JUDICIAL REVIEW OF THE SECURITY SECTOR - A GUARANTEE FOR HUMAN RIGHTS PROTECTION

Svetlin E. Stefanov

*Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences,
Department "Management of Security Systems", svetlin.stefanov65@abv.bg*

***Abstract**: Accountability for the work of the Security Sector is exercised through the control of various actors, including the judiciary, expert bodies, parliamentary committees and data protection authorities. This control is crucial: it helps to ensure that services are accountable for their actions, and encourages the development of effective internal safeguards within the services. Control is not a lack of confidence, but a desire to make things clear.*

***Keywords**: Judicial review, Security Sector, Human Rights Protection*

СЪДЕБНИЯТ КОНТРОЛ ВЪРХУ СЕКТОРА ЗА СИГУРНОСТ – ГАРАНЦИЯ ЗА ЗАЩИТА ПРАВАТА НА ГРАЖДАНИТЕ

Светлин Е. Стефанов

Въведение

Отчетност върху работата на сектор „Сигурност" се осъществява чрез контрол от различни субекти, включително съдебната власт, експертни органи, парламентарни комисии и органи за защита на данните. Този контрол е от решаващо значение: той спомага да се гарантира, че службите носят отговорност за своите действия, и насърчава развитието на ефективни вътрешни предпазни механизми в рамките на службите. Контролът не е липса на доверие, а желание нещата да са ясни.

Контролът е част от управленческия процес и има за цел да провери дали определена система е в нужните параметри, за да изпълнява предназначението и функциите си. В зависимост от гледната точка и функциите си, контролът бива външен и вътрешен; предварителен, ат-хок и последващ; финансов, одитен, функционален или с цел сертифицирането на дадено звено за определен вид дейности и т.н.

Изложение

Според чл. 21 от Закона за управление и функциониране на системата за защита на националната сигурност, върху дейността на органите и структурите от системата за защита на националната сигурност се осъществява парламентарен, административен, съдебен и граждански контрол [1].

Контролът в службите за сигурност се осъществява на няколко нива както следва:
- ръководител на служба за сигурност;
- изпълнителна власт;
- съдебна власт и прокуратура;
- парламентарен контрол;
- контрол от гражданския сектор, осъществяван от граждани и неправителствени организации /НПО/.

Специализираните парламентарни комисии обикновено акцентират върху оценяването на правителствените политики в сектора. Органите за защита на данните разполагат с правомощия над сектор сигурност – главно поради залегналото в законодателството провомощие за контрол при използване на личните данни.

Съдебната власт и експертните органи участват най-често в контрола върху мерките за наблюдение. Съдебният контрол обхваща използването на специални разузнавателни средства от институциите в сектора за сигурност, прилагането на решенията на Европейския съд за правата на човека, тълкувателни решения на върховните съдилища, решения на Конституционния съд и решения на други съдилища, компетентни да разглеждат съответните дела.

Законодателна дейност в Република България се осъществява прозрачно и с обществено обсъждане, законът винаги се публикува и става известен на всички, преди да започне прилагането му. Самото създаване и развиване на правна рамка за дейността на службите за сигурност неизбежно ги поставя в положение на по-голяма прозрачност. Това означава и контрол – от политическото представителство в държавните институции, от една страна и пряко от гражданите – от друга [2].

Правилата за опазване на държавната тайна днес са прозрачни и общодостъпни чрез обнародвания Закон за защита на класифицираната информация (обн. ДВ, бр. 45 от 30.04.2002 г.). Процедурата по опазване на държавната тайна на Република България бе ревностно опазвана от обществения поглед дори през 2002 г., когато „Програма достъп до информация" (ПДИ) я поиска по реда на Закона за достъп до обществена информация. Министерският съвет разсекрети документа, в който се съдържаха тези правила, едва през 2004 г. под натиска на заведеното във Върховния административен съд дело срещу отказа (а.д. № 11243/2003 г. по описа на ВАС петчленен състав).

