ДОСТЪП ДО ТРАФИЧНИ ДАННИ В ДОСЪДЕБНАТА ФАЗА НА НАКАЗАТЕЛНОТО ПРОИЗВОДСТВО

Цветана Бързинска
Районна прокуратура – Пловдив

Димитър Попов
ВУСИ – Пловдив

Резюме: *В статията е разгледана подробно предвидената законова процедура за достъп до трафични данни в досъдебната фаза на наказателното производство, правата и задълженията на компетентните искатели и взаимодействието им с предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги.*

Ключови думи: *разследване, достъп до трафични данни, предприятия, предоставящи обществени електронни съобщителни мрежи и/или услуги.*

ACCESS TO TRAFFIC DATA IN THE PRE-TRIAL PHASE OF CRIMINAL PROCEEDINGS

Tsvetana Barzinska
District Prosecutor's Office – Plovdiv
Dimitar Popov
HSSE-Plovdiv

Abstract: *The article examines in detail the statutory procedure for access to traffic data in the pre-trial phase of criminal proceedings, the rights and obligations of competent applicants and their interaction with enterprises providing public electronic communication networks and/or services.*

Keywords: *investigation, access to traffic data, enterprises providing public electronic communication networks and/or service.*

I. Увод

Съгласно чл. 34, ал. 1 от Конституцията на Република България свободата и тайната на кореспонденцията и на другите съобщения са неприкосновени. Изключение от това правило е предвидено в ал. 2 на същата разпоредба, която казва, че изключения се допускат само с разрешение на *съдебната власт*, когато това се налага за разкриване или предотвратяване на *тежки* престъпления. От една страна това изключение представлява сериозна намеса в личната сфера на гражданите. От друга страна то обслужва особено важни цели с висок обществен интерес, свързани с националната сигурност, обществения ред, отбраната, обществената сигурност, предотвратяването, разследването, разкриването и преследването на престъпления. По-

ради това следва да се търси баланс между преследваната легитимна цел и конституционно залегналото право на гражданите на неприкосновеност на свободата и тайната на кореспонденцията и на другите съобщения. Този баланс е застъпен и в европейското законодателство и в практиката на Съда на Европейския съюз /СЕС/.

Европейското законодателство не изключва намеса в личната сфера на индивида, но категорично сочи, че тя трябва да се свежда до строго необходимото и да са предвидени ясни и точни правила, определящи обхвата на тази намеса. В член 15, параграф 1 от Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 година относно обработката на лични данни и защитата на правото на неприкосновеност на личния живот в сектора на електронните комуникации /Директива 2002/58/ЕО/ се сочи, че 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 същата директива, когато такова ограничаване представлява *необходима, подходяща и пропорционална мярка* в рамките на демократично общество, за да гарантира националната сигурност (т.е държавната сигурност), отбрана, обществена безопасност и превенцията, разследването, разкриването и преследването на престъпления или неразрешено използване на електронна комуникационна система, както е посочено в член 13, параграф 1 от Директива 95/46/ЕО[1]. В тази връзка, държавите-членки могат, *inter alia*, да одобрят законодателни мерки, предвиждащи съхранението на данни за *ограничен период*, оправдани на основанията, изложени в 13, параграф 1 от Директива 95/46/ЕО. Всички законодателни мерки, обаче трябва да бъдат в съответствие с общите принципи на законодателството на Общността, включително онези, упоменати в член 6, параграф 1 и 2 от Договора за Европейския съюз.

По преюдициално запитване на Република България беше издадено Решение на СЕС от 17 ноември 2022 г. по дело С-350/21 г., в което съдът в Люксембург сочи, че член 15, параграф 1 от Директива 2002/58/ЕО във връзка с членове 7, 8 и 11 и член 52, параграф 1 от Хартата на основните права на Европейския съюз трябва да се тълкува в смисъл, че не се допуска национално законодателство, което предвижда 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, дори ако посоченото законодателство ограничава във времето това общо и неизбирателно запазване до период от шест месеца и предвижда определени гаранции в областта на запазването и достъпа до съответните данни. Тълкуването на посочените разпоредби не допуска и национално законодателство, което не предвижда ясно и точно, че достъпът до запазените

[1] Държавите-членки могат да приемат законодателни мерки за ограничаване на обхвата на правата и задълженията, предвидени в член 6, параграф 1, член 10, член 11, параграф 1, член 12 и член 21, ако подобно ограничаване представлява необходима мярка за гарантиране на: а/ националната сигурност; б/ отбраната; в/ обществената сигурност; г/ предотвратяването, резследването, разкриването и преследването на углавни престъпления или за нарушения на етичните кодекси при регламентираните професии; д/ важни икономически и финансови интереси на държавата-членка или на Европейския съюз, включително валутни, бюджетни и данъчни въпроси; е/ функции по наблюдение, проверка или регламентиране, свързани, дори случайно, с упражняването на официални правомощия в случаите, посочени в букви в), г) и д); ж/ защита на съответното физическо лице или на правата и свободите на други лица.

