласно Закона за защита на личните данни, изменен през 2019 г. с цел транспониране на Директива (ЕС) 2016/680 (вж. пар. 221, 224 и 227 по-горе), към момента няма доказателства да са ефективни по отношение на тайното наблюдение и освен това не са достъпни за юридическите лица.

355.  От това следва, че българското законодателство не предоставя ефективни средства за правна защита на всички лица, които подозират, без конкретни доказателства, че са били неоправдано подложени на тайно наблюдение. От това следва също, че възражението на правителството, че средствата за правна защита на национално равнище не са изчерпани, което беше свързано с разглеждане съществото на оплакването (вж. пар. 259 по-горе), трябва да бъде отхвърлено.

Заключение

356.  Макар и значително подобрени, след като бяха разгледани от Съда в *Асоциация за европейска интеграция и права на човека и* *Екимджиев* (цитирано по-горе), законите, уреждащи тайното наблюдение в България, както се прилагат на практика, все още не отговарят на минималните гаранции срещу произвол и злоупотреби, изисквани по член 8 от Конвенцията, в следните отношения:

а) вътрешните правила, регулиращи съхранението и унищожаването на материали, получени чрез използване на СРС, не са достъпни за обществеността (вж. пар. 296 *по-горе*);

б)  терминът „обекти“ в чл. 12, ал. 1 от ЗСРС не е дефиниран по начин, че да гарантира, че не може да служи като основа за произволно наблюдение (вж. пар. 303 по-горе);

в) прекомерната продължителност на първоначалното разрешение за използване на СРС по съображения за защита на националната сигурност – две години – значително отслабва съдебния контрол, на който е подложено това наблюдение (вж. пар. 305 по-горе);

г) процедурата по разрешаване използването на СРС, както функционира на практика, не е в състояние да гарантира, че се прибягва до наблюдение само когато „е необходимо в едно демократично общество“ (вж. пар. 307 -322 по-горе);

д) в законовите разпоредби, уреждащи съхранението, достъпа, преглед, използването, съобщаването и унищожаването на данните от наблюдението, съществуват редица празноти (вж. пар. 326 -332 по-горе);

е)  системата за надзор, както е организирана понастоящем, не отговаря на изискванията за достатъчна независимост, компетентност и правомощия (вж. пар. 335 -347 по-горе);

ж) уредбата на уведомяването е твърде ограничаваща (вж. пар. 349 -351 по-горе); и

з) специалното средство за правна защита, иск по член 2, ал. 1, точка 7 от ЗОДОВ, не е на разположение на практика при всички възможни сценарии, не гарантира проверка на обосноваността на всеки един случай на използване на СРС (във връзка с разумно съмнение и пропорционалност), не е достъпно за юридически лица и е ограничено от гледна точка на възможностите за обезвреда (вж. пар. 266 - 273 и 352 - 355 по-горе).

357.  Тези недостатъци в правния режим изглежда са оказали реално влияние върху функционирането на системата за тайно наблюдение в България. Повтарящите се скандали, свързани с тайното наблюдение (вж. пар. 56, 57, 59 и 67 по-горе), предполагат наличието на практики на злоупотреба с наблюдение, които изглежда се дължат поне отчасти на недостатъчните правни гаранции (вж. *Асоциация за европейска интеграция и права на човека и* *Екимджиев*, § 92, и *Роман Захаров*, § 303, и двете цитирани по-горе).

358.  От това следва, че българските закони, уреждащи тайното наблюдение, не отговарят напълно на изискването за „качество на закона“ и са неспособни да ограничат „намесата “, произтичаща от уредбата на тайното наблюдение в България, до това, което е „необходимо в едно демократично общество“.

359.  Следователно е налице нарушение на член 8 от Конвенцията.

* 1. ЗАПАЗВАНЕ И ДОСТЪП ДО ТРАФИЧНИ ДАННИ

360.  Жалбоподателите се оплакват също така, че системата за съхранение и последващ достъп до трафични данни в България не отговаря на изискванията на член 8 от Конвенцията и че в това отношение те не разполагат с ефективни средства за правна защита в нарушение на член 13 от Конвенцията.

361.  С оглед на съдебната практика на Съда (вж. *Роман Захаров*, пар. 307) посоченото оплакване също подлежи на разглеждане единствено по член 8 от Конвенцията, чийто текст, доколкото е уместно, е посочен в пар. 247 по-горе.

* + 1. Допустимост
       1. Твърденията на страните
          1. Статус на жертва на жалбоподателите

Правителството

362.  Правителството посочва, че жалбоподателите не могат да твърдят, че са жертва на нарушение на правото им на зачитане на личния им живот или кореспонденция. Това е така, защото по българското законодателство данните за трафика могат да бъдат достъпни само във връзка с тежки престъпления, дори когато националната сигурност е застрашена. Освен това, тъй като в България юридическите лица не могат да понесат наказателна отговорност, двете организации са извън обхвата на оспорваните закони.

363.  По - нататък правителството твърди, че жалбоподателите, които са разполагали с необходимия правен експертен опит, са могли да сезират специалната парламентарна комисия да провери дали техните задържани трафични данни са били обект на незаконен достъп. Тази комисия също така е длъжна да информира физическите лица за неправомерни искания за достъп или за осъществен достъп до техните трафични данни по своя собствена инициатива. Физическите лица биха могли да потърсят информация за това и съгласно Закона за защита на личните данни, който с изменението през 2019 г. е транспонирал Директива (ЕС) 2016/380 или съгласно Общия регламент за защита на данните - от самите доставчици на комуникационни услуги или от Комисията за защита на личните данни. Процедурата по уведомяване е съчетана с възможности за подаване на жалба до тази Комисия и за търсене на обезщетение от доставчиците на съобщителни услуги или от съответните органи съгласно разпоредбите на Закона за защита на личните данни или по общия исков ред. Тъй като тези средства за правна защита са ефективни, неизползването им от страна на жалбоподателите ги лишава от статут на жертви и превръща жалбата им в *actio popularis*.

Жалбоподателите

364.  Жалбоподателите изтъкват, че с оглед на сходствата между тайното наблюдение и съхраняването и последващия достъп до данни за трафика, подходът към въпроса дали биха могли да претендират, че са жертви на намеса в правата им по член 8 от Конвенцията по отношение на достъпа до такива данни, трябва да бъде същият като този, възприет от Съда по отношение на тайното наблюдение. Всички те са използвали електронни съобщителни услуги, а разглежданите закони са се прилагали за всички такива потребители, включително юридически лица. Фактът, че тези закони дават възможност на органите да имат достъп до съхранявани данни само във връзка със сериозни престъпления – правило, което при всички случаи е пренебрегвано в няколко известни случая – не променя тази позиция, особено с оглед на многохилядните заявления за достъп през всяка от последните години и слабите механизми за надзор. Освен това жалбоподателите подчертават, че запазените данни са позволили профилиране на всички лица в страната. Незаконното използване на тази процедура в дисциплинарни производства срещу съдии и прокурори през периода 2010 -2011 г. показва в голяма степен потенциала за злоупотреби.

