# КОНТРОЛ НА ЕЛЕКТРОННАТА КОМУНИКАЦИЯ ЗА ЗАЩИТА НА НАЦИОНАЛНАТА СИГУРНОСТ

**Огнян Стоичков**

# CONTROL OF ELECTRONIC COMMUNICATION TO PROTECT NATIONAL SECURITY

**Ognyan Stoichkov**

***Резюме**: Изследвано е българското законодателство, част от практиката на ЕСПЧ и на Съда на ЕС за обработване на лични данни в сектора на електронните съобщения и релевантните актове на Европейския съюз, относно контрола на електронната комуникация за защита на националната сигурност.*

*Първият основен проблем е необходимостта от спешна актуализация на нормативната ни уредба, съобразно Решение по дело C 350/21 от 17.11.2022 г. за България, с което Съдът на ЕС постановява, че не допуска национално законодателство, което предвижда превантивно общо и неизбирателно запазване на данни за трафик и на данни за местонахождение, без да гарантира, че лицата, са били уведомени за това в степента, предвидена от правото на Съюза.*

*Вторият проблем е свързан с пределите и съдебният контрол при определяне на националната сигурност, като основание за контрол на електронната комуникация.*

***Ключови думи:** Национална сигурност**,** електронни съобщения, трафични данни, Закон за електронните съобщения, Съд на Европейския съюз.*

***Summary**: The Bulgarian legislation, part of the practice of the ECHR and the Court of the EU for the processing of personal data in the sector of electronic communications and the relevant acts of the European Union, regarding the control of electronic communication for the protection of national security, have been studied.*

*The first main problem is the need for an urgent update of our regulations, in accordance with the Decision in case C 350/21 of 17.11. 2022 for Bulgaria, with which the EU Court ruled that it does not allow national legislation that provides for the preventive general and non-selective retention of traffic data and location data, without ensuring that the individuals have been notified of this to the extent foreseen of Union law.*

*The second problem is related to the limits and judicial control in determining national security, as a basis for control of electronic communication.*

***Key words**: National security, electronic communications, traffic data, Law on electronic communications, Court of Justice of the European Union.*

**УВОД**

Съгласно българското законодателство – чл. 251б, ал. 1 Закона за електронните съобщения (ЗЕС) и чл.159а, ал. 1 Наказателно-процесуалния кодекс (НПК) предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, съхраняват **за срок от 6 месеца данни**, създадени или обработени в процеса на тяхната дейност, които са необходими за: 1. проследяване и идентифициране на източника на връзката; 2. идентифициране на направлението на връзката; 3. идентифициране на датата, часа и продължителността на връзката; 4. идентифициране на типа на връзката; 5. идентифициране на крайното устройство на потребителя или на това, което се представя за негово крайно устройство; 6. установяване на идентификатор на ползваните клетки.

Посочените данни са т.нар. **трафични данни**, справките за които в практиката се определят още като „телефонни разпечатки“. В съюзното право се означават и като **„електронно доказателство“**. Съществена характеристика на тези данни е, че *не съдържат информация за съдържание на комуникацията*, която се придобива само по реда на Закона за специалните разузнавателни средства.

**I. ОБЩ РЕД ЗА ЗАПАЗВАНЕ И ПРЕДОСТАВЯНЕ НА ДАННИ**

**1. По Закона за електронните съобщения**

*1.1. Допустими цели за съхраняване и предоставяне на трафични данни.* Лимитивно изброени в чл. 251б, ал. 2 ЗЕС:

- за нуждите на националната сигурност;

- за предотвратяване, разкриване и разследване на тежки престъпления;

- за предотвратяване на тежки престъпления в рамките на оперативно - издирвателната дейност по реда на глава девета от Закона за противодействие на корупцията;

- за издирване на обявено за общодържавно издирване лице, което е осъдено за тежко престъпление на лишаване от свобода с влязла в сила присъда, чието изпълнение на наказанието не е отложено по реда на чл. 66 Наказателния кодекс (НК) и присъдата не е приведена в изпълнение, или което е изпаднало или може да изпадне в положение, поставящо в риск живота или здравето му;

- за издирване и спасяване на лица в случаите по чл. 38, ал. 3 от Закона за защита при бедствия. (само данните по чл. 251б, ал. 1, т. 6 )

*1.2. Компетентни органи, които могат да искат справка*.