През 2009 г. Европейският съд по правата на човека, промени предишната си практика, според която чл. 10 от Европейската конвенция за правата на човека (ЕКПЧ) не задължава държавите да предоставят информация на желаещите да я получат. В същата година бе отворена за подписване и ратификация от държавите, членки на Съвета на Европа, първата в света Конвенция за достъпа до официални документи. През 2013 г. Комитетът на министрите на държавите, членки на Съвета на Европа, прие Препоръка относно националната сигурност и достъпа до информация, последвана от резолюция на Парламентарната асамблея, към държавите членки да подобрят баланса между правото на обществото да знае и защитата на легитимните интереси на националната сигурност. През 2015 г. бе приета резолюция на ПАСЕ и съответно препоръка относно подобряване на защитата на информаторите (whistleblowers), която се позовава на посочения документ и реферира изрично към случая „Сноудън". Достъпът на гражданите до информация и защитата на личните им данни са неразривно свързани. Често се сочи, че тези права представляват двете страни на една и съща монета. В демократичните общества по правило гражданите имат широк достъп до информацията, която се съхранява от институциите, а последните имат ограничен достъп до данните на гражданите.

Правната уредба при използване на специални разузнавателни средства от институциите в сектора за сигурност след 1990 г. :

С разпоредбата на чл. 34 от Конституцията от 1991 г. бе гарантирано правото на неприкосновеност на кореспонденцията и другите съобщения. Според алинея втора от тази разпоредба намесата в това право може да е осъществявана единствено с разрешение на орган на съдебната власт, когато е наложително за предотвратяване или разкриване на тежки престъпления. През 1994 г. е приет първият Закон за специалните разузнавателни средства (ЗСРС). През 1997 г. е от-

менен с новоприетия и сега действащ ЗСРС. Основен принцип на закона е използването на СРС след издаване на съдебно разрешение. Изключение от този принцип е допустимо само при непосредствена опасност за извършване на тежко умишлено престъпление или за националната сигурност. Непосредствено след приемането на ЗСРС (1997 г.) е поставен въпросът за конституционосъобразността на отделни разпоредби. Главния прокурор поставя четири въпроса, по които се произнася Конституционният съд. Това са съответства ли на Конституцията: 1. съществуването на хипотеза в ЗСРС, при която съдът се произнася впоследствие, а не преди използването на специалното разузнавателно средство (СРС)? 2. правомощието на министъра на вътрешните работи да прекрати прилагането на СРС преди срока? 3. правомощието на министъра на вътрешните работи да вземе решение за използване на СРС при получаване на резултати извън направеното искане? 4. задължението на министъра на вътрешните работи да осъществява контрол по използването на СРС? С решение от 1998 г. Конституционният съд отхвърля искането [3].

През 2001 г. е изготвен доклад от ВКП относно използването на СРС през периода 1999-2000 г. Според доклада през периода януари 1999 – януари 2001 г. съдилищата са разрешили използването на СРС в 10 000 случая, като за изготвяне на доказателства в наказателни производства са послужили едва 2 – 3 % от тях. Данните са цитирани в решение на Европейския съд по правата на човека от 28 юни 2007 г. [4]. Достъп до доклада бе отказан по реда на ЗДОИ на Българския хелзинкски комитет (БХК), като за основание за отказ прокуратурата посочи обстоятелството, че е маркиран с гриф за сигурност „за служебно ползване" и представлява служебна тайна. Състави на Софийския градски съд и на Върховния административен съд отхвърлиха жалбата на БХК, подадена със съдействието на „Програма достъп до информация" (ПДИ), като се позоваха на чл. 33 от ЗСРС, според който информацията за факти и сведения за прилагането на СРС по реда на закона, както и събраните данни не подлежат на разгласяване. Отхвърлен е доводът, че междувременно е изтекъл предвиденият в ЗЗКИ срок с мотива, че декласифицирането се извършва само от компетентния служител [5].