данни е *ограничен до строго необходимото за постигането на преследваната с това запазване цел*. Що се отнася до това дали съответното национално законодателство трябва ясно и точно да предвижда, че достъпът до запазените данни е ограничен до строго необходимото за постигането на преследваната с това запазване цел, от съдебната практика следва, че за да се изпълни изискването за пропорционалност, съгласно което дерогациите и ограниченията на защитата на личните данни трябва да се въвеждат в границите на строго необходимото, компетентните национални органи трябва да гарантират във всеки конкретен случай, че както визираните категории данни, така и продължителността, за която се иска достъп до тях, са ограничени, в зависимост от обстоятелствата по случая, до строго необходимото за целите на въпросното разследване (решение от 2 март 2021 г., Prokuratuur (Условия за достъп до данните за електронните съобщения), C-746/18, EU:C:2021:152, т. 38 и цитираната съдебна практика). За да изпълни изискването за пропорционалност, националната правна уредба трябва да предвижда ясни и точни правила, които да уреждат обхвата и прилагането на разглежданата мярка и да налагат минимални изисквания, така че лицата, чиито лични данни са засегнати, да разполагат с достатъчно гаранции, позволяващи ефикасна защита на тези данни срещу рискове от злоупотреби. Приета на основание член 15, параграф 1 от Директива 2002/58 национална правна уредба, която урежда достъпа на компетентните органи до запазените данни за трафик и данни за местонахождение, не може да се ограничи до изискването достъпът на органите до данните да отговаря на преследваната с тази правна уредба цел, а трябва да предвижда също материални и процесуални условия за това използване (в този смисъл решение от 5 април 2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 103 и 104 и цитираната съдебна практика).

В националното ни законодателство процедурата за достъп до трафични данни в досъдебната фаза на наказателното производство има изцяло законова регламентация, надлежно уредена в Наказателно-процесуалния кодекс /НПК/ и Закона за електронните съобщения /ЗЕС/. Нормативна уредба на първо място е предвидена в НПК. В разпоредбата на чл. 159а от НПК[2] е разписана възможност по искане на наблюдаващия прокурор в досъдебното производство (ДП), предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги (наричани по-нататък за краткост предприятията), да предоставят определен тип трафични данни (ТД).

Основната цел на изложението е да подпомогне прокурорите, наблюдаващи конкретни досъдебни производства в процеса, свързан с изготвяне на искания за достъп до ТД, комуникацията с предприятията, компетентния съд, издаващ разпореждания, с които се разрешава достъпът, получаването и използването на ТД, унищожаването им или прилагането им по съответните ДП, цялостното администриране на процеса. Изложението е основно с практическа насоченост.

II. Общи понятия и определения:

1. Преди да разгледаме процедурата, свързана с достъпа до ТД, трябва да обърнем внимание на самото понятие ТД и какво се включва в него.

Възможно най-краткият и обобщаващ отговор[3] е, че ТД са **данни, обработвани от предприятията**, за: целите на **преноса** на едно **съобщение** по електронна съоб-

[2] Чл. 159а от НПК (*) (Нов – ДВ, бр. 24 от 2015 г., в сила от 31.03.2015 г.)
[3] Изведен от т. 71 на § 1 от Допълнителните разпоредби на ЗЕС

щителна мрежа; необходими за **таксуването** му; данни за **местоположението**, и **свързаните с тях данни**, необходими за **идентифициране на абонат или регистриран потребител**. Така даденото определение обхваща огромен обем от различни видове ТД, но за целите на наказателното производство законодателят е предвидил[4] че могат да се искат и ползват само и единствено ТД за **идентифициране,** а именно: проследяване и идентифициране на източника на връзката; идентифициране на направлението на връзката; идентифициране на датата, часа и продължителността на връзката; идентифициране на типа на връзката; идентифициране на крайното устройство на потребителя или на това, което се представя за негово крайно устройство; установяване на идентификатор на ползваните клетки. Именно поради възможността да възникне необходимост от ползването на ТД за идентифициране в хода на разследването по конкретно ДП, предприятията имат законово задължение да съхраняват за срок от 6 месеца тези данни, създадени или обработени в процеса на тяхната дейност.

