

ДО

**КОНСТИТУЦИОННИЯ СЪД НА
РЕПУБЛИКА БЪЛГАРИЯ**

По к.д. № 19/2025 г.

Правно мнение

от

Георги Сулев, адвокат, член на САК, личен номер 1300810210, със служебен адрес: гр. София, п.к. 1000, бул. „Цар Освободител“ № 10, ет.3, тел.: +35929321100, georgi.sulev@dgkv.com

Относно: Конституционно дело № 19/2025 г. образувано по искане на президента на Република България за установяване на противоконституционност и несъответствие с общо признати норми на международното право и с международните договори, по които България е страна, на разпоредбите на чл. 251б, ал. 2, изречение първо в частта „както и за производства за нарушения на чл. 15 от Закона за защита на конкуренцията“; чл. 251в, ал. 1, т. 6; чл. 251г, ал. 2 в частта „или нарушения на чл. 15 от Закона за защита на конкуренцията“ и чл. 251г, ал. 9 от Закона за електронните съобщения (обн., ДВ, бр. 41 от 22.05.2007 г., поел. изм. бр. 100 от 25.11.2025 г.)

УВАЖАЕМИ ГОСПОЖИ И ГОСПОДА КОНСТИТУЦИОННИ СЪДИИ,

Във връзка с Определение на Конституционния съд („КС“) от 16 декември 2025 г., представям своето правно мнение по предмета на конституционно дело № 19/2025 г., образувано на основание чл. 149, ал. 1, т. 2 и т. 4, предл. второ от Конституцията на Република България по искане на президента на Република България за установяване на противоконституционност и за съответствие с общопризнати норми на международното право и с международните договори, по които България е страна, на следните разпоредби на Закона за електронните съобщения („ЗЕС“, обн. ДВ, бр. 41 от 2007 г., поел. изм. бр. 100 от 2025 г.): чл. 251б, ал. 2, изречение първо в частта „както и за производства за нарушения на чл. 15 от Закона за защита на конкуренцията“; чл. 251в, ал. 1, т. 6; чл. 251г, ал. 2 в частта „или нарушения на чл. 15 от Закона за защита на конкуренцията“ и чл. 251г, ал. 9.

Оспорваните разпоредби са приети с §42 от преходните и заключителни разпоредби на Закона за изменение и допълнение на Закона за защита на конкуренцията („ЗИД на ЗЗК“, обн. ДВ, бр. 95 от 2025 г.). Този комплекс от норми предвижда правомощия на Комисията за защита на конкуренцията („КЗК“) и реда, по който тя може да получава достъп и използва трафични данни и данни за идентифициране на крайните ползватели, съхранявани от предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги в случаите, когато са необходими за установяване на забранени споразумения, решения и съгласувани практики между предприятия, които имат за цел или резултат предотвратяване, ограничаване или нарушаване на конкуренцията. Съгласно чл. 251в, ал. 1, т. 6 от ЗЕС, правомощията на КЗК са ограничени до данните по чл. 251б, ал. 1, т. 1, 3 и 5 от ЗЕС при интернет достъп. В искането вносителят поддържа, че е налице противоречие на разпоредбите с прогласените в чл. 4, чл. 32, ал. 1 и 2, чл. 34, ал.1 и 2 и чл. 57, ал. 1 и 3 от Конституцията принципи на правовата държава, на неприкосновеност на личния живот, на

свободата и тайната на кореспонденцията и на неотменимост на основните права на гражданите. Според вносителя, така установените правила за достъп, използване и съхранение на данни позволяват необоснована и непропорционална намеса на държавата в конституционно защитеното лично пространство на гражданите, която се осъществява при липса на легитимна цел от конституционен ранг, чиято защита да налага ограничение на основни права, както и при липса на адекватни законови механизми, които да гарантират законоустановеност и обективност на намесата.

Считам, че оспорените разпоредби не съответстват на чл. 32, ал. 1 от Конституцията, защото по същество представляват неоправдана намеса в личното пространство на гражданите, която не съответства на гарантираната неприкосновеност на личния живот. Предвиденият достъп на КЗК до данните нарушава и основното право на свобода и тайна на кореспонденцията, гарантирано от чл. 34, ал. 1 от Конституцията, защото е в състояние да породви чувство на уязвимост и да накърни възможността на лицата да се ползват от правото на свобода и тайна на кореспонденцията, да развиват отношения с други лица и да упражняват други основни права чрез използване на електронни съобщителни услуги. Още повече, че действащата нормативна уредба за съхраняване на трафични данни и данни за местоположението, установена със ЗЕС, не съответства на правото на ЕС и международното право, така както е тълкувано в юриспруденцията на Съда на ЕС („СЕС“)¹ и Европейския съд по правата на човека („ЕСПЧ“)².

Основните конституционни права на гражданите не следва да бъдат ограничавани с цел улесняване на доказването на административни нарушения от страна на КЗК, независимо от това каква е тежестта на нарушенията. Предвидената съществена намеса в основните права на гражданите е също така непропорционална, защото не е абсолютно необходима за целите на разкриване и доказване на конкретната категория административни нарушения по чл. 15 от ЗЗК и съществуват други подходи за събиране на електронни доказателства от КЗК за целите на доказване на нарушенията. Подробните ми аргументи са следните:

1. Характер на данните, съхранявани на основание чл. 251б, ал. 1, т. 1, 3 и 5 от ЗЕС при интернет достъп.

По силата на атакуваните разпоредби, КЗК получава правомощия да иска и получава достъп до следните данни, включително трафични данни, определени в чл. 251 и, ал. 1 от ЗЕС: i) **данни за идентифициране на крайния ползвател, за когото е определен IP адрес, идентификатор на крайния ползвател или телефонен номер в момента на връзката** (чл. 251 и, ал. 1, т. 2 от ЗЕС); ii) **дата и час на влизане и излизане в/от услугата интернет достъп**, основаващи се на определена часова зона, **заедно с IP адреса, динамичен или статичен**, определен за връзката от доставчика на услугата интернет достъп (чл. 251 и, ал. 3, т. 2 от ЗЕС); iii) **викацият телефонен номер** за комутируем достъп, **цифрова абонатна линия (DSL) или друга крайна точка на инициатора на връзката** (чл. 251 и, ал. 5, т. 3 от ЗЕС).

Съхраняваната информация на основание чл. 251б, ал. 1, т. 1, 3 и 5 от ЗЕС ще позволи на КЗК да идентифицира абоната за всяка отделна сесия, заедно с IP адреса, който му е предоставен, датата и часа на всяка сесия при ползване на достъп до интернет и крайната точка на мрежата, чрез която се инициира връзката. Сами по себе си, съхранените данни на основание ЗЕС не позволяват да се установи с кои сървъри/клиенти е осъществена връзка от конкретния краен ползвател, както и самото съдържание на

¹ Вж. напр. Решение от 17 ноември 2022 г., *Специализирана прокуратура*, С-350/21.

² Вж. *Ekimdzhiev and Others v. Bulgaria*, no. 70078/12, § 419, 11 януари 2022, ECHR 2022.