През 2000 г. въпросът за съобразността на ЗСРС с Конвенцията за защита правата на човека и основните свободи бе поставен в Страсбург [6]. С решение на ЕСПЧ от 28 юни 2007 г. (окончателно от 30 януари 2008 г.) по делото на „Асоциация за европейска интеграция и права на човека и Екимджиев срещу България" [7] редица положения от ЗСРС бяха обявени за водещи до системно нарушение на чл. 8 от Европейската конвенция за правата на човека, според който всеки има право на зачитане на личния му живот и кореспонденция. В решението на ЕСПЧ се отбелязват редица дефекти в системата за тайно следене, установена със ЗСРС, които водят до системно нарушение на правата на гражданите по чл. 8 от ЕКПЧ. Отбелязва се липсата на независима институция, осъществяваща контрол върху дейността по прилагането на СРС, извън министъра на вътрешните работи. Посочена е липсата на орган, който да проверява спазват ли се условията в разрешенията за използване на СРС, добросъвестно ли се възпроизвеждат оригиналните данни в писмените записи и унищожават ли се в срок тези данни. Липсват правилници, определящи със съответната степен на точност начина на проверка на данните, получени чрез използване на специални разузнавателни средства, или процедурите за запазване на тяхната цялост и поверителност и процедурите за тяхното унищожаване. Не е описан начинът, по който министърът на вътрешните работи осъществява контрол. Съдията, издал разрешението, не се уведомява впоследствие за резултатите от използването на СРС и не осъществява последващ контрол върху законосъобразността му. Нито министърът, нито някое друго длъжностно лице е задължено да докладва редовно на независим орган или на обществото за цялостното функциониране на системата или за мерките, прилагани в отделни случаи. Ако събраните данни попадат извън обсега на искането за използване на специални разузнавателни средства, министърът на вътрешните работи е този, който решава, по свое усмотрение и без никакъв независим контрол, какво трябва да бъде направено с тях. Не на последно място, в коментираното решение ЕСПЧ отбелязва, че съгласно българския закон лицата, по отношение на които са използвани специални разузнавателни средства, не са уведомявани за този факт по никое време и при никакви обстоятелства. По този въпрос

жалби подават в Страсбург и други български граждани. България е осъдена за същото нарушение на чл. 8 на ЕКПЧ и по делата „Хаджиев с/у България" и „Нацев с/у България" [8].

Законодателни изменения в ЗСРС през 2008 – 2009 г. В резултат на решението на ЕСПЧ бе предприето изменение в закона. С изменението и допълнението на ЗСРС през 2008 г. се създаде Национално бюро за контрол над специалните разузнавателни средства. Бюрото просъществува едва няколко месеца, като при смяната на политическата власт през 2009 г. с ново изменение и допълнение на ЗСРС контролът бе предоставен на създадена парламентарна подкомисия към Комисията по правни въпроси. Националното бюро за контрол на СРС бе отново създадено през 2013 г., като смяната на властта след изборите през октомври 2014 г. не доведе до рокада на състава. С изменението през 2009 г. се въведе задължение за последващо информиране на съдията, дал разрешението за прилагане на СРС. Той обаче не се произнася по законността на това прилагане. Създаде се парламентарна подкомисия към Комисията по правни въпроси, която да осъществява контрол, основно като събира информация и подготвя годишен доклад по въпросите на прилагането на СРС. Подкомисията не бе натоварена с функции да налага санкции, но получи правомощието да информира гражданите за незаконно прилагане на СРС спрямо тях. С изменение в Закона за отговорността на държавата и общините за вреди се предвиди възможност да се търси обезщетение за незаконно приложени СРС. Промените бяха в правилната посока, но развитието през следващите години показа, че не са достатъчни.

Изменения на ЗСРС през 2013 – 2019 г. В резултат на активния дебат през годините ЗСРС бе изменен и допълнен през 2013, 2015, 2016, 2017, 2018 и 2019 г. С измененията от 2013 г. на ЗСРЗ Националното бюро за контрол над СРС е определено като постоянно действащ орган за външен контрол по приложението на ЗСРС. Създадено бе изискване в исканията за разрешаване на СРС да се включва пълно и изчерпателно посочване на фактите и обстоятелствата, даващи основание да се предполага, че се подготвя, извършва или е извършено тежко умишлено престъпление. Бяха изчерпателно изброени престъпните състави, съставляващи тежки престъпления, за разследването на които може да се използват СРС, с което се стесни законово допустимото приложение на намесата в личното пространство по реда на ЗСРС. Освен определянето на срок за използването на СРС, се предвиди задължение за мотивиране на продължителността му. Мотивите трябва да съдържат и обосновка за невъзможността необходимите данни да бъдат събрани по друг начин или описание на изключителните трудности, с които е свързано събирането им. През 2013 г. се обособи като самостоятелна дейността по техническото прилагане на СРС и особено на подслушванията, които са най-големият дял от тях. За целта бе създадена отделна институция на изпълнителната власт, пряко подчинена на Министерския съвет – Държавна агенция „Технически операции" (ДАТО). При изключението, според което СРС може да се използват преди разрешението от съда, решението се взема от председателя на ДАТО, ДАНС или секретаря на МВР. Целта очевидно е да се неутрализира силната политическа фигура на министъра на вътрешните работи.