2. Трафични данни за **идентифициране** и значението им за разследването по ДП.

Тъй като за целите на наказателното производство е възможен достъпът само и единствено до този тип ТД (шест подвида на брой) е необходимо подробно да разгледаме какво представлява всеки един от тях и каква информация може да ни даде в хода на разследването по ДП.

2.1) Проследяване и идентифициране на източника на връзката /чл. 251и, ал. 1 от ЗЕС/:

а) При услуга за гласови съобщения – телефонния номер на викащия и данни за идентифициране на крайния ползвател.

б) При интернет достъп, електронна поща по интернет и интернет телефония – идентификатор, определен за крайния ползвател (лице, което е страна по договор с предприятие, предоставящо обществени електронни съобщителни услуги); идентификатор на крайния ползвател и телефонен номер, определени за всяко съобщение, влизащо в обществената телефонна мрежа; данни за идентифициране на крайния ползвател, за когото са определени IP адрес; идентификатор на крайния ползвател или телефонен номер в момента на връзката.

2.2) Идентифициране на направлението на връзката /чл. 251и, ал. 2 от ЗЕС/:

а) При услуга за гласови съобщения – набран номер (викан телефонен номер) и в случаите на допълнителни услуги, като пренасочване или прехвърляне на повикването, номер или номера, към които е маршрутизирано повикването, и данни за идентифициране на крайния ползвател.

б) При електронна поща по интернет и интернет телефония – идентификатор на крайния ползвател или телефонен номер на получателя/ите на интернет телефонно повикване, данни за идентифициране на крайния ползвател и идентификатор на получателя, за когото е предназначено съобщението.

2.3) Идентифициране на датата, часа и продължителността на връзката /чл. 251и, ал. 3 от ЗЕС/:

а) При услуга за гласови съобщения – дата и час на началото и края на връзката.

б) За интернет достъп, електронна поща по интернет и интернет телефония – дата и час на влизане и излизане в/от услугата интернет достъп, основаващи се на

[4] Виж чл. 159а, ал. 1 от НПК

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

2.4) Идентифициране на типа на връзката /чл. 251и, ал. 4 от ЗЕС/:

а) Вида на използваната услуга за гласови съобщения.

б) Използваната интернет услуга при електронна поща по интернет или интернет телефония.

2.5) Идентифициране на крайното устройство на потребителя или на това, което се представя за негово крайно устройство /чл. 251и, ал. 5 от ЗЕС/:

а) При фиксирана услуга за гласови съобщения – за викащия и викания телефонен номер;

б) При услуга за гласови съобщения, предоставяна чрез мобилна наземна мрежа – за викащ и викан телефонен номер; международен идентификатор на викащия мобилен краен ползвател – IMSI[5]; международен идентификатор на викания мобилен краен ползвател – IMSI; международен идентификатор на викащото мобилно крайно устройство – IMEI[6]; международен идентификатор на виканото мобилно крайно устройство – IMEI; в случай на предплатени услуги – дата и час на началното активиране на услугата и етикет за местоположение – идентификатор на клетката, от което е активирана услугата и за идентифициране на крайния ползвател;

в) При интернет достъп, електронна поща по интернет и интернет телефония – викащият телефонен номер за комутируем достъп, цифрова абонатна линия (DSL) или друга крайна точка на инициатора на връзката.

2.6) Установяване на идентификатор на ползваните клетки /чл. 251и, ал. 6 от ЗЕС/:

а) Данни за административни адреси на клетки на мобилна наземна електронна съобщителна мрежа, от които е генерирано или в които е терминирано повикване.

III. Допустимост на достъпа до ТД в досъдебната фаза

1. Оправомощени искатели.

Само и единствено **наблюдаващият прокурор** по съответното ДП може да направи искане за достъп до ТД в хода на разследването по образуваното наказателно производство, когато то се води за **тежко умишлено престъпление** по см. на чл. 93, т. 7 от Наказателния кодекс /НК/[7]. Националната правна уредба не допуска искане за достъп до ТД да се отправя от други органи с разследващи функции /разследващи полицаи, следователи и др./;

2. Изготвяне на искане за достъп до ТД.