съобщенията (например кои интернет страници са посещавани от крайния ползвател). КЗК обаче може да изиска допълнително информация от трети страни в случай, че попадат в кръга на задължени субекти да оказват съдействие на административния орган, което практически включва всички физически и юридически лица, включително предприятия, сдружения на предприятия, държавни органи и органи на местното самоуправление, неправителствени организации и Националният статистически институт (чл. 46 от ЗЗК). Следователно, данните по чл. 251б, ал. 1, т. 1, 3 и 5 от ЗЕС могат в комбинация с други данни да разкрият съобщенията, осъществявани от крайните ползватели.

Въпреки, че чл. 251и, ал. 1, т. 2 от ЗЕС посочва данни за идентификацията на „крайния ползвател“, по обективни причини тези данни са ограничени до лицето, сключило договор за услугата за достъп до интернет. Чрез данните, съхранявани от доставчика на услугата достъп до интернет е невъзможно да се установи крайния ползвател на достъпа до интернет, когато той е различен от абоната. Обичайната хипотеза е случаят, когато услугата за достъп до интернет се споделя локално с други крайни ползватели. Действащият ЗЕС, който въвежда хармонизирани разпоредби на европейското законодателство, всъщност допуска и насърчава крайните ползватели да разрешават реципрочно или по друг начин достъп до своите локални радиомрежи на други крайни ползватели, включително въз основа на инициативи на трети страни, които обединяват и правят обществено достъпни локални радиомрежи на различни крайни ползватели.³ Следователно, всеки краен ползвател може свободно да споделя достъпа до своята локална радиомрежа в района на нейния обхват, което прави данните по чл. 251б, ал. 1, т. 2 изначално неточни и съществува сериозно съмнение, дали могат да послужат за повече от предполагаема идентификация на крайния ползвател.

Основната информация, до която КЗК ще може да получи достъп са IP адресите на крайния ползвател за период от 6 месеца назад към датата на искане на достъпа. IP адресът е логически мрежов адрес, който идентифицира мрежов интерфейс на устройство в даден момент в мрежа, базирана на Интернет протокол (IP), и позволява маршрутизирането на пакети данни между устройства в различни взаимосвързани мрежи. "Интернет" е система от взаимосвързани мрежи, ползващи Интернет протокол, което им позволява да функционират като самостоятелна виртуална мрежа.⁴ Преносът на данни в Интернет се осъществява чрез пакетна комутация, при която информацията се разделя на пакети и се предава между крайни точки в мрежата. Тази комуникация обикновено се реализира в модел клиент-сървър, като е възможна и комуникация от тип peer-to-peer (P2P), при която се обменят данни директно между устройствата без централен сървър, доколкото това е технически възможно.

IP адресите се предоставят на крайните ползватели от предприятията, които им предоставят услуги за достъп до Интернет (доставчици на интернет услуги). За тази цел интернет доставчиците използват блокове от IP адреси, разпределени от съответните

³ Например в т. II.2.5.1. от Решение № 1254/21.11.2024 г. на КЗК е посочено: „Според интернет-доставчика, чрез различни технологии (жични, безжични или VPN), клиентът може да сподели предоставяната му услуга до различна стая, сграда и др. Конфигурацията на рутера и нивото на защита е отговорност на клиента и в случая е възможно използването на вътрешната компютърна мрежа на клиента без неговото предварително съгласие“. В т. II.2.5.2. от Решение № 1254/21.11.2024 г. на КЗК е посочено: „Във връзка с поставени от КЗК въпроси "А1 България" ЕАД предостави информация, че не е възможно даден IP адрес да бъде ползван от различно населено място, освен от посоченото в договора на доставчика. Ако клиентът, по време на ползване на услугата, е използвал собствено устройство, вместо предоставеното му мрежово устройство, тогава е възможно мрежата да е използвана от друг, но на същия адрес. В случай, че клиентът на услугата е споделил с някого WiFi паролата, е възможно трети лица да са ползвали неговата мрежа.“

⁴ § 1, т. 22 от ДР на ЗЕС.

регионални интернет регистри⁵. Тези IP адреси се използват за идентифициране на мрежовите връзки и позволяват асоциирането на даден IP адрес с конкретен интернет доставчик, респективно с крайния ползвател, на когото е предоставен съответният IP адрес.

При посещение на уебсайт от краен ползвател сървърът, който хоства съответния уебсайт, получава информация за публичния IP адрес, от който се осъществява заявката. В повечето случаи това е публичният IP адрес на рутера, чрез който локалната домашна или бизнес мрежа е свързана с Интернет. Както посочих по-горе, зад рутера на крайния ползвател могат да бъдат разположени множество крайни устройства - компютри, таблети, смартфони и други, които използват частни IP адреси в рамките на локалната мрежа, която може да бъде жична или безжична (Wi-Fi мрежа). Когато достъпът до Интернет се осъществява чрез мобилна мрежа, заявките преминават през инфраструктурата на мобилния оператор. В тези случаи, както при връзка клиент-сървър, така и при клиент-клиент комуникация, външните участници в обмена на данни виждат единствено публичния IP адрес на мобилния оператор, а не частния IP адрес, асоцииран с конкретното крайно устройство.

Предвид на изложеното, достъпът до съхраняваните данни по чл. 2516, ал. 1, т. 1, 3 и 5 от ЗЕС, **ще позволи** на КЗК да:

- идентифицира крайния ползвател - физическо или юридическо лице, страна по договор за достъп до интернет с доставчика на услугата;
- дата и часа на ползване на услугата и IP адресите, чрез който е ползвана услугата за достъп до интернет за последните 6 месеца;
- местоположението на крайната точка на мрежата, чрез която се ползва услугата за достъп до интернет в определено местоположение.

Данните по чл. 2516, ал. 1, т. 1, 3 и 5 от ЗЕС сами по себе си **няма да позволят на КЗК да:**

- идентифицира всички крайни ползватели, които са свързани с локалната мрежа на крайния ползвател, за който е определен IP адреса;
- установи с кои сървъри/клиенти е осъществена връзка от страна на крайния ползвател през последните 6 месеца.

2. Необходим ли е достъпът до данни, съхранявани по реда на чл. 2516, ал. 1 от ЗЕС, за целите на доказване на нарушения по чл. 15 от ЗЗК от КЗК?

От мотивите на вносителя на проекта на ЗИД на ЗЗК⁶ става ясно, че целта на предложението за предоставяне на правомощия на КЗК да иска достъп до данни за трафика е било преди всичко да се улесни доказването на забранени споразумения между участници в процедури за възлагане на обществени поръчки, насочени към тяхното манипулиране (т.нар. *bid rigging*). Според мотивите на законопроекта е необходимо събирането на достатъчно данни за наличието на координирани действия от страна на кандидатите, които имат за цел или резултат манипулирането на обществените поръчки. За целта КЗК разчита в преобладаващите случаи на косвени доказателства, които като съвкупност свидетелстват за наличие на забранено споразумение. Правомощието на КЗК да изисква достъп до тези данни, съхранявани на основание ЗЕС, е мотивирано от вносителя за *повишаване*

⁵ За територията на Европа организацията, която разпределя IP адресни ресурси на интернет доставчиците, е RIPE NCC (Réseaux IP Européens Network Coordination Centre).