365.  В българското законодателство не са предвидени ефективни процедури, чрез които жалбоподателите могат да получат информация за съхраняването или достъпа до техните данни за трафика или компенсация във връзка с това. Следователно те могат да претендират, че са жертва на нарушение поради самото съществуване на закони, позволяващи съхраняването и достъпа до такива данни.

* + - * 1. Изчерпване на вътрешните средства за правна защита

366.  Въз основа на аргументите, обобщени в пар. 363 по-горе, правителството също така заяви, че заявителите не са изчерпали националните средства за правна защита.

367.  Жалбоподателите оспорват това твърдение, като отбелязват, че когато са подали жалбата си до Съда, нито Комисията за защита на личните данни, нито специалната парламентарна комисия са имали функции, свързани със запазването или достъпа до данни за трафика. Следователно не е било възможно да подават жалби до нито един от тези органи по този въпрос.

* + - 1. Оценката на Съда

368.  Подобно на позицията във връзка с оплакването относно тайното наблюдение (вж. пар. 259 по-горе) и двете възражения на правителството са толкова тясно свързани със съществото на оплакването, че трябва да бъдат присъединени към разглеждането на оплакването по същество.

369.  Освен това жалбата не е явно необоснована по смисъла на член 35, параграф 3, буква а) от Конвенцията или недопустима на други основания. Следователно тя трябва да бъде обявена за допустима.

* + 1. Основателност
       1. Статут на жертва на жалбоподателите и наличие на намеса
          1. Твърденията на страните

370.  Представените от страните становища са обобщени в пар. 362 -365 по-горе.

* + - * 1. Оценката на Съда

371.  Съгласно българското законодателство всички доставчици на съобщителни услуги в страната трябва да съхраняват всички данни за трафика на всички свои потребители в продължение на шест месеца с оглед предоставянето на тези данни на разположение на органите за определени правоприлагащи цели (вж. пар. 161 и 163 по-горе). След това различни органи могат да получат достъп до тези данни (вж. пар. 167 -169 по-горе). Целесъобразно е тези две стъпки да се анализират поотделно, тъй като всяка от тях може да засегне правата, гарантирани съгласно член 8 от Конвенцията, по различен начин и в различна степен (вж. *mutatis mutandis*, *Centrum för* rättvisa, §§ 239 -43, както и *Big Brother Watch и други*, §§ 325 -29, и двете цитирани по-горе).

Запазване на трафични данни от доставчиците на съобщителни услуги

372.  Установено е, че самото съхраняване на данни, свързани с личния живот на дадено лице, представлява намеса в правото на това лице на зачитане на „личния живот“ (вж. по отношение на личните данни, свързани с използването на съобщителни услуги, Решение по *дело Breyer/Германия*, № 50001/12, § 81, 30 януари 2020 г.; Решение по дело *Centrum för* rättvisa, посочено по-горе, точка 244, и Решение по дело *Big Brother Watch и др*., посочено по-горе, точка 330). Всички видове данни за комуникация, предмет на спора в настоящия случай – данни за абонати, трафик и местоположение – могат да се отнасят, самостоятелно или в комбинация, до „личния живот“ на съответните лица. Българското законодателство изисква всички доставчици на съобщителни услуги в страната да запазват всички тези данни на всички потребители за потенциален последващ достъп от страна на властите (вж. пар. 161 по-горе). Не е оспорено, че двамата индивидуални жалбоподатели използват такива услуги. От това следва, че само по себе си това законово оправомощаване за задържане на данните е намеса в правото им на зачитане на техния „личен живот “, независимо от това дали съхраняваните данни след това са достъпни за органите.

373.  Това запазване се приравнява също така на намеса в правото на тези жалбоподатели на зачитане на тяхната кореспонденция. Съдът вече е постановил, че съхранението на данни за трафика и местоположението, свързани с мобилна телефонна линия, представлява намеса в правото на лицето, което използва тази линия, на зачитане на неговата „кореспонденция“ (вж. *Ben Faiza срещу Франция*, №. 31446/12, §§ 66 -67, 8 февруари 2018 г.). Няма причина да се счита другояче по отношение на други видове комуникации, като например електронните съобщения или по отношение на комуникационните данни като цяло.

374.  Що се отнася до двете организации-жалбоподатели, установено е, че съобщенията на юридическите лица са обхванати от понятието „кореспонденция“ в член 8, параграф 1 от Конвенцията (вж. *Асоциация за европейска интеграция и права на човека и Екимджиев*, § 60, и *Liblik and Others*, § 110, и двете цитирани по-горе). Не е оспорено, че двете организации също използват комуникационни услуги в България. От това следва, че законово предвиденото запазване на данни за трафика на всички потребители на съобщителни услуги в страната е намеса в правото им на зачитане на тяхната „кореспонденция “.

375.  Намесата, макар и да се извършва от частни лица – доставчици на съобщителни услуги, е предвидена в закона. Действително, доставчиците на услуги, които не спазват законоустановените си задължения за съхраняване на данни, подлежат на санкции (вж. точка 161 *по-горе*). От това следва, че намесата се осъществява от българската държава (сравнете с *Digital Rights Ireland*, цитирани в точка 233 по-горе, § 34).

Достъп на органите до запазените трафични данни

376.  Достъпът на органите до съхраняваните данни представлява допълнителна намеса в правото на зачитане на личния живот и на съобщенията съгласно член 8 от Конвенцията (вж. *mutatis mutandis*, *Centrum för* rättvisa, § 244 и *Big Brother Watch и други*, § 330, и двете цитирани по-горе). Но е ясно, че властите не осъществяват достъп до всички запазени данни за комуникация. Тъй като не е възможно физическо или юридическо лице да знае със сигурност дали е осъществен достъп до данните по този начин, е целесъобразно да се анализира въпросът дали жалбоподателите могат да твърдят, че са жертви на намеса в правата им по член 8 поради самото съществуване на закони, позволяващи на органите да направят това, като се позовават на същите критерии като тези, използвани във връзка с тайното наблюдение: а) обхват на законите, позволяващи такъв достъп и б) наличието на ефективни средства за правна защита (вж. пар. 262 -275 по-горе).

Обхват на приложимия закон

377.  Съгласно съответните законови разпоредби органите имат право на достъп до съхраняваните трафични данни на всеки, ако това е необходимо за целите на: а) националната сигурност; б) предотвратяването, разкриването или разследването на тежки престъпления; в) проследяването на хора, които са били окончателно осъдени на лишаване от свобода по отношение на тежко престъпление или които са попаднали или биха могли да попаднат в ситуация, която излага на риск живота или здравето им; и г) (това се отнася единствено за идентификационните номера на клетките) извършването на операции по издирване и спасяване на хора в беда (вж. пар. 163 по-горе). Тъй като данните за трафика всеки в България теоретично могат да станат необходими за една или повече от тези цели, и четиримата жалбоподатели, включително организациите, могат да бъдат засегнати от спорното законодателство.