Статистика относно използването на СРС. През годините неколкократно се стигна до скандали, твърдения или данни за подслушване със съмнителна законност. Още през 2001 г. се коментираше монтирането на подслушвателно устройство в дома на тогавашния главен прокурор и разработката „Гном". Един от най-нашумелите скандали с подслушване през 2008 г. бе свързан с разработка под названието „Галерия" на ДАНС, по която обект на подслушване са били журналисти и политици. Скандали около подслушванията имаше по време на първото правителство на ГЕРБ (2009 – 2013 г.), като за основно отговорна политическа фигура се сочеше тогавашният министър на вътрешните работи Цветан Цветанов, впоследствие подсъдим за отказ да бъдат използвани разрешени от съда СРС. Всяка следваща година се увеличаваше бройката на разрешенията за използване на СРС. В доклада на прокуратурата от 2001 г. са отчетени 10 000 разрешения за периода 1999 – 2000 г., т.е. средно по 5000 годишно. В решението си от 2008 г. ЕСПЧ сравнява тази бройка с данните за Великобритания, показващи цифрата 400 за телефонни подслушвания и 100 за отваряне на кореспонденция. Десет години по-късно, т.е. за 2009 г., новосъздадената парламентарна подкомисия докладва 9600 разрешения у нас. Това показва, че разрешенията са се удвоили за период от десет години. През 2010 г. се оказва, че броят на разрешенията за прилагане

на СРС стига до рекордното число от 15 864. За следващата 2011 г. те са около 14 000, като в доклада на подкомисията изрично се подчертава, че намалението е изкуствено – вследствие на включването на повече способи в едно искане по инициатива на председателя на Софийския градски съд Владимира Янева. За сметка на това броят на лицата, спрямо които са приложени СРС през 2011 г., е с 30 % по-голям от този през 2010 г. Съществено за всички тези данни за периода 1999 – 2011 г. е, че броят на използваните в съда доказателства, събрани чрез СРС, е изключително малък като процент от общия брой на разрешените – 2 – 3 % през 1999 – 2000 г. и 5 – 6 % през 2011 г. В Доклада на Националното бюро за контрол над СРС от 2015 г. не се сочи броя на разрешенията, а брой на „лицата, поставени под секретен контрол". За 2014 г. броят им е 4202, за 2013 г. – 4452, за 2012 г. – 5902, за 2011 г. – 8184, а за 2010 г. – 5763. Изводът на бюрото е, че след 2011 г. има тенденция към намаляване на броя на лицата, спрямо които са използвани СРС. Доминиращата форма на прилагане на СРС през всичките години са подслушванията. За 2014 г. са издадени 6475 разрешения за подслушване. От тях реално приложени са 4927, т.е. доста по-малък брой. Изводът е, че се ползва възможно най-дълбоко навлизащото в личното пространство средство, а резултатите от него не са значителни (следва да се има предвид, че липсва статистика колко от делата са приключили с осъдителна присъда).

В доклада на Националното бюро за контрол на специалните разузнавателни средства за извършената дейност през 2017 г. [9] и 2018 г.,[10] се посочва, че през 2017 г. са осъществени процедури със СРС по отношение на 2748 лица, през 2016 г. на 2749 лица. Наблюдава си трайна тенденция към намаляване на броя на лицата, контролирани със СРС, спрямо предходни години. Поисканите за прилагане оперативни способи са общо 17714 бр. като през 2016 г. те са били 14382 бр. В Доклада са отразени броя на поисканите видове оперативни способи. В 261 случая СРС са използвани по отношение на обекти за установяване самоличността на лица, за които е имало данни за участието им в престъпна дейност, съгласно чл. 12, ал. 1, т. 4 от ЗСРС. За 640 лица прилагането на СРС е започнало по реда и условията на чл. 17 от ЗСРС и за 28 лица по чл. 18 от ЗСРС. През 2016 г. лицата са били съответно 685 и 49. През 2017 г. исканията за използване на СРС са 5939, по които са постановени 1315 откази и 4624 разрешения. Националното бюро е констатирало, че през 2017 г. съдебният контрол върху използването и прилагането на СРС е значително завишен, за което свидетелства по-големият брой и добре мотивирани откази. По отношение на информацията, не послужила за изготвяне на веществени доказателствени средства е направен извод, че същата се унищожава в законоустановения срок, в резултат на своевременно упражняван контрол от ръководителите на органите по чл. 13 и 20 от ЗСРС. В резултат на прилагане на СРС са изготвени 1670 бр. веществени доказателствени средства, при 1431 бр. през2016г.