⁶ Вж. т. 14 от мотивите на законопроект с номер 51-554-01-156, <https://www.parliament.bg/bills/51/51-554-01-156.pdf>

ефективността и ефикасността на Комисията при извършване на проучвания за евентуално извършени нарушения по ЗЗК, процесуална икономия, повишаване на справедливостта, прозрачността и конкуренцията при провеждане на процедури за възлагане на обществени поръчки и при разходването на публични средства.

КЗК, в подкрепа на законопроекта уточнява, че е необходимо да установи подаването на оферти от един и същи IP адрес, което се счита за индикатор на тръжна манипулация. В подкрепа на тази необходимост, КЗК поддържа, че „има ключови актове, насоките на ОИСП, известие на Европейската комисия относно инструментите за борба с тайните споразумения при възлагането на обществени поръчки, публикуването от Европейската служба за борба с измамите OLAF наръчник, озаглавен „Измами в областта на обществените поръчки“⁷ Според КЗК, възможността да получи достъп до трафичните данни е необходима само в контекста на евентуални нарушения на чл. 15 от ЗЗК, при които се изисква да се докаже наличието на съгласуваност на поведението между конкурентни предприятия чрез комуникация през различни канали между тях. Данните, които могат да бъдат изисквани и предоставяни на КЗК, биха послужили единствено за доказването на комуникация между определени конкуренти, е определен кратък период от време, с които като част от доказателствената верига би било доказано неоспоримо осъществяването на състава на чл. 15 от ЗЗК.⁸

Насоките на Организацията за икономическо сътрудничество и развитие („ОИСП“) за борба с договарянето на оферти при обществени поръчки посочват, че възложителите следва да имат достъп до цифровите версии на офертите. Предупредителни признаци („warning signs“) за идентични оферти или оферти със сходен формат или метаданни могат да бъдат оферти, които са били подадени от един и същ IP адрес, документи от различни участници, създадени от един и същ автор, и/или документи от различни участници, създадени по едно и също време или в близки моменти.⁹ С други думи, насоките на ОИСП дават индикативен списък на предупредителни признаци в метаданните на файловете на електронните оферти, но не изискват изследване на цялата комуникация по интернет от страна на лицата, подали тези оферти.

В Известието на Европейската комисия („ЕК“) относно инструментите за борба с тайните споразумения при възлагането на обществени поръчки и относно насоките за прилагане на съответното основание за изключване („Известие“) ¹⁰, също не е посочена необходимостта от събирането на трафични данни от предприятията, предоставящи обществени електронни съобщителни мрежи и услуги. Известието всъщност предлага на държавите-членки в съответствие с правото на ЕС и националното право в областта на защита на личните данни да обмислят възможността: i) да осигурят на своите органи за защита на конкуренцията достъп до електронните бази данни за обществените поръчки (например до наличните национални регистри на договорите) и до подадените оферти във връзка с проучвани към момента случаи; ii) да разрешат обмена на налична информация между органите за възлагане на обществени поръчки и за защита на

⁷ Протокол № 15 / 24.09.2025 г. от съвместно заседание на Комисията по икономическа политика и иновации и Постоянно действащата подкомисия за наблюдение на дейността в областта на защитата на потребителите и ограничаването на монополите, <https://www.parliament.bg/bg/parliamentarycommittees/3599/steno/9253>

⁸ Вж. т. I.5., стр. 4 от Становище вх. № КИПИ-51-520-00-7/22.10.2025 г. от КЗК по ЗИД на ЗЗК, № 51-554-01-156, https://www.parliament.bg/pub/cW/20251022123847_%D0%BA%D0%B8%D0%BF%D0%B8-51-520-00-7%20-%20%D0%BA%D0%B7%D0%BA%20%20--.pdf

⁹ Вж. 3.2., стр. 23 от OECD Guidelines for Fighting Bid Rigging in Public Procurement (2025 Update), https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/09/oecd-guidelines-for-fighting-bid-rigging-in-public-procurement-2025-update_127880ea/cbe05a56-en.pdf

¹⁰ Известие относно инструментите за борба с тайните споразумения при възлагането на обществени поръчки и относно насоките за прилагане на съответното основание за изключване 2021/C 91/01 (ОВ С 91, 18.3.2021), [https://eur-lex.europa.eu/legal-content/BG/ALL/?uri=CELEX:52021XC0318\(01\)](https://eur-lex.europa.eu/legal-content/BG/ALL/?uri=CELEX:52021XC0318(01))

конкуренцията, така че тези органи да могат да преценяват дали са налице модели на тайно споразумение между икономическите оператори; iii) да задължат възлагащите органи да уведомяват техните централни органи за възлагане на обществени поръчки и за защита на конкуренцията за случаи, в които са изключили икономически оператор поради подозрение за тайно споразумение. С Известието също така се предлага на държавите-членки да предвидят сътрудничество при анализ на данните за обществени поръчки, с цел по-лесно откриване на признаци на тайно споразумение в процедурите за възлагане. За тази цел държавите членки се насърчават да въведат на национално равнище ясни и лесни за прилагане методи за събиране и анализ на големи обеми от данни, налични в електронните бази данни за обществените поръчки (евентуално с помощта на алгоритми, алгоритми за изкуствен интелект или машинно самообучение).¹¹ От анализа на Известието може да се направи извод, че методите за разкриване на тръжни манипулации чрез анализ на електронни доказателства разчитат на анализ на данните в електронните бази данни за обществените поръчки, а не на данните за комуникация на крайните ползватели, които са съхранявани от предприятията, предоставящи обществени електронни съобщителни мрежи и услуги. С други думи, за целите на установяване на тръжни манипулации е необходим достъп до данните, които вече са налични в администратора на сървъра, а не информацията за клиента, съхранявана от интернет доставчика.

Наръчникът на Европейската служба за борба с измамите („OLAF“) „Измами в областта на обществените поръчки“ съдържа по-подробен списък от „червени флагове“ като индикатори за възможни тръжни манипулации.¹² Според OLAF тези индикатори не представляват доказателство за антиконкурентни споразумения, а по-скоро сочат, че е необходимо допълнително разследване от орган за защита на конкуренцията, за да се установи дали съществуват такива споразумения¹³. Цитираният наръчник на OLAF също не посочва необходимост от достъп до данни за трафика, съхранявани от предприятията предоставящи обществени електронни съобщителни услуги¹⁴.

КЗК е приела свои Насоки за противодействие срещу тръжните манипулации в процедурите за възлагане на обществени поръчки ведно със списък на обстоятелства, наличието на които обуславя съмнение за тръжни манипулации¹⁵, в които комисията посочва, че е налице съмнения за тръжна манипулация, когато заявления или оферти на различни предприятия са подадени от един и същ електронен или пощенски адрес. Последното явно не изисква изследване на данните, които се съхраняват от интернет доставчика на крайния ползвател, изпратил електронни заявления или оферти. Също така, актуалните Насоки на КЗК не посочват като предупредителен признак съвпадението на IP адреса на връзката, чрез която е подадена офертата, както и не посочват, че е необходимо КЗК да има достъп до данните, свързани с комуникацията на подадените оферти за участие в процедури за обществени поръчки.