Наличие на ефективни средства за правна защита

378.  Следващият въпрос е дали съществува ефективно средство за правна защита, което може да успокои подозренията сред широката общественост, че незаконно се осъществяват и използват задържани трафични данни.

379.  Нито ЗСРС, нито член 159а от Наказателно - процесуалния кодекс предвиждат правни средства за защита по отношение на запазването или достъпа до данни за трафика.

380.  Нищо не подсказва, че средствата за правна защита съгласно член 38, ал. 1 и 7, член 39, ал. 1 и 2 и член 82, ал. 1 от Закона за защита на личните данни, формулирани след изменението от 2019 г., с цел транспониране на Директива (ЕС) 2016/680 (вж. пар. 218 и 227 по-горе), досега са били използвани за предоставяне на правна защита по отношение на запазването на трафични данни от доставчиците на съобщителни услуги или по отношение на достъпа до тях и използването им от органите. При липса на докладвани решения от българските съдилища, не е редно този съд да каже дали или как тези средства за правна защита, които са общоприложими, могат да действат в такива случаи. Вярно е, че тези средства за защита са нови и че те са част от клон на правото, който се е развил сравнително наскоро. Но правителството трябваше да обясни начина им на действие и доколкото е възможно да подкрепи техните обяснения с конкретни примери (вж. *mutatis mutandis*, *Roman* Zakharov, § 295, и *Mustafa* Sezgin Tanrıkulu, § 28 -29, и двете цитирани по-горе). Правителството обаче е неясно по този въпрос, като се задоволява да посочи само, че изменението от 2019 г. е въвело разпоредби, уреждащи отговорността на доставчиците на съобщителни услуги и съответните органи по отношение на запазените трафични данни и достъпа до тях (вж. пар. 363 и 388 по-горе, и за разлика от обстоятелствата в *Ringler* *v. Austria* (дек.) [Комитет], № 2309/10, §§ 12-13 и 51-54, 15 май 2020 г.). При липсата на допълнителни данни за действителното действие на тези средства за правна защита по отношение на данните за трафика, не може да се приеме, че понастоящем те са ефективни в това отношение. Освен това тези средства за правна защита не са достъпни за юридически лица (вж. пар. 216 и 239 по-горе).

381.  Също така няма доказателства, че е налице средство за правна защита съгласно общия закон за обезщетяване на вреди.

382.  От това следва, че опасенията на обществеността относно заплахата от злоупотреба с достъпа и използването на данни за трафика от страна на органите не могат да бъдат разсеяни в достатъчна степен от наличието на ефективни средства за правна защита в това отношение.

Заключение

383.  С оглед на изложените по-горе съображения не е необходимо да се изследва дали има риск властите да осъществят достъп до запазените данни на жалбоподателите на основание личното им положение (вж. *mutatis mutandis*, *Centrum för* *rättvisa*, посочено по-горе, §§ 175 -76).

384.  От това следва, че разглеждането на уредбата относно достъпа до задържаните данни за комуникация от страна на властите *in abstracto* е обосновано. От това следва също, че възражението на правителството, че жалбоподателите не могат да претендират, че са жертва на нарушение на член 8 от Конвенцията, за което се твърди, че е причинено от самото съществуване на такива закони, което е беше свързано с разглеждане по същество на оплакването (вж. пар. 368 по-горе), трябва да бъде отхвърлено.

* + - 1. Обоснованост на намесата
         1. Твърдения на страните

Жалбоподателите

385.  Жалбоподателите изтъкват, че начинът, по който законът е регламентирал достъпа до данни за трафика – по – специално липсата на каквото и да било изискване за органа, който прави искане за достъп, да представи доказателства в подкрепа на искането си – не е осигурил достатъчно гаранции срещу злоупотреби. Освен това няма изискване за текущ съдебен контрол. Публично достъпните съдебни решения по искания за достъп, много от които съдържат само стереотипни разсъждения, показват, че съдебният контрол в такива случаи е формален и предоставя малко гаранции срещу злоупотреби.

386.  Останалите механизми за надзор също са недостатъчни. Специалната парламентарна комисия не е длъжна да разглежда индивидуални жалби и няма публично достъпни правила, регулиращи нейната работа. Следователно не е изненадващо, че въпреки че всяка година органите отправят десетки хиляди искания за достъп до съхранявани данни за комуникация, тази комисия досега е получавала само между една и четири жалби годишно. Въпреки това докладите на комисията регистрират обезпокоителни нарушения на закона. От своя страна, Комисията за защита на личните данни просто събира статистически данни за запазването на данните за трафика. В нейните доклади не се споменават случаи, в които тя е разглеждала индивидуални жалби, и не е ясно как Общият регламент би могъл да бъде приложен във връзка с това.

387.  Освен това законът не изисква уведомяване в случаите на законосъобразен достъп до съхранявани данни за комуникация. Това е сериозен недостатък, тъй като начинът, по който се оценява законосъобразността на достъпа във всеки отделен случай е неясен. На практика това означава, че ако съдът е издал разрешение за достъп, заинтересованите лица няма да бъдат уведомени за достъпа и следователно няма да могат да използват никакви средства за правна защита във връзка с него. Исковете за обезщетение съгласно Общия регламент са неприложими, тъй като не се прилагат за обработването на данни от органите за целите на правоприлагането. За разлика от позицията по отношение на тайното наблюдение, ЗОДОВ не предвижда отговорност на съдилищата или на прокуратурата във връзка със запазени данни за трафика. Но дори законът да дава възможност да се предявят искове за обезщетение в този контекст, на практика би било трудно както за физическите, така и за юридическите лица да докажат неимуществени вреди поради такива обстоятелства, тъй като те не могат да докажат, че действие, за което не са знаели, им е причинило негативни емоции. Паричните вреди от своя страна биха били почти невъзможни за установяване. За да бъде ефективна, мярката за обезвреда в тази област трябва да бъде насочена към тези въпроси, например като се предвиди еднократно обезщетение.

Правителството

388.  Правителството твърди, че в закона ясно е посочено какви данни за трафика трябва да се съхраняват, за колко време и за какви цели. С изменението от 2019 г., с което се въвеждат Общият регламент и Директива (ЕС) 2016/680, бяха въведени строги гаранции за защита на данните и разпоредби, уреждащи отговорността на доставчиците на съобщителни услуги и на властите, и бяха разширени правомощията на надзорните органи. Съответните правила са предвидими и съдържат достатъчно гаранции срещу произвол.

389.  Задържането на данни се прави в интерес на националната сигурност и обществения ред, както и за предотвратяване на престъпления.