Съгласно чл. 251в ЗЕС оправомощените органи са: 1. специализираните дирекции, териториалните дирекции и самостоятелните териториални отдели на ДАНС; 2. Главна дирекция „Национална полиция“, Главна дирекция „Борба с организираната

престъпност“ и териториалните ѝ звена, Главна дирекция „Гранична полиция“ и териториалните ѝ звена, дирекция „Вътрешна сигурност“, СДВР и областните дирекции на МВР; 3. службите „Военно разузнаване“ и „Военна полиция“ към министъра на отбраната; 4. Държавна агенция „Разузнаване“; 5. дирекцията, осъществяваща оперативно-издирвателна дейност и разследване в Комисията за противодействие на корупцията.

В случаите по чл. 38, ал. 3 от Закона за защита при бедствия право да искат извършване на справка за тафични данни, имат Главна дирекция „Пожарна безопасност и защита на населението“ на МВР и териториалните ѝ структури.

*1.3. Ред и условия за искане и разрешаване. Запазване на справката*.

По писмено мотивирано искане на ръководителя на компетентния орган се произнася председателя или оправомощен от него съдия от районния съд. Искането, съгласно чл. 251в, ал. 3 ЗЕС, следва да съдържа: правното основание и целта, за която е необходим достъпът; регистрационен номер на преписката и данни за потребителя, когато е известен; данните, които следва да се отразят в справката; разумен период от време, който да обхваща справката, необходим за постигане на целта; пълно и изчерпателно посочване на фактите и обстоятелствата; длъжностно лице, на което да се предоставят данните.

Справката се запазва от предприятията, съгласно чл. 250, ал. 3 ЗЕС за целите на таксуването и за разплащанията по взаимно свързване до извършване на плащането, освен в случаите на тяхното оспорване или търсене на плащането по реда на този закон. Специално за роуминга се запазват и данни за местоположение – чл. 248, ал. 2, т. 1, б. „е“ ЗЕС. Извършване на плащането е ежемесечно, т.е. предприятията запазват данните за един месец.

По искане на заявителя и след разрешение на съда, справката може да се запази от предприятието в срок до три месеца. Заявителят има право да пази получената справка в същия тримесечен срок, съгласно чл.251ж, ал.2 ЗЕС

***2. По Наказателно-процесуалния кодекс***

*2.1. Допустима цел* - в хода на наказателното производство справка за данни се предоставя за разследване на тежки ***умишлени*** престъпления (чл.159а, ал. 2 НПК), за разлика от ЗЕС – за тежки престъпления. (Съдът е имал случаи да постанови откази на това основание, в досъдебни производства.)

*2.2. Компетентен орган* – наблюдаващият прокурор в досъдебното производство, след разрешение от съответния първоинстанционния съд или съдът в съдебното производство могат да искат предоставяне на справка.

*2.3. Ред и условия за искане и разрешаване. Запазване на справката.*

Изискванията към съдържанието на искането по чл. 159а, ал. 3 НПК са почти идентични с изискванията по ЗЕС.

За разлика от ЗЕС, в наказателното производство *няма законов срок за съхраняване на данните* от наблюдаващият прокурор. Те се унищожават, по негова преценка и след разрешение на съда, съгласно чл. 159а, ал. 6 НПК.

## II. ЗАПАЗВАНЕ И ПРЕДОСТАВЯНЕ НА ДАННИ ЗА ЗАЩИТА НА НАЦИОНАЛНАТА СИГУРНОСТ.

### *1. Кратък исторически преглед на уредбата*

В отменения Закон за далекосъобщенията от 2003 г., не е била предвидена възможност за предоставяне на трафични данни на компетентни органи за разкриване на престъпления или за нуждите на националната сигурност.