В заключение, от прегледа на мотивите на законопроекта и цитираните от КЗК в подкрепа документи на ЕК, OLAF и ОИСР, не може да се направи извод, че за

¹¹ *Ibid*, т. 4, стр. 9.

¹² European Commission, European Anti-Fraud Office (OLAF) (n.d.) Fraud in public procurement: A collection of red flags and best practices. Directorate D: Policy, Unit D.2: Fraud Prevention, Reporting and Analysis. Ref. Ares(2017)6254403 - 20/12/2017. <https://sfc.ec.europa.eu/system/files/documents/sfc-files/fraud-public-procurement-final-20122017-ares20176254403.pdf>

¹³ *Ibid*, стр. 31.

¹⁴ *Ibid*, стр. 25-39.

¹⁵ Решение № 972 от 19.11.2020 г. на КЗК, <https://www.cpc.bg/media/legislation/Guidelines/Bid-rigging%20Guidelines.pdf>

разкриване на нарушения на ЗЗК, по-специално тръжни манипулации е необходим достъп до данни, съхранявани на основание чл. 2516, ал. 1, т. 1, 3 и 5 от ЗЕС.

3. Съществуват ли други способи за събиране на доказателства за нарушения по чл. 15 от ЗЗК, в частност - на тръжни манипулации, които не налагат достъп до данните по чл. 2516, ал. 1, т. 1, 3 и 5 от ЗЕС при интернет достъп?

При оценката на съответствието на разпоредбите на ЗЕС, предмет на конституционното дело, следва да се отчетат възможните други подходи за събиране на електронни доказателства, които постигат същата цел без неоправдано да навлизат в личното пространство на гражданите или да нарушават свободата и тайната на кореспонденцията.

Съгласно чл. 39а, ал. 1 от Закона за обществените поръчки („ЗОП“) при възлагането на обществени поръчки се използва централизирана електронна платформа. Стопанските субекти използват платформата при подаване на заявления за участие, оферти и конкурсни проекти. Съгласно чл. 9а, ал. 2 от Правилника за прилагане на ЗОП („ПЗОП“), *„платформата поддържа запис за всяка операция, извършена от потребителите, свързана с възлагането на обществени поръчки, включително данни за създаването и обмена на документи, както и за отделните участници в операциите. Записите са доказателствено средство за цялостност и пълнота на информацията в нея, както и за авторството и времето на всяко действие“*. Събирането на данни за използваните IP адреси при обмена на пакети от данни на мрежово ниво при изпращане на офертите се осъществява при спазване на Общия регламент за защита на данните („ОРЗД“)¹⁶, който принципно допуска Агенцията за обществените поръчки („АОП“) да предостави на КЗК справка от записите на съответните операции в платформата.

Пример за събиране на електронни доказателства от КЗК - IP адреси при влизане в централизираната електронна платформа - може да бъде открит в производството, завършило с Решение № 1254 от 21.11.2024 г.¹⁷ Видно от мотивите на решението на КЗК, в предоставените от АОП данни се съдържат всички други действия, извършени във всеки от профилите във времето, в което потребителят (адвокатът) е бил активен в съответния профил. Тъй като системата записва всяко едно действие и точното му време на извършване, не е възможно в таблицата да бъдат включени всички действия, извършени в рамките на деня, поради огромния им брой. Затова са представени единствено действията влизане и излизане от профилите, за да се покаже последователността на работа в профилите на страните в ЦАИС ЕОП, която последователност заедно с доказателствата за еднакия IP адрес доказват, че едно и също лице борава с тези профили. В тази връзка е ненужно да се събират данни за часовете на подаване на офертите на други участници, тъй като изводите на Комисията не почиват единствено на часовете на подаване на офертите, а **също така и на еднакия IP адрес и последователността на работа в профилите на страните**. Следователно, КЗК може да получи необходимата информация от АОП, за да докаже подаването на оферти чрез един и същи IP адрес от участници в процедурата.

В описаната хипотеза КЗК и АОП не се подчиняват на ограниченията, предвидени със ЗЕС, а единствено на общите правила за обработване на лични данни, съгласно ОРЗД.

¹⁶ Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните), ОВ L 119, 4.5.2016.

¹⁷ Отменено от АССО на първа инстанция, Решение № 940 от 07 юли 2025 г. по а.д. № 1518/2024 г. по описа на АССО, обжалвано пред ВАС, а.д. № 12059/2025 г.

АОП може да съхранява информацията за по-дълъг период време от предвидения в ЗЕС. При действието на разпоредбите на ЗЕС, предмет на конституционното дело, КЗК може да иска достъп до данни за последните 6 месеца, считано от датата на искането, след което данните се изтриват. Това означава, че в рамките на изключително кратък период от 6 месеца, считано от датата на електронно подаване на офертите, КЗК е следвало да образува производство, да събере информация от АОП и мотивирано да изиска разрешение от съда за достъп до данните по чл. 251б, ал. 1, т. 1, 3 и 5 от ЗЕС. Въпреки, че това не е напълно изключено, новите правомощия на КЗК едва ли ще доведат до събиране на релевантни данни, защото необходимите данни ще бъдат вече заличени и така или иначе КЗК ще трябва да използва единствено информация от сървърите на АОП, за която не се прилагат ограниченията, предвидени в ЗЕС.

Следователно, за установяване на индикации за нарушение по чл. 15 от ЗЗК под формата на тръжна манипулация е необходимо КЗК единствено да изисква от АОП данните, съхранявана по реда на ППЗОП. За установяването от КЗК на използването на един и същ IP адрес и времето на подаване на офертите не е необходима информацията, съхранявана от предприятията, предоставящи достъп до интернет, на основание чл. 251б, ал. 1, т. 1, 3 и 5 от ЗЕС. При всички положения, тези данни не са определящи за доказването на нарушения по чл. 15 от ЗЗК, а може да са само предупредителен признак за наличие на тръжна манипулация.

4. Несъответствие на оспорваните разпоредби на ЗЕС с Конституцията.

Събирането и запазването на данни от телекомуникационен трафик само по себе си не представлява дейност, забранена от Конституцията или такава, която поначало следва да бъде отрецена.¹⁸ В практиката на КС последователно се поддържа, че правото на неприкосновеност на личния живот не е абсолютно¹⁹ и може да бъде ограничено по начин, съразмерен с обстоятелствата.