За достъп до данните, изброени лимитативно в чл. 159, ал. 1, т. 1 - т. 6 от НПК, наблюдаващият прокурор изготвя мотивирано писмено искане, което задължително съдържа:

[5] IMSI (International mobile subscriber identity – международната идентичност на мобилните абонати)

[6] IMEI (International Mobile Equipment Identity – международна идентичност на мобилното оборудване)

[7] „Тежко престъпление” е това, за което по закона е предвидено наказание лишаване от свобода повече от пет години, доживотен затвор или доживотен затвор без замяна

- **информация за престъплението**, за разследването на което се налага използването на данни за трафика – освен посочване на правната квалификация на деянието, трябва да се опише фактическата обстановка, касаеща престъплението. Описаната фактическа обстановка трябва да съответства на посочената правна квалификация на деянието и да касае разследването на „тежко” умишлено престъпление;
- **описание на обстоятелствата**, на които се основава искането /цел на искането/ – по какъв начин именно достъпът до исканите ТД ще спомогне за разкриване на обективната истина по конкретното дело;
- **данни за лицата**, за които се изискват данни за трафика – следва да се изясни защо именно за това лице се искат данните за трафика, т.е каква е неговата връзка /съпричастност/ с престъплението, за което се иска достъп до ТД. Данните за лицата трябва да са достатъчно индивидуализиращи и да не се допуска предоставяне на данни за трафика за друго лице.
- **разумен период от време,** който да обхваща справката[8] – периодът от време трябва да е логически обвързан с фактическата обстановка по делото и предмета на доказване и не може да бъде по-дълъг от 6 месеца. Съдът е обвързан от срока, посочен в искането. Ако съдът прецени, че той е прекалено дълъг и не съответства на фактическата обстановка по случая или надвишава максимално допустимия 6 месечен срок, той не може да издаде разрешение за друг срок, а отказва да издаде разрешение за достъп до ТД, като мотивира отказа си.
- **разследващия орган,** на който да се предоставят данните – име и фамилия, служебен адрес и служебен телефон за връзка. Справката с данните за трафика следва да се предоставя от предприятията първо на наблюдаващия прокурор, за да се отбележи в деловодните системи на прокуратурата, че е получена, след това да се изпратят на разследващите органи и службите за сигурност или службите за обществен ред, ангажирани с работата по делото, за изготвяне на анализ. Когато искането за достъп до ТД е класифицирано (оформено като класифициран документ, съдържащ класифицирана информация, представляваща държавна тайна[9] /КИ-ДТ/), трябва да се отбележи в него, че справката с данните за трафика (без значение дали съдържа явна или класифицирана информация КИ-ДТ) следва да се изпрати в регистратурата за класифицирана информация[10] (РКИ) на съответната прокуратура за конкретния наблюдаващ прокурор.
- **точно наименование на предприятието**, от което се иска предоставянето на ТД - наименованието на предприятието трябва да съответства на това, с което то фигурира в Търговския регистър и да е индивидуализирано с данни за ЕИК, седалище и адрес на управление.

Искането по чл. 159а от НПК трябва да е отправено в рамките на образувано досъдебно производство, разследването по което не е приключило. Искането се отправя до съответния първоинстанционен съд и може да касае достъп само до данни за трафика, които отговарят на лимитативно изброените в чл. 159а, ал. 1, т. 1 – т. 6 от НПК. В искането трябва изрично да се посочи достъп до кои ТД се претендира, в съответствие с разпоредбата на чл. 159а, ал. 1, т. 1 – т. 6 от НПК, а не това да се прави чрез тълкуване от съда.

[8] Съгласно чл. 159а, ал. 5 от НПК
[9] Чл. 25 от ЗЗКИ
[10] Вж. § 1, т. 7 от Допълнителните разпоредби към ЗЗКИ и чл. 51 от ППЗЗКИ

Когато отправеното до съда искане не отговаря на законовите изисквания за форма и съдържание, не е достатъчно мотивирано и не дава на съда достатъчно яснота за необходимостта от исканите данни за конкретното разследване или се иска разрешение за достъп до ТД за период, по-дълъг от необходимото, несъответен на фактическата обстановка по делото, съдът отказва да издаде разрешение за достъп до исканите ТД. В този случай нередовностите в искането могат да бъдат отстранени и отново да бъде поискано от съда издаването на разрешение. При изготвяне на искането от страна на наблюдаващия делото прокурор и при издаването на разрешение за достъп до ТД от съответния съд е необходимо да се съблюдва и относимото европейско законодателство и практиката на СЕС, с които Република България е обвързана.