През 2018 г. са използвани СРС по отношение на 3046 лица. Поисканите за прилагане оперативни способи са общо 16002 бр. В Доклада са отразени броя на поисканите видове оперативни способи. В 279 случая СРС са използвани по отношение на обекти за установяване самоличността на лица, за които е имало данни и основание да се предполага, че подготвят, извършват или са извършили тежко умишлено престъпление по чл. 12, ал. 1, т. 4 от ЗСРС, чиито анализ на данни показва относителна стабилност на тези специфични процедури. За 607 лица прилагането на СРС е започнало по реда и условията на чл. 17 от ЗСРС и за 7 лица по чл. 18 от ЗСРС. През 2018 г. исканията за използване на СРС са 6099, по които са постановени 771 откази и 5328 разрешения. Запазва се тенденцията СРС да се използват най-често за разкриване на престъпления по чл. 321 от НК /организирана престъпна група/, чл. 354а от НК /наркотични вещества/, чл. 234 от НК /акцизни стоки/, чл. 209 от НК /измама/, чл. 195 от НК /кражби/ и чл. 301 от НК /подкуп/. Запазва се относителният дял на заявителите към общия брой инициирани процедури - МВР, Прокуратура, ДАНС и СВП-МО. Информацията, не послужила за изготвяне на веществени доказателствени средства се унищожава в законоустановения срок, а изготвените веществени доказателствени средства са 1714 бр., което увеличение свидетелства за ефективността на прилаганите СРС.

Достъп до данни за трафика съгласно Закона за електронните съобщения. Запазване на данните за трафика на електронни съобщения и осигуряване на пряк достъп до тези данни съгласно Наредба № 40 от 2008 г.

С развиването на технологиите нарасна възможността за използването на данни за електронните съобщения, обменяни чрез мобилните оператори и доставчиците на интернет услуги, за целите на борбата с престъпността. Преди създаването на нарочна нормативна уредба осигуряването на възможност за такъв достъп до базите данни бе включено в изискванията към лицензиите на мобилните оператори. През 2006 г. се прие директива на Европейския парламент и на Съвета за запазването на данни за трафика на електронни съобщения, с която бяха задължени държавите, членки на Европейския съюз (ЕС), да приемат законодателство, чрез което да осигурят запазването на данни за трафика на електронни съобщения за период между 6 и 24 месеца. Целта на хармонизирането на законодателството на държавите, членки на ЕС, бе да се гарантира, че данните са достъпни за разследването, разкриването и преследването на сериозни престъпления, както те са определени в националното право на всяка държава членка.

През януари 2008 г. директивата бе въведена в българското законодателство чрез наредба, издадена съвместно от министъра на вътрешните работи и председателя на Държавната агенция за информационни технологии и съобщения [11]. За разлика от директивата в наредбата е определен много по-широк обхват на престъпленията, за разкриването на които се създава задължението за запазване на данните, свързани с трафика на електронни съобщения, и ред за достъпа до тях. В наредбата се посочва, че запазването и достъпът до данните са просто с цел „разкриване на престъпления", без да се ограничат до категорията „сериозни престъпления", както това е сторено в директивата. Другата цел на запазването и достъпа до данни е формулирана пределно общо – „за нуждите на националната сигурност", като такава цел не е заявена въобще в директивата. С чл. 5 от Наредба № 40/2008 г. бе предвидена възможност органите на досъдебното производство или съда и службите за сигурност да получават достъп при обикновено писмено поискване, без предварително разрешение от съдебен орган. От друга страна, дирекция в МВР придоби възможността да получи неограничен пряк технически достъп до данните за трафика на електронни съобщения чрез компютърен терминал.