КС е имал възможност нееднократно да преценява противопоставянето на конкуриращи се основни права, основани на конституционно защитени ценности и интереси. Относими за настоящото дело са Решение № 2 от 12.03.2015 г. по по к.д. № 8/2014 г., с което са обявени за противоконституционни чл. 250а - чл. 250е, чл. 251 и чл. 251а от ЗЕС в редакция ДВ, бр. 14/2015 г., както и Решение № 15 от 17.11.2020 г. по к.д. № 4/2020 г., с което са обявени за противоконституционни чл. 251б, ал. 2, изр. трето, чл. 251 в, ал. 2, изр. второ, чл. 251 г, ал. 5 относно думите „и в случаите по чл. 251б, ал. 2, изречение трето“ и чл. 251 г¹, ал. 1, изр. второ, ал. 3 и 4 относно думите „и чл. 251 в, ал. 2, изречение второ“ от ЗЕС в редакция ДВ, бр. 28/2020 г. В тези решения, КС подчертава, че *макар и въведен като средство за постигането на една легитимна цел от общ интерес, както за Европейския съюз, така и за всяка национална държава, за да бъде оценен като необходим, подходящ и съразмерен в условията на едно демократично общество, режимът на събиране и запазване на данните от целия телекомуникационен трафик (общо и без повод), така и достъпът до тях, безспорно представлява сериозна намеса в личния живот на гражданите и следва да бъде уреден по начин, съобразен с най-високите възможни стандарти на сигурност.*

Според КС, *традиционното разбиране за неприкосновеност на личния живот се свързва с правото на определена сфера на автономност на индивида, преди всичко в отношенията с публичната власт. Неприкосновеността на личния живот принадлежи към първото поколение основни права, насочени към защитата на физическия и духовния*

¹⁸ Решение № 2/2015 г. на КС по к.д. № 8/2014 г., Решение № 15/2020 г. на КС по к.д. № 4/2020 г.

¹⁹ Решение № 15/2020 г. на КС по к.д. № 4/2020 г. и цитираната там практика.

интегритет на човешката личност и по-специално автономията, и частната сфера на индивида. Тази категория права се утвърждава във всички съвременни конституции и се ползва с изключително висока степен на правна защита, както в националните демократични правни системи, така и в международните и европейските системи за защита на основните права²⁰. Гарантираната от чл. 32, ал. 1 на Конституцията неприкосновеност обхваща всички аспекти на личния живот, включително „информационно самоопределение“, създаване и поддържане на взаимоотношения и контакти с други лица и пр. - своеобразен комплекс от ценности, които не се поддават на изчерпателно дефиниране и формират обособената интимна сфера на човека, за навлизането в която трябва да съществува преграда²¹. Правото на неприкосновеност на личния живот, уредено в чл. 32, ал. 1 от Конституцията включва и възможността на индивида да решава принципно самостоятелно кога и при какви граници да разкрива лична информация за живота си, както и правото на всяко лице автономно (лично) да реши доколко и пред кого да сподели факти от личния си живот²².

Правото на неприкосновеност на личния живот не е абсолютно и може да бъде ограничено по начин, съразмерен с обстоятелствата. Източник на такива ограничения могат да са основните права на другите и защитени от Конституцията блага. КС подчертава, че правото на неприкосновеност на личния живот не е абсолютно и може, но само при спазване на изискванията на чл. 8 от Конвенцията за защита правата на човека и основните свободи, да бъде ограничавано със закон, да преследва една или повече легитимни цели, и, което е съществено - ограничаването да е необходимо в демократичното общество. КЗПЧОС предвижда в чл. 8 (2) изчерпателен списък на целите, легитимиращи ограничаването на това право, като посочва *inter alia* защитата на правата и свободите на другите. Хартата на основните права на Европейския съюз е формулирана по-отворено и допуска ограничаване за цели от общ интерес, признати от ЕС, или ако ограниченията отговарят на необходимостта да се защитят правата и свободите на други хора, при спазване на принципа на пропорционалност (чл. 52 (1) ХОПЕС).²³

С оспорените разпоредби, предмет на настоящото дело, се въвежда ограничение на правото на неприкосновеност на личния живот с ясно формулирана цел - необходимост от събиране на електронни доказателства за улесняване на установяване на нарушения по чл. 15 от ЗЗК, съгласно който се забраняват споразумения, решения и съгласувани практики между предприятия, които имат за цел или резултат предотвратяване, ограничаване или нарушаване на конкуренцията. По-специално, целта е доказването на наличието на индикации на тръжна манипулация като форма на антиконкурентно споразумение между участниците в процедура на възлагане на обществена поръчка. Предотвратяването на нелоялната конкуренцията е посочена измежду основните начала с чл. 19 от Конституцията, но постигането на тази цел ще отговаря на Конституцията, ако ограничаването на основните права на гражданите е съразмерно.

Чрез предвидения с атакуваната уредба правен режим за предоставяне на достъп до трафични данни по чл. 251б, ал. 1, т. 1, 3 и 5 от ЗЕС, съхранявани в продължение на 6 месеца, няма да се разкрива съдържанието на съобщенията, което принципно важи за цялата рамка на съхраняване на данни на основание ЗЕС. Съхраняването на данни за трафика при използване на достъп до интернет само себе си засяга правото на свобода и тайна на кореспонденцията и ограничава изпращането на съобщения чрез електронно съобщителни услуги, особено ако се касае за комуникация на или с лица, които са

²⁰ Решение № 4/2006 г. на КС по к. д. № 11/2005 г., Решение № 15/2020 г. на КС по к.д. № 4/2020 г.

²¹ Решение № 15/2020 г. на КС по к.д. № 4/2020 г. и цитираните там решения.

²² Решение № 15/2020 г. на КС по к.д. № 4/2020 г.

²³ Решение № 15/2020 г. на КС по к.д. № 4/2020 г.

задължени да спазват професионална или друга тайна или са податели на сигнали. На следващо място, чрез достъпът до съхраняваните данни по реда на чл. 2516 и сл. от ЗЕС може да бъде събрана чувствителна информация за начина на живот, навиците, придвижването, интересите, дори предпочитанията на субектите на данни - физическите лица, които ползват услугата за достъп до интернет. Посредством анализ дори само на данните, до които ще има достъп КЗК, могат да бъдат изградени профили за отделни индивиди или групи хора. Поведенческото профилиране е възможно като се направят изводи за трудова заетост, начин на живот, социален статус, работа от разстояние, работа на смени, географско използване на достъпа до интернет (работно място, у дома, работа от разстояние). Дългият период на съхранение на данните също така позволява да се прогнозира бъдещото поведение на ползвателите на достъп до интернет, напр. в кой момент от денонощието и къде използват достъп до интернет. Прогнозираното поведение се улеснява от пълното идентифициране на абоната на услугата, а при наличие на други данни, съхранявани от сървърите, с които се свързва крайния ползвател на достъп до интернет, ще бъде възможно да се разкрият частично и самите съобщения (какво съдържание е достъпвано от крайния ползвател на сървъра) и да се идентифицират лицата. Въпреки, че достъпът до данните по чл. 2516, ал. 1, т. 1, 3 и 5 от ЗЕС не разкрива съдържанието на самите съобщения, е налице съществена намеса в неприкосновеността на личния живот, тъй като дава възможност за профилиране на засегнатото лице чрез систематизиране на данни за шест месеца, които са свързани с навиците му за използване на достъп до интернет.