390.  Що се отнася до необходимостта от това задържане, няма европейски консенсус относно нуждата от запазване на трафични данни и конкретните условия за това. Дори след решенията на Съда на ЕС относно *Digital Rights Ireland and Others*, *както и относно Tele2 Sverige, Watson и други* (вж. точки 233 и 240 по-горе), много държави - членки на Европейския съюз не са отменили изцяло своите закони, предвиждащи общо запазване на данни за трафика, тъй като това е ценен инструмент за борба с тежката престъпност. Един по - рестриктивен подход би могъл да попречи на правилното функциониране на този инструмент. Съдът на ЕС не e отхвърлил напълно значението на запазването на комуникационните данни и въпросът остава в рамките на свободата на преценка на държавите.

391.  В България до задържаните данни за трафика може да се осъществи достъп само във връзка с тежки престъпления и въз основа на съдебно разрешение. Законът определя по изчерпателен начин органите, които биха могли да направят искане, и изисква от тях да посочат достатъчно причини, поради които те следва да бъдат уважени. Ако материалите в подкрепа на искането са недостатъчни, съдиите могат да поискат допълнителна информация и решенията им в такива случаи обикновено са добре обосновани. Възможността доставчиците на съобщителни услуги да откажат достъп до съхраняваните от тях данни, ако липсват необходимите предпоставки, е допълнителна предпазна мярка срещу злоупотреби.

392.  Също така има ясни правила относно унищожаването на запазените данни и съдията, издал разрешение за достъп, следва да бъде информиран за това унищожаване. Освен това целият процес е под надзора на Комисията за защита на личните данни и специалната парламентарна комисия.

393.  На последно място, що се отнася до уведомяването и средствата за правна защита, правителството се позовава на представените вечеаргументи относно статута на жертва на жалбоподателите (вж. пар. 363 по-горе).

* + - * 1. Оценката на Съда

Общи принципи

394.  С оглед на технологичното и социално развитие през последните две десетилетия в областта на електронните съобщения, трафичните данни днес могат да разкрият много лична информация. Ако бъдат получени от властите в цялост, тези данни могат да бъдат използвани за създаване на личен профил на дадено лице чрез картографиране на социални мрежи, проследяване на местоположението, проследяване на сърфирането в интернет, картографиране на моделите на комуникация и поглед към това с кого е взаимодействало това лице (вж. *Centrum för* rättvisa, § 256 и *Big Brother Watch и други*, § 342, и двете цитирани по-горе). Следователно придобиването на тези данни чрез прихващане в цялост може да бъде също толкова интрузивно, колкото и придобиването в цялост на съдържанието на съобщенията, поради което тяхното прихващане, съхраняване и търсене от страна на органите трябва да бъдат анализирани чрез позоваване на същите гаранции като тези, приложими към съдържанието (вж. *Centrum för* rättvisa, § 277 и *Big Brother Watch и други*, § 363, и двете цитирани по-горе).

395.  Тук трябва да се добави, че по същия начин общото запазване на трафични данни от доставчиците на съобщителни услуги и достъпът до тях от страна на органите в отделни случаи трябва да бъдат придружени, *mutatis mutandis*, от същите гаранции като тайното наблюдение (вж. точки 291 -293 по-горе).

Прилагане на тези принципи

Достъпност на закона

396.  Всички законови разпоредби, уреждащи съхраняването на данни за трафика и достъпа до тях от страна на органите, са публикувани официално и по този начин са достъпни за обществеността.

Защита на съхраняваните данни от доставчиците на съобщителни услуги

397.  Българското законодателство изрично изисква доставчиците на съобщителни услуги да запазват и обработват съхранени данни за трафика в съответствие с правилата за защита на личните данни, както и да бъдат въведени различни технически и организационни механизми, за да се гарантира, че тези данни не са обект на неправомерен достъп, разкриване или промяна и че те се унищожават при изтичане на законоустановения срок за тяхното съхранение (вж. пар. 164 -166 по-горе).

Основания, въз основа на които органите имат достъп до запазените данни

398.  В България законът определя изчерпателно основанията, въз основа на които органите могат да търсят достъп до запазените данни: защита на националната сигурност; предотвратяване, разкриване или разследване на тежки престъпления; проследяване на хора, които са осъдени на лишаване от свобода по отношение на такива престъпления; проследяване на хора, които са изпаднали или биха могли да попаднат в ситуация, която излага на риск живота или здравето им; и (само що се отнася до данни за местоположението) провеждане на операции по издирване и спасяване на хора в беда (вж. пар. 163 по-горе). Следователно законът е достатъчно ясен по този въпрос. Както е отбелязано в пар. 301 по-горе, по отношение на тайното наблюдение, самото обстоятелство, че едно от основанията за достъп до съхраняваните данни за трафика е „национална сигурност “, само по себе си не противоречи на член 8 от Конвенцията.

399.  Във връзка с това трябва да се отбележи, че когато през 2020 г. българският парламент разшири възможните основания за придобиване на запазени данни, така че те да включват прилагане на мерки за изолация и карантина във връзка с инфекциозни заболявания, Конституционният съд отмени тези нови разпоредби в цялост, на основание, че създават предпоставки за непропорционална намеса в конституционното право на неприкосновеност на личния живот (вж. пар. 158 и 159 по-горе).

Процедура за получаване на достъп

Стандартна процедура

400.  Българското законодателство съдържа правила, които имат за цел да гарантират, че органите имат достъп до съхраняваните трафични данни само когато това е оправдано. На първо място, само ограничен брой органи могат да потърсят достъп до тези данни в рамките на съответните си правомощия (вж. пар. 167 -169 по-горе). По - важното е, че такъв достъп може да бъде предоставен само от председателя на компетентния съд или от съдия, на когото е делегирано това правомощие (за достъп, поискан извън рамките на вече висящо наказателно производство), или от съдия от компетентния първоинстанционен съд (за достъп, поискан от прокурор в хода на наказателното производство) (вж. пар. 173 -177 по-горе).

401.  Тези гаранции обаче не отговарят на необходимите стандарти за ефективност в няколко отношения.

402.  Исканията за достъп, подадени извън рамките на вече висящо наказателно производство, трябва да посочват не само основанията за искането на достъп до такива данни и целта, за която те се търсят, но също така да съдържат пълно описание на обстоятелствата, които показват, че данните са необходими за съответната цел (вж. пар. 171 по-горе). За разлика от тази ситуация няма изискване исканията за достъп, подадени в хода на наказателното производство, макар да се очаква да съдържат информация за предполагаемото престъпление във връзка с което се иска достъп, да съдържат мотиви защо въпросните данни са наистина необходими – те трябва да съдържат само описание на обстоятелствата, които са в основата на искането за достъп, което изглежда като доста по-слабо изискване (вж. пар. 172 по-горе). Следователно законът не уточнява във всички случаи, че достъпът във всеки отделен случай може да се търси и предостави само ако произтичащата от това намеса в правата по член 8 на съответното (ите) лице(а) би била наистина необходима и пропорционална.