Тълкуването на съобразността на Наредба № 40/2008 г. с Конституцията и ЕКПЧ Наредба №40/2008г., приетото от Върховния административен бе оспорена от „Програма достъп до информация" (ПДИ) пред Върховния административен съд с аргументи за противоречие с Конституцията и Европейската конвенция за правата на човека. Тричленният състав на ВАС обяви жалбата за допустима, но я отхвърли по същество като неоснователна. С решение от 11 декември 2008 г., постановено по касационна жалба на ПДИ, петчленен състав на ВАС отмени изцяло чл. 5 от наредбата, отнасящ се до регламентирането на достъпа на държавни органи до запазваните данни за трафика на електронни съобщения [12]. Съдът приема по отношение на разпоредбата, предвиждаща достъп на дирекция в МВР чрез компютърен терминал, че всъщност нормата „не поставя никакви ограничения по отношение данните, до които се разрешава достъпът чрез компютърен терминал, а изразът „за нуждите на оперативно-издирвателната дейност" е много общ и не дава гаранции за спазване на чл. 32, ал. 1 от Конституцията на Република България, че личният живот на гражданите е неприкосновен. Не е установен способ за съблюдаване конституционния принцип по отношение правото на защита срещу незаконна намеса в личния и семейния живот на отделната личност, както и срещу посегателство върху неговата чест, достойнство и добро име". Що се отнася до регламентирана възможност разследващите органи, прокуратурата и съдът да получават достъп до данни за трафика „за нуждите на наказателния процес", а службите за сигурност – „в случай на необходимост, свързана с националната сигурност", след представяне на писмено искане, петчленният състав на ВАС намира, че формулираният текст не поставя условия, препятстващи злоупотреба с възможността да се нарушават конституционно гарантирани права на гражданите, като не е предвидено препращане към специалните закони Наказателнопроцесуален кодекс, Закон за специалните разузнавателни средства, Закон за защита на личните данни, в които са конкретизирани предпоставките за допускане достъп до определени данни, свързани с личния живот и личните данни на отделната личност. Като извод съдът намира, че трите алинеи на чл. 5 от Наредба № 40/2008 г. нарушават чл. 32 и чл. 34 от Конституцията и чл. 8 от ЕКПЧ.

Законова регламентация на запазването и достъпа до данни за трафика на електронни съобщения. След отмяната на чл. 5 от Наредба № 40/2008 г. през януари 2009 г. започна обсъждане в парламента на внесени текстове за изменение и допълнение на Закона за електронните съобщения (ЗЕС). Бе въведен задължителен съдебен контрол, като за всеки индивидуален достъп до данни за трафика следва да се поиска отделно разрешение от окръжния съд. Кръгът на престъпленията, за чието разкриване и разследване се допускаше достъп до трафични данни, бе стеснен до категориите „тежки" и „компютърни" престъпления. Срокът за запазване на данните бе определен на 12 месеца. След парламентарните избори през 2009 г. администрацията на новия министър на вътрешните работи изготви нов проект за изменение и допълнение на ЗЕС, насочен към улесняване на достъпа на органите на Министерството до данни за трафика на електронни съобщения. След обсъждания през 2010 г. бе приет нов вариант на текстовете на ЗЕС, отнасящи се до запазването и достъпа до данни за трафика на електронни съобщения. Той отново не предвиждаше пряк технически достъп до запазените данни. Предвиди се по-широк кръг от органи, имащи възможност да поискат достъп до трафични данни. Бе регламентирано данните за целите на оперативната дейност да се предоставят след разрешение от районния съд, а за целите на разследването на престъпления – по реда на Наказателнопроцесуалния кодекс. Кръгът на престъпленията, за чието разкриване и разследване се допуска достъп до трафични данни, бе отново разширен, като освен категорията „тежки престъпления" бе включена и категорията компютърни престъпления.