С приемането на ЗЕС през 2007 г., изрично се допуска, за нуждите на националната сигурност и за разкриване на престъпления предоставянето на тези данни, по реда и условията на наредба.[1]

Върховният административен съд (ВАС), с решение от 2008 г. отменя чл.5 от издадената, на основание на ЗЕС, Наредба № 40 от 07.01.2008 г.[2]

В последващата редакция от 2009 г. на чл. 251 от ЗЕС, националната сигурност **отпада** като основание за предоставяне на данни и се прецизира текста относно престъпленията – „за разкриване и разследване на тежки престъпления и престъпления по глава девета „а“ от Наказателния кодекс“. С препращаща норма е указано, че данните се използват по реда и условията на **Закон за специалните**

[1] Закон за електронните съобщение (Обн. ДВ. бр.41 от 22 Май 2007 г.) – Чл. 251. (1) За нуждите на националната сигурност, както и за разкриване на престъпления, предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, съхраняват за срок от **12 месеца** определени категории данни. Данни, разкриващи съдържанието на съобщенията, не могат да бъдат съхранявани по този ред. (2) Категориите данни по ал. 1, както и редът, по който се съхраняват и предоставят, се определят с наредба на министъра на вътрешните работи и председателя на Държавната агенция за информационни технологии и съобщения

[2] Решение № 13627 по адм.д. № 11799/2008 г., 5 чл.с. ВАС – „В чл. 5, ал. 2 и 3 от Наредбата е регламентирана възможността разследващите органи, прокуратурата и съда „за нуждите на наказателния процес“, а службите за сигурност „в случай на необходимост, свързана с националната сигурност“, да получат от предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, достъп до съхранявани от тях данни след представяне на писмено искане. Така формулираният текст не поставя условия, препятстващи злоупотреба с възможността да се нарушават конституционно гарантирани права на гражданите. Не е предвидено препращане към специалните закони – НПК, **ЗСРС**, ЗЗЛД, в които са конкретизирани предпоставките за допускане достъп до определени данни, свързани с личния живот и личните данни на отделната личност. Върховният административен съд счита, че текстът на чл. 5 от Наредба № 40/2008 г. противоречи на разпоредбата на чл. 8 от ЕКПЧ“.

**разузнавателни средства (ЗСРС)**[3]. Възприетата законодателна техника е била най-удачна, с оглед разпоредбите на Закона за нормативните актове[4], относно уреждане на обществени отношения от една област, свързани с ограничаване на конституционните права по чл. 32 и чл. 34 от Конституцията на Република България (КРБ), при идентични хипотези и в двата закона – разкриване и разследване на престъпления и за нуждите на национална сигурност.

С изменение и допълнение на ЗЕС от 2010 г. законодателят е уредил същата материя с друг подход – не с препращане към реда и условията на ЗСРС, а с подробна процедура в ЗЕС (чл. 250а – чл. 251а), обявени за противоконституционни с Решение № 2 по к.д. № 8 от 2014г.

В чл. 250а, ал. 2 ЗЕС, в редакция от 2010 г., отново *липсва националната сигурност*, като основание за използване на данни, въпреки че съгласно разпоредбата на чл. 73, ал. 3, т. 7, б. „в“ ЗЕС предприятията осъществяващи обществени електронни съобщения, са длъжни да предоставят трафични данни и на това основание[5]. Последната цитирана разпоредба не е подлагана на проверка за съответствие с КРБ. Конституционният съд, въпреки многобройните си решения, касаещи разпоредби на ЗЕС, не е бил сезиран относно националната сигурност в хипотезата на чл. 73, ал. 3, т. 7, б. „в“ ЗЕС и нейната конституционна търпимост, с оглед на липсата и като възможно основание за ограничаване на права по чл. 32 и чл. 34 от КРБ.

***2. Допустими цели за съхраняване и предоставяне на трафични данни***

С редакцията на чл. 251б, ал. 2 ЗЕС от 2015 г. изрично се предвиди възможността „за ***нуждите*** на националната сигурност“ да се съхраняват и предоставят данни. Текстът не е прецизен, тъй като в приетата терминология в съюзното право, както и в аналогични хипотези в ЗСРС се използва словосъчетанието – „за ***защита*** на националната сигурност“.

Към момента, защитата на националната сигурност е уредена в редица закони, като едно от основанията за ограничаване или лишаване от права. Като примери, могат да се посочат: разкриване на сведения, съставляващи банкова тайна, с решение на районния съдия (чл. 62, ал.7

[3] Закон за електронните съобщения (Изм. – ДВ, бр. 17 от 2009 г.) – чл. 251, ал.1 и 2, чл. 304 и сл. за прихващане на електронни съобщения в реално време. (В наименованието на глава 19 от закона е използвана непрецизната терминология „…защита на националната сигурност и **опазване на обществения ред**“. Така и в чл. 73, ал. 3, т. 7)

[4] Закон за нормативните актове (Обн. ДВ. бр.27 от 1973 г.) – чл. 10, ал. 1.