Следователно, комплексът от норми, предмет на конституционното дело, представлява съществена намеса в основни, конституционно защитени права на гражданите и следва да се третира като изключение от конституционните норми на чл. 32, ал. 1 и чл. 34, ал. 1. Съгласно изискванията на чл. 32, ал. 2 и чл. 34, ал. 2 от Конституцията изключенията следва да са уредени от закон; да се допускат само с разрешение на съдебната власт; и само когато това се налага за разкриване и предотвратяване на тежки престъпления.²⁴ В случая оспорената уредба изпълнява първото и второто конституционно изискване като Конституцията не допуска ограничаването на основни права на гражданите, когато не е предвидено за разкриване на тежки престъпления (чл. 34, ал. 2 от Конституцията). Поради това, въведените ограничения на основните права, прогласени от чл. 32, ал. 1 и чл. 34, ал. 1 от Конституцията, не могат да бъдат оправдани от целта за подпомагане или улесняване на доказването на административни нарушения по чл. 15 от ЗЗК. Доказването на нарушения по чл. 15 от ЗЗК безспорно е от обществено значение, но дейността на КЗК е насочена единствено към установяване на административни нарушения, което не оправдава ограничаването на основните конституционно-гарантирани права на неприкосновеност на личния живот и тайната на съобщенията. Само на това основание, атакуваните текстове на ЗЕС в тяхната цялост следва да се приемат за противоконституционни.

В становището на вносителя е отчетено, че принципно е необходимо КЗК да разполага с разширени способности и средства за доказване на тръжни манипулации. Счита се, че постигането на тази цел не следва да ограничава непропорционално конституционно гарантираната неприкосновеност на личния живот на гражданите и неприкосновеността на свободата и тайната на кореспонденцията и на другите съобщения. *В Конституцията принципът на пропорционалността в контекста на ограничаването на основните права не е изрично прогласен, но се съдържа имплицитно в редица правни конструкции. Този принцип има широко приложение в съвременната правова държава и доминиращо значение за контрола върху публичната власт, осъществяван с мащаба на основните*

²⁴ Решение № 2/2015 г. на КС по к. д. № 8/2014 г.

права. Прилага се като решаващ критерий за вида и обхвата на конституционно допустимите ограничения със закон, както и за определянето на конкретни граници при упражняване на основни права.²⁵ За законодателството принципът на пропорционалност е утвърден като необходим ориентир и мяра за съразмерност, когато се отнася за ограничаване на основни права. Постулатът за съразмерност присъства осезаемо в практиката на българския Конституционен съд с последователно развивано съдържание, като мерило за границите на търпима намеса на държавата в пространството на основните права²⁶

Възможността КЗК да изисква трафични данни и данни за идентификация на крайните ползватели на достъп до интернет, съхранявани общо и неизбирателно за период от шест месеца, с цел единствено да улесни доказването на нарушения по чл. 15 от ЗЗК се явява явно несъразмерно предвид контекста на обществените отношения, които са регулирани. На първо място, достъпът до тези данни не е необходим на КЗК за да приеме, че има предупредителни признаци за наличие на антиконкурентно споразумение, защото административният орган разполага с данни от други източници. КЗК може да изиска достъп до данните, съхранявани в централизираната електронна платформа за обществени поръчки от АОП, която да предостави данни за използваните IP адреси в съответствие с ОРЗД²⁷, доколкото е необходимо комисията да установи единствено използването на един и същ IP адрес на връзката, чрез която са подавани офертите. Без значение е кое лице е крайния ползвател на услугата за достъп до интернет, т.е. абоната по договора за услугата, както и кога и за колко време е използвал тази услуга през последните 6 месеца. Идентифицирането на конкретния краен ползвател, доколкото изобщо е възможно да се осъществи безспорно чрез данните по чл. 2516, ал. 1, т. 2 от ЗЕС, не е определящо за наличието на предупредителния признак за наличие на тръжна манипулация. В този смисъл, достъпът до данни за трафика и идентификацията на конкретния ползвател не е необходим за доказване на нарушение по чл. 15 от ЗЗК и са налице други мерки, които да постигат поставената цел за улесняване на доказването на нарушението без да е необходима описаната съществена намеса в основните права на гражданите.

КС приема, че когато държавите предприемат законодателни мерки, за да ограничат обхвата на правата, следва да отчитат, че всяко ограничение трябва да е съобразено със същността на основните права и свободи и да представлява необходима, подходяща и пропорционална мярка в рамките на демократичното общество, за да гарантира националната сигурност, отбрана, обществената безопасност и предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнение на наложени наказания, включително предпазването от и предотвратяването на заплахи за обществената сигурност или други важни цели от широк обществен интерес за Съюза или за държавите членки, и по-специално важен икономически или финансов интерес на Съюза или на държава членка, включително паричните, бюджетните и данъчните въпроси, общественото здраве, социалната сигурност (по арг. от чл. 23 ОРЗД).²⁸ Защитата на основното право на неприкосновеност на личния живот изисква ограниченията за защита на личните данни да се въвеждат в границите на строго необходимото. С атакуваните разпоредби се цели събиране на данни за улесняване на доказването на административни нарушения при положение, че съществуват други методи за събиране на тези доказателства, сериозната

²⁵ Решение № 15/2020 г. на КС по к.д. № 4/2020 г.

²⁶ Решение № 15/2020 г. на КС по к.д. № 4/2020 г. и цитираните там решения.

²⁷ Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните), ОВ L 119, 4.5.2016.

²⁸ Решение № 15/2020 г. на КС по к.д. № 4/2020 г.

намеса в основните права на гражданите не се явява строго необходима и пропорционална, поради което следва да се приеме, че не съответства на Конституцията.

5. Несъответствие на оспорваните разпоредби на ЗЕС с правото на ЕС.

Считам, че оспорените разпоредби взети в тяхната цялост противоречат на чл. 15(1) във връзка с чл. 6 от Директива 2002/58/ЕО относно правото на неприкосновеност на личния живот в сектора на електронните комуникации Директива („Директива 2002/58/ЕО“)²⁹. Съгласно чл. 15(1) от Директива 2002/58/ЕО, 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, както е посочено в член 13, параграф 1 от Директива 95/46/ЕО. В тази връзка чл. 6 от Директива 2002/58/ЕО изрично изисква данните за трафика, отнасящи се до абонати и **потребители**³⁰, обработени и съхранени от доставчика на публични комуникационни мрежи или публично достъпни електронни комуникационни услуги, трябва да бъдат изтрети или да се направят анонимни, когато не са необходими повече за целите на предаване на комуникация, без да засяга използването на данните за изготвяне на сметки, плащания за взаимно свързване, маркетинг на услуги или решаване на спорове. Чл. 15(1) от Директива 2002/58/ЕО отразява чл. 8 от Европейската конвенция за правата на човека („ЕКПЧ“) и се прилага по отношение на всички потребители на услуги, включително за бизнес цели, независимо от това дали са абонати по договор за електроннообщителна услуга или само ползватели на услугата (последното е обичайния контекст, когато се касае за служители в предприятия). Директива 2002/58/ЕО защитава и легитимните интереси на абонати, които са юридически лица, вкл. конфиденциалността на техните съобщения и свързаните трафични данни³¹.