В НПК не *се съдържа забрана* делото да се предостави на съдията от съответния първоинстанционен съд, компетентен да разреши достъпа до исканите ТД, каквато съществува в разпоредбата на чл. 222, ал. 1 и чл. 223, ал. 1 от НПК. При това считам, че е абсолютно необходимо на съдията да се предоставят всички материали по делото. По този начин съдът ще има възможност да прецени всички обстоятелства по случая, включително необходимостта и пропорционалността от предоставяне на исканите ТД за целите на конкретното разследване.

3. Компетентен съд.

Компетентен да се произнесе по така направеното искане е съдия от съответния първоинстанционен съд[11] /районен или окръжен/, който издава мотивирано разпореждане, с което разрешава или отказва да разреши достъпа до исканите ТД. В разпореждането на компетентния съд, с което разрешава достъп до данните по смисъла на чл. 159, ал. 1, т. 1 - т. 6 от НПК, се посочват: данните за трафика, които следва да се отразят в справката; разумен период от време, който да обхваща справката; разследващият орган, на който да се предоставят данните; предприятието, което следва да ги предостави.

IV. Използване на получените ТД по ДП. Унищожаване на получените ТД.

След получаване на справката с данните за трафика (в повечето случаи предоставената информацията, съдържаща ТД е записана на оптичен носител) от предприятията, наблюдаващият прокурор я изпраща на водещия разследването и оперативните служители, работещи по случая, с цел извършване на анализ на ТД. Резултатите от анализа се оформят в нарочна аналитична справка, която се изпраща на наблюдаващия прокурор и се прилага по ДП. Когато получената от предприятията справката съдържа данни за трафика, които са свързани с обстоятелствата по делото и допринасят за тяхното изясняване, те се прилагат поделото. При внасяне на обвинителен акт те се внасят в съда, заедно с другите материали по делото.

Когато получената от предприятията справка съдържа данни за трафика, които не са свързани с обстоятелствата по делото и не допринасят за тяхното изясняване, наблюдаващият прокурор изготвя мотивирано писмено предложение до съдията, разрешил достъпа, с искане за унищожаване на информацията /справката/, касаеща ТД. Процедурата по унищожаване също е законово регламентирана в разпоредлата на чл. 159а, ал. 6 от НПК, което е гарант за това, че получената информация ще бъде ползвана **само** за целите на конкретното разследване и, че няма да бъдат създадени

[11] В хипотеза на чл. 159а, ал. 1 от НПК

предпоставки за нарушаване правата и свободите на гражданите, по отношение на които е бил изискан достъп до ТД. Редът за унищожаване на справки по чл. 159а, ал. 6 от НПК се определя от Главния прокурор с нарочна заповед. В заповедта е посочено съдържанието на писменото предложение, което се отправя до съдията, разрешил достъпа до ТД по конкретното дело. Предложението трябва да е мотивирано, относно необходимостта от унищожаване на получената информация */следва да се посочи, че след извършен преглед, анализ и преценка на получените ТД (в зависимост кои данните следва да бъдат унищожени или всички заедно) се е установило, че същите не са свързани с обстоятелствата по образуваното ДП и не допринасят за тяхното изясняване/*. В този случай наблюдаващият прокурор предлага на съда да бъде издадено разпореждане за унищожаване на получените данни за трафика. След получаване на съдебното разпореждане за унищожаване на информацията /справката/, наблюдаващият прокурор незабавно изпраща екземпляр или заверен препис от него на предприятието, което ги е предоставило.

Получените съдебни разпореждания за унищожаване на информация /справки/, съдържащи данни за трафика, се изпълняват от съответната прокуратура, поискала достъп до тях. Некласифицираните документи се унищожават от постоянно действаща комисия от служители, в състав председател и двама членове. Комисията се назначава със заповед на административния ръководител. Некласифицираните документи се унищажават посредством нарязване – с резачка /шредер/ за унищожаване на информационни носители по начин, непозволяващ изцяло или частично възстановяване на материала и възпроизвеждане на информацията. Класифицираните документи се унищожават от тричленна комисия, в състав председател – служителят по сигурността на информацията и членове – двама служители с издадени разрешения за достъп до класифицирана информация до най-високото ниво на класификация на информацията, която ще се унищожава. Комисията се назначава със заповед на ръководителя на организационната единица[12]. Документите, съдържащи класифицирана информация, се унищажават посредством нарязване – с резачка /шредер/ за унищожаване на информационни носители, отговаряща на изискванията за нивото на класификация на информацията, подлежаща на унищожаване или повисоко */съгласно Методиката за изграждане и оценка на средствата и системите за физическа сигурност на класифицираната информация, приета на заседание на ДКСИ с протокол № 165-I/30.06.2004 г., изменена с решение № 2-I от 08.01.2009 г./*