[5] Закон за електронните съобщения - Чл.73, ал.3, т.7. да съдейства за защита на обществения интерес, за защита на националната сигурност и за осигуряване на електронни съобщения за нуждите на отбраната и при кризи, като:……. в) предоставя възможност за законосъобразно проследяване на трафик по мрежата си от страна на компетентните държавни органи;

Закон за кредитните институции)[6]; отстраняване на участник от обществена поръчка (чл. 157, ал. 2, т. 6 Закон за обществените поръчки); прекратяване на концесионен договор (чл. 146, ал. 1, т. 1 Закон за концесиите); забрана за напускане и връщане в страната на български граждани (чл. 23, ал. 3 Закон за българските документи за самоличност); при придобиване на българско гражданство (чл. 19 Закон за българското гражданство); относно защита на личните данни (чл. 37а, ал. 1 Закон за защита на личните данни); определяне на информация като държавна тайна и вреда (чл. 28 и параграф 1, т. 15 Закон за защита на класифицираната информация); киберпревенция, мониторинг и събиране на информация от комуникационните системи (чл. 14, ал. 2, т. 2, съответно чл. 15, ал. 3, т. 1 Закон за киберсигурност) (Стойков и др., 2015); ограничаване на публичния достъп и услуги от пространствените данни (чл. 17, ал. 2, т. 2 Закон за достъп до пространствените данни); отказ или ограничаване на медийна услуга от други държави (чл. 5, ал. 7 Закон за радиото и телевизията); ограничаване на правото на вероизповедание (чл. 7 Закон за вероизповеданията) и т.н.

***3. Компетентни органи, които могат да искат справка за нуждите на националната сигурност***

Съгласно чл. 251в ЗЕС оправомощените органи, със съответна компетентност за защита на националната сигурност са: 1. специализираните дирекции, териториалните дирекции и самостоятелните териториални отдели на ДАНС; 2. Служба „Военно разузнаване“; 3. Държавна агенция „Разузнаване“ и 4. Главна дирекция „Борба с организираната престъпност“ (ГДБОП) и териториалните ѝ звена[7]. (С оглед разпоредбата на чл. 39, ал. 2, т. 10 ЗМВР – ГДБОП е компетентен орган по отношение на организираната престъпна дейност, свързана с терористични актове.)

На основание чл. 159а, ал. 1 НПК – наблюдаващият прокурор в досъдебно производство може да иска данни за разследване на престъпления, свързани с националната сигурност от съответния първоинстанционен съд. Същото право има и съдът в съдебно производство.

***4. Ред и условия за искане и разрешаване за нуждите на националната сигурност.***

Съгласно чл. 251г, ал. 2 – Достъпът до данните за предотвратяване, разкриване и разследване на престъпления по чл. 108а, ал. 1 - 4, ал. 6 и

[6] Виж Йорданова, Г. (Ноември 2022). За финансирането на тероризма като секюритизиран проблем. *Сигурност и отбрана,* (1), 172-173, 178-180. https://institute.nvu.bg/sites/default/files/inline-files/2022-1-14-yordanova.pdf

[7] Закон за електронните съобщения, чл. 251в, ал.1 – „Право да искат извършване на справка за данните по чл. 251б, ал. 1, когато данните са *необходими за изпълнение на техните правомощия*…“

7, чл. 109, ал. 3, чл. 110, ал. 1, предл. шесто, чл. 110, ал. 2 от НК се осъществява след разрешение от председателя на **Софийския градски съд** или от оправомощен от него съдия (Велчев, 2014).

В случаите на непосредствена опасност от извършване на посочените престъпление законът е уредил възможността за *предоставяне на незабавен достъп* до данните въз основа на искане на съответния ръководител на структурите, с последваща съдебна санкция в срок до 24 часа – потвърждаване или отказване на достъпа.

*Съществените въпроси, които могат да се поставят*, относно посочената уредба – в останалите случаи на защита на националната сигурност, извън възможните терористични престъпления,[8] кой е компетентния съд и приложима ли е възможността за незабавен достъп до данни? При сегашната несъвършена редакция на закона би следвало да се приложи общия ред – сезира се районния съд, без задължение за бързо произнасяне в 24 часов срок и без възможност за незабавен достъп до данни.