От значение за точното тълкуване и приложение на чл. 15(1) от Директива 2002/58/ЕО е тълкуването, залегнало в jurisprudence на СЕС. След отмяната с Решение от 08 април 2014 г. по обединени дела C-293/12 и C-594/12 *Digital Rights Ireland Ltd* на Директива 2006/22/ЕО за запазване на данни, създадени или обработени, във връзка с предоставянето на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи и за изменение на Директива 2002/58/ЕО през 2014 г., СЕС се е произнасял в редица решения относно съответствието на национално законодателство на държавите-членки с правото на ЕС:

²⁹ 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), ОВ ОВ L 201, г., последно изменение с Директива 2009/136/ЕО, <https://eur-lex.europa.eu/legal-content/BG/TXT/HTML/?uri=CELEX:02002L0058-20091219>

³⁰ Съгласно чл. 2, б. „а“ от Директива 2002/58/ЕО, „потребител“ означава всяко физическо лице, използващо публично достъпни електронни комуникационни услуги за частни или бизнес цели, без да е необходимо да се е абонира за тази услуга.

³¹ Съгласно чл. 1(2) от Директива 2002/58/ЕО. Чл. 8 от ЕКПЧ също защитава кореспонденцията на юридическите лица (*Ekimdzhiev and Others v. Bulgaria*, no. 70078/12, § 374, 11 януари 2022).

В решението си по делата *Tele2 Sverige* и *Watson*³² СЕС е постановил, че правото на ЕС не допуска общо запазване на трафични данни и данни за местоположението, но допуска съхраняването на данни по целенасочен начин. Такова съхраняване трябва да бъде ограничено до строго необходимото, като се отчитат категориите данни, които се запазват, засегнатите средства за комуникация, лицата, до които се отнасят данните, и избрания срок на съхранение. Достъпът на националните органи до съхранените данни следва да бъде ограничен до целта за борба с тежката престъпност и трябва да бъде подчинен на предварителен контрол от независим орган. В *Ministerio Fiscal*³³, СЕС посочва, че достъпът до запазени трафични данни и данни за местоположението може да бъде оправдан за разкриване на престъпления, ако не представлява сериозно нарушение на основни права. В решението по C-511/18, *La Quadrature du Net и др.*³⁴ СЕС потвърди забраната на общо и неизбирателно съхраняване на тези данни, но допусна някои законодателни мерки при специфични цели и условия: i) общото и неизбирателно съхраняване на данни е позволено единствено при сериозна заплахата за националната сигурност, която е реална и предвидима, като решението подлежи на ефективен съдебен или независим контрол; ii) целево запазване на данни, ограничено по категории лица или географски критерий, за ограничен период за целите на опазването на националната сигурност, борбата с тежката престъпност и предотвратяването на сериозни заплахи срещу обществената сигурност; iii) общо и неизбирателно запазване на IP адреси за ограничен период за целите на опазването на националната сигурност, борбата с тежката престъпност и предотвратяването на сериозни заплахи срещу обществената сигурност; iv) общо и неизбирателно запазване на данни за идентифициране на потребителите на електронни съобщителни услуги за целите на опазването на националната сигурност, на борбата с престъпността и на опазването на обществената сигурност; v) задължение за доставчиците на електронни съобщителни услуги да извършват ускорено запазване на трафични данни и данни за местоположението за определен период, след решение на компетентен орган и ефективен съдебен контрол. Тези мерки трябва да гарантират, че запазването на данни се извършва при спазване на съответните материални и процесуални условия и че засегнатите лица имат ефективни защиты срещу риска от злоупотреби. Съдът уточнява още, че автоматизираният анализ и събирането на трафични данни и данни за местоположението в реално време от доставчици е позволено само в специфични ситуации и при определени условия. Освен това националните наказателни съдилища трябва да игнорират информация и доказателства, получени чрез общо и безразборно запазване на данни в нарушение на правото на ЕС, ако: i) лицата, срещу които се водят производства, не могат да се произнесат ефективно по тези доказателства; и ii) информацията и/или доказателствата се отнасят до област, с която съдиите нямат познания и която може да окаже съществено влияние върху установяването на фактите. Принципните положения в *La Quadrature du Net и др.* са повторени от СЕС в *Commissioner of An Garda Síochána*³⁵ и *SpaceNet и Telekom Deutschland*³⁶.

В решението по C-746/18, *Prokuratuur*³⁷ СЕС е уточнил, че член 15, параграф 1 от Директива 2002/58 във връзка с членове 7, 8 и 11 и с член 52, параграф 1 от Хартата [Харта на основните права на ЕС] трябва да се тълкува в смисъл, че **не допуска**

³² Решение от 21 декември 2016 г., *Tele2 Sverige AB срещу Post- och telestyrelsen и Secretary of State for the Home Department срещу Tom Watson и др.*, C-203/15 и C-698/15, ECLI:EU:C:2016:970.

³³ Решение от 2 октомври 2018 г., *Ministerio Fiscal*, C-207/16, ECLI:EU:C:2018:788.

³⁴ Решение от 6 октомври 2020 г., *La Quadrature du Net и др.*, C-511/18, ECLI:EU:C:2020:791.

³⁵ Решение от 5 април 2022 г., *G.D. v Commissioner of An Garda Síochána and Others*, C-140/20, ECLI:EU:C:2022:258.

³⁶ Решение от 20 септември 2022 г., *Bundesrepublik Deutschland срещу SpaceNet AG и Telekom Deutschland GmbH*, C-793/19 и C-794/19.

³⁷ Решение от 2 март 2021 г., *H.K. v Prokuratuur*, C-746/18, ECLI:EU:C:2021:152.

национална правна уредба, позволяваща достъпа на публични органи до съвкупност от данни за трафик или данни за местонахождение, които могат да предоставят информация за комуникациите, извършени от ползвател на средство за електронна комуникация, или за местонахождението на използваните от него крайни устройства и да позволят да се направят точни изводи относно неговия личен живот, за целите на предотвратяването, разследването, разкриването и преследването на престъпления, без този достъп да е ограничен до производствата за борба с тежката престъпност или за предотвратяване на сериозни заплахи за обществената сигурност, независимо от продължителността на периода, за който е поискан достъпът до посочените данни, и от обема или вида на наличните данни за подобен период.