Статистика относно достъпа до данни за трафика на електронни съобщения. Според информация от парламента през 2008 г. органите на МВР са получили около 300 000 разпечатки с данни за трафика на електронните съобщения на около 40 000 абоната [13]. С измененията и допълненията в ЗЕС от 2010 г. обаче се позволи по-широк достъп при по-нисък стандарт на защита и гарантиране на правата на хората. Според официалния доклад на компетентната парламентарна подкомисия за периода от 1 януари до 9 май 2010 г., когато действа режимът на достъп, приет с измененията и допълненията на ЗЕС от 2009 г., броят на разрешенията за достъп е 2760, докато за периода от 10 май 2010 г., когато влизат в сила новите изменения и допълнения в ЗЕС, до 31 декември 2010 г. броят им вече е 18 845. Част от измененията в закона създават възможност за заобикаляне на режима за достъп до трафични данни само след съдебно разрешение. Още през 2010 г. прокуратурата приема тълкуване, според което не е необходимо съдебно разрешение, когато достъпът до данни за трафика на електронни съобщения е необходим за целите на разследването на тежки и компютърни престъпления. Действително, с редакцията от 2010 г. по отношение на тези случаи ЗЕС препраща към реда по НПК. Последният оправомощава съда или органите на досъдебното производство да искат от лица да им предадат намиращите се у тях данни, включително „за трафика". Според официалния доклад на компетентната парламентарна подкомисия за 2011 г. в 58 702 случая достъп до данни по ЗЕС е предоставен по реда на НПК (тоест без съдебно разрешение), а след съдебно разрешение по реда на чл. 250б, ал. 1 от ЗЕС е предоставен едва в 15 350 случая. След промените в ЗЕС през 2010 г. броят на разрешенията за достъп до данни по ЗЕС сериозно расте – от общо 20 605 разрешения през 2010 г. числото се увеличава на общо 74 052 през 2011 г., т.е. само за една година броят е нараснал повече от три пъти.

Решения на Съда на Европейския съюз и Конституционния съд. През април 2014 г. Съдът на Европейския съюз обяви Директива 2006/24/ ЕО за невалидна [14]. Според мотивите на съда е налице несъответствие на директивата с разпоредбите на чл. 7, чл. 8 и чл. 52, § 1 от Хартата на основните права на Европейския съюз. През същата година омбудсманът внесе в Конституционния съд на Република България искане за обявяване на разпоредбите в ЗЕС, които въвеждат Директива 2006/24/ЕО, за несъответни на Конституцията. Като заинтересовани страни бяха конституирани държавни органи и неправителствени организации. С решение от март 2015 г. Конституционният съд обяви за противоконституционни всички отнасящи се до запазването на данни за трафика и достъпа до тях разпоредби от ЗЕС [15]. Според Конституционния съд е възможно материята да бъде уредена по начин, който е съвместим с основния закон. Това означава държавната намеса, изразяваща се в задължението за запазване на данни за трафика и възможността за

достъпа до тях, да е уредена със закон, да е в рамките на предвиденото с основния закон изключение, да е подчинена на легитимна/и цел/и от общ интерес. В решението се приема, че запазването на всички данни за трафика на гражданите без оглед евентуалното им участие в престъпна дейност, не е непропорционална мярка, за разлика от срока на запазването. Той е прекомерно дълъг според съда, тъй като натрупването на едногодишна база данни от комуникационен трафик позволява тяхното използване не само за изготвянето на подробен личностен профил (с всички проблеми, които това създава), но и постигане на точна и детайлна диференциация на трайните, обичайни, инцидентни прояви на конкретното лице, неговите контакти, увлечения, интереси, включително с отграничаването на тези, представляващи прецедент в неговото поведение и реакции, а също и систематизиране по различни критерии на местата, които посещава трайно, често, рядко или инцидентно, както и точна идентификация на лицата, с които го прави. Конституционният съд стига до извода, че не са налице необходимите процедурни гаранции за гарантиране на правата на гражданите, като прави съпоставка и с аналогичната уредба на материята, свързана с използването на специални разузнавателни средства. Също така Конституционният съд счита, че оспореното законодателно решение за елиминиране на съдебния контрол в хипотезата на отправено искане за достъп до трафични данни от орган на досъдебното производство (с препратката към реда по НПК) е в противоречие с установените от Конституцията, Европейската харта за правата на човека и КЗПЧОС стандарти. Непосредствено след решението на Конституционния съд бяха приети изменения и допълнения в ЗЕС, които преуредиха материята, свързана със запазването на данни за трафика на електронни съобщения и достъпа до тях [16].