## III. РЕШЕНИЯ НА ЕСПЧ И НА СЪДА НА ЕВРОПЕЙСКИЯ СЪЮЗ ЗА БЪЛГАРИЯ

### *1.Решение по делото Екимджиев и др. срещу България от 2022 г.*[9]

Европейския съд по правата на човека (ЕСПЧ) констатира нарушение на чл. 8 от Конвенцията за защита на правата на човека и основните свободи (КЗПЧОС) по отношение на процедурите и нормативната уредба по ЗЕС и НПК, при съхраняване и достъп до данни.

Европейският съд е приел в § 216, следното: разпоредбите на ЗЗЛД се прилагат само за физически лица, независимо дали се отнасят до обработването на лични данни, попадащи в обхвата на Регламент (ЕС) 2016/679 (GDPR) или **до обработването на такива данни от органите за целите на правоприлагането** (чл. 1, ал. 1 и 2).

Съдът допълва, че администраторът или обработващият лични данни може да ограничи изцяло или частично правата на субекта на данни, предвидени в чл. 12-22 от GDPR, ако упражняването на тези права или изпълнението на това задължение би създало риск за: **а)** националната сигурност, **б)** обществения ред и сигурност или **в)**

[8] Виж Маринов, П. (Ноември 2022). Изследване на влияещите фактори върху процесите на радикализация в България. *Сигурност и отбрана,* (1), 148-149. https://institute.nvu.bg/sites/default/files/inline-files/2022-1-13-marinov.pdf

[9] Европейски съд по правата на човека. (2022, януари 11). *Решение на ЕСПЧ (четвърто отделение) по дело „Екимджиев и други срещу България“*. Извлечено септември 16, 2023 г., от https://hudoc.echr.coe.int/fre#{%22languageisocode%22:[%22BUL%22],%22appno%22:[%2270078/12%22],%22documentcollectionid2%22:[%22CHAMBER%22],%22itemid%22:[%22001-218290%22]}

предотвратяването, разследването, разкриването или наказателното преследване на престъпления (чл. 37а, ал. 1 ЗЗЛД, чл. 23, § 1 от GDPR)

В § 220 от решението се посочва, че администраторът на данни може **да забави или да откаже (изцяло или частично) да предостави на субекта на данни информация**, когато това е необходимо, за да: **1.** не се допусне възпрепятстването на служебни или законово регламентирани проверки, разследвания или процедури; **2.** не се допусне неблагоприятно засягане на предотвратяването, разкриването, разследването или наказателното преследване на престъпления или изпълнението на наказания; **3**. се защити общественият ред и сигурност; **4**. се защити националната сигурност; **5**. се защитят правата и свободите на други лица. *След отпадане на обстоятелство администраторът предоставя без забавяне исканата информация в двумесечен срок.* (чл. 54, ал. 3 и 4 ЗЗЛД и чл. 13, § 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* (КЗЛД или Инспектората към ВСС (чл. 55, ал. 5 ЗЗЛД и член 15, § 4 от Директивата).

Във всички тези случаи на ограничаване на правата на субектите на данни те могат да сезират КЗЛД или Инспектората към ВСС *(в зависимост от това дали данните се обработват от несъдебен или съдебен орган).* Ако получат такава жалба, посочените органи трябва да проверят дали ограничението е законосъобразно (чл. 57, ал. 1 ЗЗЛД и чл. 17, § 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.

В същото решение по дело Екимджиев и др. срещу България от 2022 г., ЕСПЧ анализира и други релевантни актове на ЕС – *Директива 2002/58/ЕО на ЕП и на Съвета* 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 и електронни комуникации)[10]. Цитирано е решение на СЕС от 21.12.2016 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 АпАдмС на Стокхолм и от АпС

[10] Директива 2002/58/ЕО на Европейския парламент и на Съвета, чл. 15, § 1 – „Държавите-членки могат да приемат законодателни мерки, за да ограничат обхвата на правата и задълженията, предвидени в член 5, член 6, член 8, параграф 1, 2, 3, и 4 и член 9 от настоящата директива, когато такова ограничаване представлява необходима, подходяща и пропорционална мярка в рамките на демократично общество, за да гарантира национална сигурност (т.е. държавна сигурност), отбрана, обществена безопасност и превенцията, разследването, разкриването и преследването на криминални нарушения или неразрешено използване на електронна комуникационна система, …“. (Европейски парламент и Съвет на Европейския съюз, 2002)

на Англия и Уелс, в което се приема, 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. В решение от 2.10.2018 г. (Ministerio Fiscal, C-207/16, EU:C:2018:788), по предварително запитване от Провинциалния съд на Тарагона, Испания, СЕС постановява, 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, дори и да не е оправдана от необходимостта от борба с „тежката“ престъпност.