За унищожаването на информацията /справката/ се съставя протокол по образец, приложение към заповедта на Главния прокурор. Протоколът се съставя в два екземпляра, един за наблюдателните материали и един за съдията, издал разпореждането за унищожаване, като се подписва от членове на комисията. Екземпляр от протокола за унищожаване се изпраща на съдията в 7-дневен срок от получаване на разпореждането за унищожаване. Протоколът за унищожаване е част от документацията по административното приключване на процедурата, свързана с достъпа до ТД в хода на ДП и се съхранява за нуждите на прокуратурата, искала достъпа до ТД и с цел бъдещи проверки от контролните органи[13].

[12] Вж. ОЕ по смисъла на § 1, т. 3 от Допълнителни разпоредби на ЗЗКИ.

[13] Парламентарната Комисия за контрол над службите за сигурност, прилагането и използването на специалните разузнавателни средства и достъпът до данните по Закона за електронните съобщения.

V. ЗАКЛЮЧЕНИЕ

В досъдебната фаза на наказателното производство процедурата за достъп до трафични данни, включително за използването им и тяхното унищожаване, когато не допринасят за изясняване на обстоятелствата по делото, има изцяло законова регламентация, надлежно уредена в НПК и ЗЕС. Това, разбира се, не е случайно. Чрез достъпа до такива данни се засяга една много чувствителна сфера, каквато е личната сфера, която е неприкосновена според Конституцията на Република България. Поради това, ясно разписаната процедура е гаранция за защита на правата на гражданите. Познаването на отделните видове ТД, които законодателят е предвидил да бъдат предоставяни в досъдебната фаза на наказателното производство, законовият ред за достъп до ТД, анализирането и използването им по ДП, могат да са от съществено значение за разкриване на обективната истина по съответното ДП, а понякога са и единствена възможност за установяване на обективната истина по делото и лицата, съпричастни към извършеното престъпление.

В заключението ще си позволя да посоча още едно тълкуване на СЕС по дело С-724/19 г., с което разясни, че „Директивата относно Европейската заповед за разследване не допуска в досъдебната фаза на наказателното производство прокурорът да издава европейска заповед за разследване с цел събиране на данни за трафика и местонахождението, свързани с далекосъобщения, когато в сходен национален случай разпореждането на процесуално-следствено действие за достъп до такива данни е от изключителната компетентност на съдия“. Според Съда в Люксембург прокурорът може да издава Европейска заповед за разследване /ЕЗР/, но само за действия, за които е компетентен и по националното право. СЕС уточнява и, че „изпълняващият орган не може да отстрани евентуалното неизпълнение на изискванията към издаването на такава заповед“. Посоченото тълкуване на СЕС доведе до изменение на българския Закон за ЕЗР (Изм. - ДВ, бр. 36 от 2024 г.), като в чл.5, ал.1, т.1 от същия се предвиди следното: „Европейската заповед за разследване в Република България се издава: 1. в досъдебното производство: а) от съответния прокурор; б) от съответния прокурор – въз основа на предварително разрешение от съдия, когато за извършване на действието по разследване българското законодателство изисква такова; съдията прави преценка за необходимостта и пропорционалността от нейното издаване и се произнася по реда и в сроковете, установени в сходен национален случай; в) от съответния съд по искане на прокурора, когато единствен компетентен орган да разпореди извършването на действие по разследването в национален случай е съдът.

VI. ИЗПОЛЗВАНИ ИЗТОЧНИЦИ:

[1] Конституция на Република България;
[2] Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 година относно обработката на лични данни и защитата на правото на неприкосновеност на личния живот в сектора на електронните комуникации;
[3] Наказателен кодекс;
[4] Наказателно-процесуален кодекс;
[5] Закон електронните съобщения;
[6] Закон за защита на класифицираната информация и правилник за прилагането му;
[7] Закон за европейската заповед за разследване;