Отказ на достъп до информация по ЗДОИ в случаите на класифицирана информация. Още с приемането на ЗДОИ през 2000 г. бе предвидена възможност за контрол върху законосъобразността на засекретяването на информация. Според приетата регламентация съдът е в правомощието си да изиска съответните доказателства за това, че информацията е законосъобразно засекретена, да ги разгледа в закрито заседание и да се произнася по въпроса. С приемането на Закона за защита на класифицираната информация разпоредбата в ЗДОИ бе съответно редактирана, като контролът се осъществява върху „законосъобразността на маркирането с гриф за сигурност“. В практиката на съдилищата правомощието за изискване на необходимите доказателства се изразява в задължаване на държавната институция ответник да представи по делото съответния класифициран документ [17] Обикновено съдебните състави се фокусират върху процесуалните аспекти на класифицирането на информацията, но не винаги се ограничават само до тях. Следователно разглеждането на основанията за класифициране на документа с оглед въпроса би ли произтекла вреда от широкия достъп до съдържанието му не е изключено от обхвата на съдебния контрол. Изискването на класифициран документ след приключване на устните прения се приема за съществено процесуално нарушение. Следователно възможността на страните да обсъдят констатациите на съда, макар и направени в закрито съдебно заседание, се явява важен елемент от правото на справедлив процес. Непроизнасянето по въпроса дали даден документ, предмет на искане за достъп до информация, е законосъобразно класифициран, след като е бил преглеждан в закрито заседание, е съществено процесуално нарушение [18]

Изводи

От изложеното следва изводът, че законодателството предоставя съществени възможности на гражданите да инициират процедура по преценка на законосъобразността на класифицирането на даден документ като държавна или служебна тайна. Преценката се извършва от независим орган – административен съд, при събиране на необходимите доказателства и спазване на принципа за равенство на страните и състезателност на съдебния процес. Предвидената процедура и практиката по прилагането ú представлява важна гаранция за правата на гражданите и средство за граждански контрол върху законосъобразността на дейността по засекретяване на информация.

References

1. Закон за управление и функциониране на системата за защита на националната сигурност, Обн.ДВ бр.61 от 11 авг.2015 г.
2. Кашъмов, Александър. Съдебен контрол върху сектора за сигурност. В : Границите на секратността. С.,2015 г., с. 56.
3. Решение № 1 от 10 февруари 1998 г. по конституционно дело № 17/1997 г., докладчик конституционният съдия Неделчо Беронов.
4. Решение по делото на „Асоциация за европейска интеграция и права на човека и Екимджиев с/у България”
5. Решение на Софийския градски съд, III-а състав по а.д. № 642/2002 г., оставено в сила от състав на Върховния административен съд, пето отделение, с Решение № 2557/21.03.2005 г. по а.д. № 6362/2004 г.
6. Решение на Софийския градски съд, III-а състав по а.д. № 642/2002 г., оставено в сила от състав на Върховния административен съд, пето отделение, с Решение № 2557/21.03.2005 г. по а.д. № 6362/2004 г.
7. Жалба № 62540/00.
8. Жалба № 22373/2004 и жалба № 27097/2004.Решенията са окончателни от началото на 2013 г
9. Доклад на Националното бюро за контрол на специалните разузнавателни средства за извършената дейност през 2017 г.,, внесен в НС на 31.05.2018 г.
10. Доклад на Националното бюро за контрол на специалните разузнавателни средства за извършената дейност през 2018 г.,, внесен в НС на 30.05.2019 г.
11. Наредба No 40 от 07.01.2008 г. за категориите данни и реда, по който се съхраняват и предоставят от предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, за нуждите на националната сигурност и за разкриване на престъпления.
12. Решение № 13627 от 11.12.2008 г. по адм. д. № 11799/2008 г. (обн., дв, бр. 108 от 2008 г.)
13. Данните бяха публикувани в пресата с източник тогавашния председател на парламентарната правна комисия
14. Решение от 8.04.2014 г. на Съда на Европейския съюз, разширен състав, по съединени дела C-293/12 и C-594/12.
15. Решение № 2 от 12 март 2015 г. по к.д. № 8/2014 г. (обн. ДВ бр. 23 от 2015 г.).
16. Закона за електронните съобщения, Обн. ДВ бр. 24 от 2015 г.
17. Определение от 27 март от 2003 г. по а.д. № 9898/2002 г. на Върховния административен съд, пето отделение, Определение от 22 декември 2005 г. по а.д.№ 4596/2005 г. на Върховния административен съд, пето отделение.
18. Решение № 3875/28.04.2005 г. по а.д. № 592/2005 г. на Върховния административен съд, петчленен състав.