С решение от 6.10.2020 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, СЕС приема, че чл. 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 е 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.

Съдът приема, 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, 30.01.2020 г.; Решение по дело *Centrum för rättvisa* и Решение по дело *Big Brother Watch и др*.). 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.

По отношение на **надзора на процедурите**, осъществяван от КЗЛД, от съда и от компетентната парламентарна комисия, ЕСПЧ приема, че:

- *по отношение на КЗЛД* – съгласно чл.261а ЗЕС, правомощията на Комисията се ограничават само до предприятията, предоставящи данни. От друга страна, по силата на ЗЗЛД същата Комисия има за задача да контролира начина, по който органите обработват лични данни за целите на правоприлагането;

- *по отношение на съда*, издал разрешение за достъп – той не може да осигури ефективен текущ контрол, както и да присъди обезщетение на лицето;

- *по отношение на парламентарната комисия* – няма изискване към експертния състав, осъществяващ проверки да е с подходяща юридическа квалификация. Комисията няма правомощия по отношение на процедурата по НПК, свързани с контрол и даване на указания, освен да получава статистическа информация.

Режимът на **уведомяване на засегнатото лице** също не удовлетворява стандартите на КЗПЧОС.

Както е отбелязано 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.*

ЕСПЧ отбелязва, че не са представени данни, че до момента такова уведомление е осъществявано от администратора по силата на чл. 54, ал. 4 от ЗЗЛД. Също така няма информация 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.

Правомощията на парламентарната комисия, съгласно чл. 261б, ал. 4 ЗЕС са ограничени при уведомяване на лицето само за неправомерни действия на оперативните служби и предприятия, относно данните и то при ограничителни условия, свързани с опасност за постигане на целите на предоставянето им ( § 416 и § 417).

От изложеното 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“. Следователно е налице нарушение на чл. 8 от Конвенцията.

***2. Решение на Съда на ЕС по дело C 350/21 от 17.11.2022 г.***[11]

Съдът на ЕС постановява, че Директива 2002/58 трябва да се тълкува, в смисъл, че не допуска:

- национално законодателство, относно превантивно, за целите на борбата с тежката престъпност и предотвратяването на сериозни заплахи за обществената сигурност, общо и неизбирателно запазване на данни за трафик и на данни за местонахождение по ЗЕС;

- не допускат национална правна уредба, която предвижда достъп от страна на националните органи, компетентни в областта на разследването на престъпления, до законно запазени данни за трафик и данни за местонахождение, без да гарантира, че лицата, до чиито данни са имали достъп тези национални органи, са били уведомени за това в степента, предвидена от правото на Съюза, и без посочените лица да разполагат с правно средство за защита срещу неправомерен достъп до тези данни.

## IV. ПРЕДЛОЖЕНИЯ ЗА УСЪВЪРШЕНСТВАНЕ НА КОНТРОЛА НА ЕЛЕКТРОННАТА КОМУНИКАЦИЯ В РЕПУБЛИКА БЪЛГАРИЯ

Основното предложение е процедурата по съхраняване на данни и предоставяне на справки да се уреди в ЗСРС по аналогичен ред и условия с използването на специални разузнавателни средства.

*1.Националната сигурност като основание за контрол на електронната комуникация, само при реална настояща или предвидима заплаха и за строго необходим период на нейното съществуване*:

– *общо и неизбирателно запазване* на данни за трафик и на данни за местонахождение;

– *целево запазване* на данни за трафик и на данни за местонахождение, в зависимост от категориите *засегнати лица или посредством географски критерий*, включително обекти с масово пребиваване[12];

– общо и неизбирателно запазване на IP адреси, дадени на източника на свързване с интернет, както и запазване на данни относно самоличността на ползвателите на електронни съобщителни средства ;

– ***бързо запазване на данните за трафик и на данните за местонахождение***.