403.  Както и при процедурата за разрешаване на тайно наблюдение (вж. пар. 309 по-горе), на този етап може да се констатира още един възможен недостатък: въпреки че е необходимо производството за достъп до данни да се провежда без уведомяване на лицата, достъп до чиито данни се търси, органът, който иска достъп, не е длъжен да разкрива пред съдията напълно и добросъвестно всички въпроси, свързани с основателността на неговото искане за достъп, включително въпроси, които могат да отслабят неговото искане.

404.  Законът не изисква материалите в подкрепа на искането за достъп да бъдат приложени към него, което в много случаи може да попречи на съдията, който разглежда искането, да провери дали то е основателно.

405.  Законът също така не изисква съдиите, разглеждащи такива искания, да излагат причините, поради които са решили, че предоставянето на достъп до въпросните данни е действително необходимо (вж. пар. 179 и 180 по-горе). Както вече беше отбелязано във връзка с процедурата за разрешаване на тайно наблюдение (вж. точка 313 по-горе), предоставянето на мотиви, дори и кратко, е единственият начин да се гарантира, че съдията, разглеждащ искането за достъп, е прегледал подробно заявлението и материалите, които го подкрепят, и действително е насочил съзнанието си към въпросите дали достъпът до въпросните данни е обоснована и пропорционална намеса в правата по член 8 на лицето (лицата), до чиито данни се осъществява достъп, както и на всяко лице(лица), което (които) е вероятно да бъде (ат) засегнато (и) от това.

406.  От това следва, че процедурите за достъп на съответните органи до съхраняваните данни за трафика не гарантират по ефективен начин, че такъв достъп се предоставя само когато е действително необходим и пропорционален във всеки отделен случай.

Неотложна процедура

407.  От друга страна, не изглежда да възниква отделен въпрос по отношение на спешната процедура, съгласно която органите могат да получат достъп до съхраняваните данни за трафика без предварително съдебно разрешение, ако съществува непосредствена опасност от извършване на престъпление, свързано с тероризъм (вж. пар. 183 по-горе). Когато органите прибягват до тази неотложна процедура, компетентният съдия трябва в срок от двадесет и четири часа да оцени и одобри със задна дата необходимостта от това; в противен случай всички данни, предоставени съгласно искането за пряк достъп, трябва да бъдат унищожени от органа, който го е получил (вж. пар. 184 и 185 по-горе). Освен това тази спешна процедура очевидно се използва пестеливо (вж. пар. 186 по-горе и я сравни с таблицата в пар. 182 по-горе).

Време, през което органите могат да съхраняват и използват данни, които впоследствие не се използват в наказателното производство

408.  Законът за електронните съобщения гласи, че всички комуникационни данни, които не са използвани за образуване на наказателно производство, трябва да бъдат унищожени в срок от три месеца от получаването им от органите и че всички данни, до които е осъществен достъп по спешната процедура, трябва незабавно да бъдат унищожени по същия начин, ако компетентният съдия не е одобрил прилагането на спешната процедура (вж. пар. 194 и 195 по-горе). За разлика от тази ситуация, няма определен такъв срок по отношение на данните, до които е осъществен достъп в хода на наказателното производство. Въпреки че изглежда, че въпросът е обхванат от вътрешни правила, издадени от главния прокурор, те не са достъпни за обществеността и не е ясно какво казват (вж. пар 196 по-горе). Нищо не сочи, че разпоредбите на Закона за защита на личните данни, изменен през 2019 г. с цел транспониране на Директива (ЕС) 2016/680 (вж. пар. 219 по-горе), досега са били използвани за запълване на тази празнота.

Процедури за съхраняване, достъп, преглед, използване, съобщаване и унищожаване на данни, до които органите имат достъп

409.  Законът за електронните съобщения и Наказателно - процесуалният кодекс не казват нищо за процедурите за съхраняване, достъп, преглед, използване, съобщаване и унищожаване на комуникационни данни, до които органите имат достъп, и тези въпроси не са конкретно обхванати от правилата, уреждащи прокурорските преписки и съдебните дела (вж. пар. 193 по-горе). Изглежда, че тези данни просто се съхраняват в наказателното дело, следват неговата съдба и могат да бъдат достъпни за всеки, който има достъп до самото дело (пак там). Не може да се приеме, че това осигурява подходящо ниво на защита на данните, които понякога могат да засягат интимни аспекти от личния живот на някого или могат по друг начин да позволят непропорционално нахлуване в личния живот на засегнатите лица или в „кореспонденцията“ на засегнатите юридически лица. Тук също така нищо не подсказва, че разпоредбите на Закона за защита на личните данни, изменен през 2019 г. с цел транспониране на Директива (ЕС) 2016/680 (вж. пар. 219 по-горе), досега са били използвани за запълване на тази празнота.

Правила за надзор

410.  В България три органа могат да осъществяват надзор относно задържането на трафични данни и последващия достъп до тях от страна на органите: а) Комисията за защита на личните данни; б) съдията, издал заповедта за достъп; и в) същата парламентарна комисия, която контролира тайното наблюдение (вж. пар. 197 -210 по-горе).

411.  Съгласно Закона за електронните съобщения Комисията за защита на личните данни може (а) да поиска от доставчиците на съобщителни услуги да ѝ предоставят всякаква информация, свързана с правомощията й в тази област, (б) да проверят как тези доставчици изпълняват задълженията си да съобщават нарушенията на сигурността на личните данни на потребителите и (в) да проверят техническите и организационните мерки, предприети от тези доставчици за съхраняване на запазените комуникационни данни (вж. пар. 201 и 202 по-горе). Тя може също така да дава обвързващи указания на доставчиците на съобщителни услуги и да ги санкционира (вж. пар. 203 и 204 по-горе). Но правомощията й съгласно Закона за защита на личните данни изглежда се ограничават до надзора върху доставчиците на съобщителни услуги (вж. пар. 198 по-горе); тя няма изрични правомощия съгласно този закон по отношение на органите, които имат достъп до съхраняваните данни за трафика.

412.  Вярно е, че съгласно разпоредбите на Закона за защита на личните данни, изменен през 2019 г. с цел транспониране на Директива (ЕС) 2016/680, същата Комисия – както и Инспекторатъткъм Висшия съдебен съвет – имат за задача да контролират начина, по който органите обработват лични данни за целите на правоприлагането (вж. пар. 225 по-горе). Но нищо не предполага, че някой от тези два органа досега се е възползвал от тези правомощия по отношение на комуникационните данни.

413.  От своя страна съдията, издал разрешението за достъп, не е в състояние да осигури ефективен надзор. Наистина той или тя трябва да бъде информиран за унищожаването на неподходящи или ирелевантни трафични данни, до които органите имат достъп (вж. пар. 197 по-горе). Но този съдия няма правомощия да разпорежда мерки за обезвреда. Освен това той не е оправомощен или не се очаква да извършва проверки на място и изпълнява надзорните си задължения единствено въз основа на доклада, представен от органите. Макар и ценна гаранция, този механизъм е недостатъчен, за да се гарантира, че не се злоупотребява с правомощията за достъп до данни.