[11] Съд на Европейския съюз. (2022, ноември 17). *Решение на съда (шести състав) по дело C-350/21 с предмет преюдициално запитване, отправено на основание член 267 ДФЕС от Специализиран наказателен съд (България) с определение от 3 юни 2021 г.* Извлечено септември 16, 2023 г., от https://eur-lex.europa.eu/legal-content/BG/TXT/HTML/?uri=CELEX:62021CJ0350

[12] Виж Милушев, Л. (Декември 2022). Специфики при изграждане на система за сигурност в обекти с масово пребиваване на хора. *Сигурност и отбрана,* (2), 168-171. https://institute.nvu.bg/sites/default/files/inline-files/2022-2-11-milushev.pdf

– задължение за доставчиците на електронни съобщителни услуги, да използват автоматизиран анализ, както и **да събират в реално време** на данни за трафик и на данни за местонахождение за лица, за които съществуват основателни подозрения, че участват в ***терористични дейности***[13].

Законодателно следва да се реши по категоричен начин въпросът *националната сигурност самостоятелно основание за контрол* на електронната комуникация ли следва да се запази или да се предвиди само в случаи на предотвратяване на тежки умишлени престъпления по глава първа от особената част на НК, по подобие на уредбата в ЗСРС[14].

*2. Компетентен съд*

Разрешаване за предоставяне на справка за защита на националната сигурност само от Софийски градски съд, по аналогия с разпоредбата на чл.35, ал. 4, предл. 2 НПК – за престъпления по глава първа от особената част на НК.

*3. Ред за искане и разрешаване на достъпа до трафични данни.*

Да се уреди процедурата по подобие на разпоредбите на чл.12-18 ЗСРС. Запазване на трафични данни, само за в бъдещ период след съдебно разпореждане.

*4. Срокове за съхраняване на данни.*

Възможно е данни за местонахождение да се запазват от предприятията за по-кратък срок – до 2 месеца, а други данни – до 4 месеца. Допустимият при сегашната уредба шест месечен срок е прекомерен[15].

*5. Задължение на заявителя да уведоми засегнатото лице*.

В три месечен срок след срока за запазване на данните от заявителя, същият е задължен да уведоми засегнатото лице. Отлагане на уведомяването е допустимо само след разрешение на съответният съд, разпоредил предоставяне на справката, когато това ще създаде опасност за постигане на целите на достъпа.

*6. Контрол на процедурите*

В случай, че процедурата по съхраняване и предоставяне на данни се уреди в ЗСРС, логичното предложение е един орган да осъществява надзор над същата – Националното бюро за контрол на СРС.

---

[13] Виж Съд на Европейския съюз. (2020, октомври 6). *Решение на съда (голям състав) по съединени дела C-511/18, C-512/18 и C-520/18, с предмет преюдициални запитвания, отправени на основание член 267 ДФЕС от Conseil d'État (Държавен съвет, Франция) с актове от 26 юли 2018 г., постъпили в Съда на 3 август 2018 г. (C-511/18 и C-512/18), и от Cour constitutionnelle (Конституционен съд, Белгия) с акт от 19 юли 2018 г*. Извлечено септември 16, 2023 г., от https://curia.europa.eu/juris/liste.jsf?language=en&num=C-511/18

[14] ЗСРС, чл. 21, ал. 1, т. 2.

[15] Съгласно § 176 на Закона за съобщенията (TKG) на ФРГ, сроковете са – четири седмици за данните за местонахождение и десет седмици за другите данни. (Telekommunikationsgesetz, 2021).

**ЗАКЛЮЧЕНИЕ**

След постановяване на решенията на ЕСПЧ и на Съдът на ЕС от 2022 г. за България, уредбата на процедурите и организацията на органите, свързана с контрол на електронната комуникация следва се актуализират, като се постави акцент върху ясното и точно дефиниране на защита на националната сигурност, като основание за съхраняване и предоставяне на трафични данни, в допустимите предели на Конституцията на Република България, на ЕКПЧОС и на основните актове на съюзното право.

Направените предложения са опит за прилагане на принципите на законност, необходимост и пропорционалност при защита на националната сигурност и защита правата на контролираното лице.