414.  Основният надзорен орган, специалната парламентарна комисия, може да упражнява надзор както върху доставчиците на съобщителни услуги, така и върху съответните органи (вж. пар. 205 по-горе) и разполага с широки правомощия за събиране на информация и за проверки (вж. пар. 207 по-горе). Нейните годишни доклади показват, че тя редовно извършва проверки чрез експертите, които наема (вж. пар. 208 -210 по-горе). Няколко недостатъка обаче подкопават нейната ефективност. Първо, няма изискване нейните членове да бъдат лица с юридическа квалификация или опит (вж. пар. 206 по-горе). На второ място, тя няма правомощия да разпорежда мерки за обезвреда в конкретни случаи, като например унищожаването на запазени или комуникационни данни, до които е осъществен достъп; тя може да дава само инструкции, предназначени да подобрят съответните процедури (вж. пар. 211 по-горе). Ако открие нередности, тя може само да доведе въпроса до знанието на разследващите органи или да информира ръководителите на съответните органи, които са направили искането за достъп и на доставчиците на съобщителни услуги (вж. пар. 212 по-горе).

415.  С оглед на посочените по-горе недостатъци, правилата за задържане на трафични данни и последващия достъп до тях от страна на органите в България, както са разписани понастоящем, не изглеждат в състояние да предоставят ефективни гаранции срещу злоупотреби в това отношение.

Уведомление

416.  Законът за защита на личните данни изисква специалната парламентарна комисия да уведоми дадено лице, ако неговите/нейните задържани данни за трафика са били обект на достъп или под заплаха от незаконен достъп, ако такова уведомление не би нарушило целта, за която тези данни са били обект на достъп (вж. пар. 213 по-горе). Въпреки това, както е отбелязано в пар. 349 по-горе по отношение на тайното наблюдение, съгласно практиката на Съда такова уведомяване се изисква във всички случаи, а не само в случаите, когато данните са били предмет на незаконен достъп, веднага след като уведомлението може да бъде направено, без да се застрашава целта на достъпа.

417.  Няма данни, че до момента такова уведомление е осъществявано по силата на член 54, ал. 4 от Закона за защита на личните данни, изменен през 2019 г. с цел транспониране на Директива (ЕС) 2016/680 (вж. пар. 220 по-горе). Също така не изглежда досега да е имало случаи, в които едно лице да е имало възможност да получи информация за задържането или достъпа до своите комуникационни данни съгласно чл. 37а, чл. 55, ал. 3 *in fine*, чл. 56, ал. 6 *in fine* или чл. 57, ал. 1 и 2 от същия закон, както е формулиран след изменението от 2019 г. (вж. точки 217, 221 и 224 по-горе). Правителството е неясно по този въпрос, като се задоволи да каже, че изменението е въвело разпоредби, даващи възможност на физическите лица да получават такава информация по отношение на съхраняваните данни и данните, обект на достъп (вж. пар. 363 по-горе, и за разлика от обстоятелствата в *Ringler*, цитирани по-горе, § 12 -13 и 51 -54). При липсата на допълнителни данни за действителното действие на тези разпоредби за защита на данните по отношение на задържаните трафични данни, не може да се приеме, че те понастоящем са ефективни в това отношение. Освен това правото да бъдеш уведомен не е на разположение на юридическите лица (вж. пар. 216, 234 и 239 по-горе).

Средства за правна защита

418.  Както вече беше отбелязано в пар. 379 -381 по-горе, не е доказано, че в България съществуват ефективни средства за правна защита по отношение на запазването и достъпа до трафични данни. Следователно възражението на правителството, че жалбоподателите не са изчерпали националните средства за защита в това отношение, което беше присъединено към съществото на оплакването (вж. пар. 368 по-горе), трябва да бъде отхвърлено.

Заключение

419.  Въпреки че разпоредбите, уреждащи задържането на трафични данни и последващия достъп до тях от страна на органите, бяха значително подобрени, след като Конституционният съд ги разгледа през 2015 г. в резултат на решението на Съда на ЕС по делото за *Digital Rights Ireland and Others* (вж. точка 156 по-горе), тези разпоредби, както се прилагат на практика, все още не отговарят на минималните гаранции срещу произвол и злоупотреби, изисквани от член 8 от Конвенцията, в следните отношения:

а) процедурата за получаване на разрешение не изглежда в състояние да гарантира, че органите имат достъп до съхраняваните трафични данни само когато това е „необходимо в едно демократично общество“ (вж. пар. 400 -406 по-горе);

б)  не са определени ясни срокове за унищожаване на данните, до които органите имат достъп в хода на наказателното производство (вж. пар. 408 по-горе);

в)  не съществуват публично достъпни правила относно съхраняването, достъпа, прегледа, използването, съобщаването и унищожаването на комуникационни данни, до които органите имат достъп (вж. пар. 409 по-горе);

г)  системата за надзор, както е организирана понастоящем, не изглежда в състояние ефективно да проверява злоупотребите (вж. пар. 410 -415 по-горе);

д)  действащият понастоящем режим на уведомяване е твърде ограничен (вж. пар. 416 и 417 по-горе); и

е) не изглежда да е налице ефективно средство за правна защита (вж. пар. 379 -381 и 418 по-горе).

420.  От това следва, че тези закони не отговарят напълно на изискването за „качество на закона“ и са неспособни да ограничат „намесата“, произтичаща от системата за задържане и достъп до трафични данни в България, до това, което е „необходимо в едно демократично общество“.

421.  Следователно е налице нарушение на чл. 8 от Конвенцията и в този смисъл.

* 1. ПРИЛОЖЕНИЕ НА ЧЛ. 41 ОТ КОНВЕНЦИЯТА

422.  Чл. 41 от Конвенцията предвижда:

„Ако съдът установи, че е имало нарушение на конвенцията или на протоколите към нея и ако вътрешното право на високодоговарящата страна допуска само частично обезщетение за последиците от това нарушение, съдът присъжда, ако това е необходимо, справедливо удовлетворение на потърпевшата страна.”

* + 1. Вреди
       1. Исканията на жалбоподателите и коментарите на правителството по тях

423.  Първият и вторият жалбоподателиправят искане за по 5 000 евро (евро) за твърдяна неудовлетвореност и разочарование, произтичащи от дефектите в системата за тайно наблюдение в България, които бяха илюстрирани с множество скандали, разкриващи случаи на незаконно и произволно наблюдение.

424.  Третият и четвъртият жалбоподатели правят искане за неопределена сума по отношение на неимуществените вреди, за които се твърди, че са понесени от тях поради нарушаването на техните права на неприкосновеност на личния живот, произтичащи от несъвместимостта на законите, уреждащи тайното наблюдение и задържането и достъпа до трафични данни с изискванията на Конвенцията.

425.  Правителството оспорва изцяло исканията, като отбелязва, че в предишни такива случаи не е било присъдено нищо по отношение на неимуществени вреди.

* + - 1. Оценката на Съда

426.  Констатациите за нарушение представляват достатъчно справедливо удовлетворение за всяка неимуществена вреда, понесена от жалбоподателите в резултат на двете нарушения на член 8 от Конвенцията, установени в този случай (вж. член 312 от *Роман Захаров* и член 379 -80 от *Centrum för* rättvisa, както е цитирано по-горе).

427.  Всъщност съгласно член 46 решение, с което Съдът установява нарушение на Конвенцията или на протоколите към нея, налага на ответната държава задължение да избере, под надзора на Комитета на министрите, общите и/или, ако е уместно, индивидуалните мерки, които да бъдат предприети в нейния вътрешен правен ред, за да се прекрати нарушението и да се направи възможно премахване на последствията от него по начин, който би възстановил, доколкото е възможно, положението, което би възникнало, ако то не беше допуснато. Освен това от Конвенцията и по - специално от член 1 следва, че при ратифицирането ѝ договарящите държави са поели ангажимент да гарантират съвместимостта на вътрешното си законодателство с нея (вж. по-горе, пар. 311).

428.  В този случай, що се отнася до тайното наблюдение, тези общи мерки ще трябва да допълнят тези, които българските власти вече са предприели, за да изпълнят *Асоциация за европейска интеграция и права на човека и Екимджиев* (цитирани по-горе).

* + 1. Разходи и разноски
       1. Исканията на жалбоподателите и коментарите на правителството по тях

429.  Първият и вторият жалбоподател не са поискали възстановяване на адвокатски хонорари, заявявайки, че техните представители са работили по случая безплатно. Те обаче заедно търсят възстановяване на 1 032 лв., направени за превода на техните становища на английски език, и 25,50 лв. под формата на пощенски разходи. Правят искане всяка присъдена сума в това отношение да бъде изплатена на Екимджиев и Партньори, адвокатската кантора, в която работят техните представители. В подкрепа на твърденията си те представят два договора за преводачески услуги и пощенски разписки.

430.  Третият и четвъртият жалбоподатели търсят възстановяване на 2750 EUR адвокатски хонорари, направени за тяхното представителство пред Съда съответно от г - н A.A. Кашъмов (750 евро) и г - н A.E. Кашъмов (2000 евро). В подкрепа на тези твърдения те представят договори за правни услуги съответно между Фондацията за достъп до информация и г-н A.E. Кашъмов и между г-н А.Е. Кашъмов и г-н А.А. Кашъмов, таблици с разчет и разписки.

431.  Правителството оспорва стойността на искането за разноски за превод на първия и втория жалбоподатели, както и на искането за адвокатски хонорари на третия и четвъртия жалбоподатели. Според него и двете са прекомерни.

* + - 1. Оценката на Съда

432.  Съгласно практиката на Съда жалбоподателите имат право на възстановяване на разходите и разноските, но само доколкото те са действителни и необходими и са в разумни граници.

433.  В този случай няма основание да се предполага, че разходите за превод и пощенските разходи, заявени от първия и втория жалбоподатели (вж. пар. 429 по-горе), не са действително направени от тях. С оглед на обема на становищата на тези заявители разходите за превод могат също да се разглеждат като необходими и разумни по отношение на квантовата стойност. Следователно те трябва да бъдат изцяло възстановени. Превърнати в евро, тези суми възлизат съответно на 527,65 EUR и 13,04 EUR, което прави общо 540,69 EUR. Към тях следва да се добави всеки данък, който може да бъде начислен на жалбоподателите. По тяхно искане сумите трябва да бъдат внесени по банковата сметка на Екимджиев и Партньори, адвокатската кантора, в която работят техните представители.

434.  С оглед на сложността на повдигнатите по делото въпроси, адвокатските разноски, предявени от третия и четвъртия жалбоподатели (вж. пар. 430 по-горе), също могат да бъдат приети като необходими и разумни по отношение на стойността. Следователно те трябва да бъдат изцяло присъдени, без да се приспадат всички данъци, които могат да бъдат начислени на тези жалбоподатели.

* + 1. Лихва за забава

435.  Съдът счита за целесъобразно лихвеният процент за забава да се основава на пределния лихвен процент на кредитиране на Европейската централна банка, към който следва да се добавят три процентни пункта.

1. ПО ТЕЗИ СЪОБРАЖЕНИЯ СЪДЪТ ЕДИНОДУШНО
2. *Присъединява* възраженията на правителството по отношение на статута на жертва на жалбоподателите и изчерпването на вътрешноправните средства за защита във връзка с оплакването относно системата за тайно наблюдение към разглеждането по същество и ги *отхвърля*;
3. *Присъединява* възраженията на правителството по отношение на статута на жертва на жалбоподателите и изчерпването на вътрешноправните средства за защита във връзка с оплакването относно задържането и последващия достъп до трафични данни към разглеждането по същество и ги *отхвърля*;
4. *Обявява* жалбата за допустима;
5. *Приема*, че е налице нарушение на чл. 8 от Конвенцията по отношение на системата за използване на специални разузнавателни средства в България;
6. Приема, че е налице нарушение на член 8 от Конвенцията по отношение на системата за задържане и последващ достъп до трафични данни в България;
7. Приема, че констатираните нарушения сами по себе си представляват достатъчно справедливо удовлетворение за всяка неимуществена вреда, понесена от четиримата жалбоподатели поради констатираните по делото две нарушения на член 8 от Конвенцията;
8. *Приема,*
   1. че държавата ответник трябва да заплати на жалбоподателите в срок от три месеца от датата, на която това решение стане окончателно, в съответствие с чл. 44, ал. 2 от Конвенцията, следните суми във връзка с разходи и разноски, които трябва да се конвертират във валутата на държавата ответник по курса, приложим към датата на изплащане:
      1. съвместно на първия и втория кандидат 540,69 евро (петстотин четиридесет и четири евро и шестдесет и девет цента), плюс всеки данък, който може да им бъде начислен, да бъдат внесени по банковата сметка на Екимджиев и Партньори, адвокатската кантора, в която работят представителите на тези жалбоподатели;
      2. на третия жалбоподател - 750 EUR (седемстотин и петдесет евро) плюс данъка, който може да му бъде начислен;
      3. на четвъртия жалбоподател - 2 000 EUR (две хиляди евро) плюс всички данъци, които могат да му бъдат начислени;

(б) че от изтичането на горепосочените три месеца до изплащането, върху горепосочените суми се дължи проста лихва при лихвен процент, равен на пределния лихвен процент на Европейската централна банка през периода на неизпълнение, към който се добавят три процентни пункта;

1. *Отхвърля* останалата част от иска на жалбоподателите за справедливо удовлетворение.