**ЛИТЕРАТУРА:**

Велчев, Б. (2014). *Престъпления против Републиката*. Сиела. // Velchev, B. (2014). *Prestapleniya protiv Republikata*. Siela.

Европейски парламент и Съвет на Европейския съюз. (2002). Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 година 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 и електронни комуникации). *OJ L 201, 31.7.2002, p. 37–47*. Извлечено септември 16, 2023 г., от https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A32002L0058&qid=1606395563171

Европейски съд по правата на човека. (2022, януари 11). Решение на ЕСПЧ (четвърто отделение) по дело „Екимджиев и други срещу България“. Извлечено септември 16, 2023 г., от https://hudoc.echr.coe.int/fre#{%22languageisocode%22:[%22BUL%22],%22appno%22:[%2270078/12%22],%22documentcollectionid2%22:[%22CHAMBER%22],%22itemid%22:[%22001-218290%22]}

Йорданова, Г. (Ноември 2022). За финансирането на тероризма като секюритизиран проблем. *Сигурност и отбрана,* (1), 170-181. https://institute.nvu.bg/sites/default/files/inline-files/2022-1-14-yordanova.pdf // Yordanova, G. (Noemvri 2022). Za finansiraneto na terorizma kato sekyuritiziran problem. *Sigurnost i otbrana,* (1), 170-181. https://institute.nvu.bg/sites/default/files/inline-files/2022-1-14-yordanova.pdf

Маринов, П. (Ноември 2022). Изследване на влияещите фактори върху процесите на радикализация в България. *Сигурност и отбрана*, (1), 148-169. https://institute.nvu.bg/sites/default/files/inline-

files/2022-1-13-marinov.pdf // Marinov, P. (Noemvri 2022). Izsledvane na vliyaeshtite faktori varhu protsesite na radikalizatsiya v Balgariya. *Sigurnost i otbrana,* (1), 148-169. https://institute.nvu.bg/sites/default/files/inline-files/2022-1-13-marinov.pdf

Милушев, Л. (Декември 2022). Специфики при изграждане на система за сигурност в обекти с масово пребиваване на хора. *Сигурност и отбрана*, (2), 166-184. https://institute.nvu.bg/sites/default/files/inline-files/2022-2-11-milushev.pdf // Milushev, L. (Dekemvri 2022). Spetsifiki pri izgrazhdane na sistema za sigurnost v obekti s masovo prebivavane na hora. *Sigurnost i otbrana,* (2), 166-184. https://institute.nvu.bg/sites/default/files/inline-files/2022-2-11-milushev.pdf

Стойков, С., Марин, Н., Маринов, Р., Кочев, Й. (2015). Проблеми пред информационната сигурност. *Сигурност*. ISSN-2367-6833 // Stoykov, S., Marin, N., Marinov, R., Kochev, Y. (2015). Problemi pred informatsionnata sigurnost. *Sigurnost*. ISSN-2367-6833

Съд на Европейския съюз. (2020, октомври 6). *Решение на съда (голям състав) по съединени дела C-511/18, C-512/18 и C-520/18, с предмет преюдициални запитвания, отправени на основание член 267 ДФЕС от Conseil d'État (Държавен съвет, Франция) с актове от 26 юли 2018 г., постъпили в Съда на 3 август 2018 г. (C-511/18 и C-512/18), и от Cour constitutionnelle (Конституционен съд, Белгия) с акт от 19 юли 2018 г*. Извлечено септември 16, 2023 г., от https://curia.europa.eu/juris/liste.jsf?language=en&num=C-511/18

Съд на Европейския съюз. (2022, ноември 17). *Решение на съда (шести състав) по дело C-350/21 с предмет преюдициално запитване, отправено на основание член 267 ДФЕС от Специализиран наказателен съд (България) с определение от 3 юни 2021 г.* Извлечено септември 16, 2023 г., от https://eur-lex.europa.eu/legal-content/BG/TXT/HTML/?uri=CELEX:62021CJ0350

Telekommunikationsgesetz (2021). Teil 10 - Öffentliche Sicherheit und Notfallvorsorge (§§ 164 - 190). Abschnitt 1 - Öffentliche Sicherheit (§§ 164 - 183). § 176 Pflichten zur Speicherung von Verkehrsdaten. Dejure.org. Retrieved September 16, 2023, from https://dejure.org/gesetze/TKG/176.html