Съставено на английски език и съобщено писмено на 11 януари 2022 г. съгласно правило 77, параграфи 2 и 3 от Правилника на съда.

Андреа Тамиети Тим Айке  
 Секретар Председател

1. Съществува малка разлика между двата списъка: престъплението по чл. 320, ал. 2 от Наказателния кодекс (явно подбуждане към терористичен акт или приготовление към престъпление) фигурира в чл. 3, ал. 1 от Закона от 1997 г., но не и в чл. 172, ал. 2 от Наказателно-процесуалния кодекс. [↑](#footnote-ref-1)
2. Член 2 от Закона за управление и функциониране на системата за защита на националната сигурност от 2015 г. определя „националната сигурност“ като „динамично състояние на обществото и държавата, при което са защитени териториалната цялост, суверенитетът и конституционно установеният ред на страната, когато са гарантирани демократичното функциониране на институциите и основните права и свободи на гражданите, в резултат на което нацията запазва и увеличава своето благосъстояние и се развива, както и когато страната успешно защитава националните си интереси и реализира националните си приоритети“. [↑](#footnote-ref-2)
3. Тази дирекция е част от Комисията за противодействие на корупцията и за отнемане на незаконно придобито имущество (вж. *Тодоров и др. срещу България*, № 50705/11 и 6 други, § 92, 13 юли 2021 г.). [↑](#footnote-ref-3)
4. Между 2013 г. и 2015 г. правилото гласи, че съдията може да поиска представянето на тези материали (член 15, ал. 2 от Закона от 1997 г., в редакцията между м. август 2013 г. и м. юни 2015 г.). [↑](#footnote-ref-4)
5. Изглежда, че несъответствието е възникнало, тъй като формулировката на член 174, ал. 4 от Кодекса все още съвпада с тази на член 15, ал. 2 от Закона от 1997 г. преди изменението му през юни 2015 г. (те бяха изменени паралелно през август 2013 г.), тъй като изменението от юни 2015 г. се отнасяше само до член 15 от Закона от 1997 г. [↑](#footnote-ref-5)
6. Специализираният наказателен съд започва да функционира през 2012 г. (вж. параграф 46 по-горе). [↑](#footnote-ref-6)
7. Няма публично достъпни данни за общия брой на издадените разрешения за използване на СРС в България през 2012 и 2013 г. [↑](#footnote-ref-7)
8. Между юни 2015 г. и ноември 2017 г. този срок е бил седемдесет и два часа (чл. 15, ал. 1 в редакцията между м. юни 2015 г. и м. ноември 2017 г.). Между м. август 2013 г. и м. юни 2015 г. в чл. 15 не са предвидени никакви срокове. Преди м. август 2013 г. съгласно член 15, ал. 2, в редакцията след първоначалното влизане в сила на закона през 1997 г., от съдията се изисква да се произнесе по искането за използване на СРС „веднага след получаването му“. [↑](#footnote-ref-8)
9. Член 174, ал. 4 (ал. 3 преди 2011 г.) от Наказателно - процесуалния кодекс, в редакцията между първоначалното му влизане в сила през 2005 г. и м. август 2013 г., също изисква от съдията да се произнесе по искането за използване на СРС „веднага след получаването му“. [↑](#footnote-ref-9)
10. В първия си годишен доклад за 2014 г. Националното бюро посочва (на стр. 11 - 15), че 184 от тези искания е трябвало да бъдат отхвърлени от съответните съдии, тъй като са опорочени от нередности. В последващите си доклади Бюрото не прави подобен анализ. [↑](#footnote-ref-10)
11. Терминът, използван от закона, е „два месеца“ (вж. параграф 79 буква в) и бележка под линия 12 по-долу). [↑](#footnote-ref-11)
12. До 2015 г. срокът във всички случаи е до два месеца, с възможно удължаване до шест месеца (член 21, ал. 1 и 2 от Закона от 1997 г., в редакцията между 1997 г. и 2015 г.). [↑](#footnote-ref-12)
13. Общото правило в член 36 от Закона за защита на класифицираната информация от 2002 г. е, че никое длъжностно лице няма достъп до класифицирана информация, освен ако не притежава подходящо ниво на достъп до нея. Заемащите редица други длъжности (президент на републиката, министър-председател, председател на парламента, министри от правителството, главен секретар на Министерския съвет, народни представители, конституционни съдии, съдии, прокурори, следователи, членове на Висшия съдебен съвет и членове на неговия Инспекторат, както и адвокати с частна практика) обаче не подлежат на такъв контрол и получават разрешение за достъп до всички нива на класифицирана информация (при спазване обаче на принципа „необходимост да се знае“ за всички тях, с изключение на президента на републиката, министър-председателя и председателя на парламента) автоматично, когато поемат задълженията си (чл. 39, ал. 1 - 3 от същия закон). [↑](#footnote-ref-13)
14. [whttp://www.nbksrs.bg/за-нас/състав-на-бюрото/](http://www.nbksrs.bg/за-нас/състав-на-бюрото/) (разглеждано на 30 юли 2021 г.) [↑](#footnote-ref-14)
15. Той има висяща жалба пред Съда във връзка с тези въпроси (№ 34584/18), в която повдига оплаквания по членове 8 и 10 от Конвенцията относно освобождаването си от длъжност и по член 6 §1 от Конвенцията поради твърдяна несправедливост характе на производството, в което е оспорил отнемането на разрешението за достъп. [↑](#footnote-ref-15)
16. Годишният доклад на Комисията за 2021 г., който следва да съдържа статистическите данни за 2020 г., все още не е публикуван. [↑](#footnote-ref-16)
17. В годишния си доклад за 2015 г. комисията заключава(на стр. 91), че малкият брой доставчици на комуникационни услуги, които ѝ докладват във връзка със запазването на данни, вероятно се дължи на тълкуването на закона от страна на доставчиците като изискващ от тях да докладват само ако са получили искане за достъп от органите през отчетния период. [↑](#footnote-ref-17)
18. За определението за „тежко престъпление“ по българското законодателство вж. параграф 18 по-горе. [↑](#footnote-ref-18)
19. Вж. бележка под линия 3 по-горе. [↑](#footnote-ref-19)
20. Сумата от броя на разрешенията за достъп и на решенията за отказ на заявления за достъп всяка година е по-голяма от годишния брой на заявленията (вж. таблицата в точка 170 по-горе), тъй като ако дадено заявление за достъп се отнася до данни, съхранявани от няколко доставчици на комуникационни услуги, някои съдилища издават отделно разрешение за достъп на всеки от тези доставчици. [↑](#footnote-ref-20)
21. Годишният доклад на Комисията за 2021 г., който следва да съдържа статистическите данни за 2020 г., все още не е публикуван. [↑](#footnote-ref-21)
22. Изискването за докладване пред Европейската Комисия изглежда е останало от член 10, параграф 1 от Директивата относно запазване на данните (вж. точка 232 по-долу). [↑](#footnote-ref-22)