С *Giudice delle indagini preliminari presso il Tribunale di Bolzano*³⁸, СЕС потвърждава установената съдебна практика, съгласно която достъпът до трафични данни или данни за местоположението може да се предостави само ако тези данни са били запазени от доставчиците в съответствие с Директива 2002/58/ЕО, която не допуска законодателни мерки, предвиждащи за тази цел превантивно общо и неизбирателно запазване на данни за трафик и за местонахождение³⁹. Достъп до трафични данни или данни за местоположението представляват сериозна намеса в закрепените в членове 7 и 8 от Хартата основни права на ЕС („ХОПЕС“) като се има предвид, че от тези данни може да се извлече информация за комуникациите на ползвателите на средства за електронна комуникация или за местонахождението на използваните крайни устройства, както и да се направят точни изводи относно личния живот за лицата, като други фактори, свързани с пропорционалността на такова искане за достъп, като например продължителността на искания достъп до данните, не могат да доведат до обосноваването на достъпа с общата цел за предотвратяване, разследване, разкриване и преследване на престъпленията.⁴⁰ За целта трябва да се установи дали достъпът до трафични данни или данни за местоположение, представлява сериозна намеса в основните права по членове 7 и 8 от ХОПЕС⁴¹. В случай, че се установи че се касае за сериозна намеса в основните права, достъпът до трафични данни или данни за местоположението може да бъде оправдан само поради необходимост от борба със сериозни нарушения - тежки престъпления или сериозна заплаха за обществената сигурност, като точния обхват на понятието „сериозни нарушения“ се определя от националното право.⁴²

В случая, предоставяният достъп на КЗК до данните по чл. 251б, ал. 1, т. 1, 3 и 5 от ЗЕС отговаря на критериите за сериозна намеса в основните права по членове 7 и 8 от ХОПЕС, тъй като дава възможност за профилиране на засегнатите лица чрез систематизиране на данни за шест месеца за използване на услуга за достъп до интернет. Това не се променя от изложеното по-горе за невъзможността винаги да бъде идентифицирано конкретното лице, което в даден момент ползва достъпа до интернет, поради това че пълният анализ на данните ще позволи да се различат отделни лица, които ползват достъпа до интернет, особено ако са налице и други данни за достъпването съдържание. Като се има предвид, постоянната практика на СЕС, съгласно която съхраняването и достъпът до данни за трафика или данни за местоположението представлява сериозна намеса в основни права, която може да бъде оправдан само поради необходимост от борба със сериозни нарушения (тежки престъпления или сериозна заплаха

³⁸ Решение от 30 април 2024 г., *Giudice delle indagini preliminari presso il Tribunale di Bolzano*, C-178/22, ECLI:EU:C:2024.

³⁹ *Ibid*, т. 35 и цитираната там съдебна практика.

⁴⁰ *Ibid*, т. 36 и цитираната там практика.

⁴¹ *Ibid*, т. 37-39 и цитираната там практика.

⁴² *Ibid*, т. 36 и цитираната там практика

за обществената сигурност), следва да се приеме, че атакуваните разпоредби, предмет на конституционното дело, противоречат на чл. 15(1) от Директива 2002/58/ЕО и членове 7 и 8 от ХОПЕС.

6. Несъответствие на оспорваните разпоредби на ЗЕС с общопризнати норми на международното право и с международните договори, по които България е страна.

Оспорените разпоредби противоречат на чл. 8 от Конвенцията за защита на правата на човека и основните свободи („КЗПЧОС“), чл. 12 от Всеобщата декларация за правата на човека, както и с чл. 5 и чл. 17 от Международния пакт за граждански и политически права. В тази връзка, КС е имал възможност да посочи, че „правото на неприкосновеност на личния живот не е абсолютно и може, но само при спазване на изискванията на чл. 8 от Конвенцията за защита правата на човека и основните свободи, да бъде ограничавано със закон, да преследва една или повече легитимни цели, и, което е съществено - ограничаването да е необходимо в демократичното общество“⁴³. Съгласно чл. 8(2) от КЗПЧОС, намесата на държавните власти в упражняването на правото на личен живот е недопустима, освен в случаите, предвидени в закона и необходими в едно демократично общество в интерес на националната и обществената сигурност или на икономическото благосъстояние на страната, за предотвратяване на безредици или престъпления, за защита на здравето и морала или на правата и свободите на другите.

От значение за конституционното дело е решението *Škoberne v. Slovenia*⁴⁴, където ЕСПЧ систематизира своята практика във връзка със съхраняването и достъпа до трафични данни, данни за местоположението и данни за идентифициране на абонатите. ЕСПЧ приема, че данните за абонати, трафик и местоположение могат да се отнасят - самостоятелно или в комбинация - до „личния живот“ на засегнатите лица. Самото запазване на данни, свързани с личния живот на някого, представлява намеса в правото на това лице на зачитане на неговия или нейния „личен живот“. Това представлява и намеса в правото на зачитане на кореспонденцията на съответното лице. Последващото използване на съхранените данни няма значение за това заключение. Достъпът на властите до запазени данни обаче представлява допълнителна намеса в правото на зачитане на личния живот и комуникациите по член 8 от Конвенцията⁴⁵

Според ЕСПЧ, предвид технологичното и социално развитие в сферата на електронните комуникации, данните от комуникациите в днешно време могат да разкрият голямо количество лична информация. Ако бъдат получени от властите в голям мащаб, такива данни могат да бъдат използвани за рисуване на интимна картина на дадено лице чрез, *inter alia*, картографиране на социалните мрежи, проследяване на местоположението, картографиране на комуникационни модели и информация за това с кого е взаимодействало това лице. Следователно придобиването на такива данни чрез масово прихващане може да бъде също толкова натрапчиво, колкото и масовото придобиване на съдържанието на комуникациите, поради което тяхното прихващане, запазване и търсене от страна на властите трябва да се анализира чрез позоваване на същите гаранции, приложими за съдържанието. **Тази констатация се отнася и за общото запазване на комуникационни данни от доставчиците на комуникационни услуги и достъпа до тях от страна на властите в отделни случаи**, което трябва да бъде

⁴³ Решение № 8 от 2019 г. на КС по к.д. № № 4/2019.

⁴⁴ *Škoberne v. Slovenia*, no. 19920/20, 15 февруари 2024, ECHR 2024.

⁴⁵ *Ibid*, § 118 и цитираните там решения на ЕСПЧ.

придружено, *mutatis mutandis*, от същите гаранции, отнасящи се до тайното наблюдение.⁴⁶

Всяка намеса в правата на дадено лице по член 8 може да бъде оправдана съгласно член 8(2) само ако е предвидена от закона, преследва една или повече от легитимните цели, посочени в тази разпоредба, и е необходима в едно демократично общество за постигането на такава цел. *По въпроса дали една намеса е била „необходима в едно демократично общество“ за постигане на легитимна цел, националните органи разполагат с определена свобода на преценка при избора на средствата за постигане на легитимните цели, inter alia, за защита на националната сигурност или за предотвратяване и преследване на престъпления.*⁴⁷ При преценката на тази свобода се взимат предвид всички обстоятелства по делото, като например естеството, обхватът и продължителността на възможните мерки, основанията за тяхното разпореждане, органите, компетентни да ги разрешават, прилагат и контролират, както и видът на средството за защита, предвидено в националното право.

Следва да се приеме, че съхраняването и достъпа до данни за трафика и идентификация на крайния ползвател на достъпа до интернет, предвидена с разпоредбите на ЗЕС, предмет на конституционното дело, поначало представляват сериозна намеса в правата по чл. 8 от КЗПЧОС. Системното наблюдение, произтичащо от задължителното запазване на данни за електронни съобщения, представлява пречка за упражняването на правото на неприкосновеност на личния живот на всички ползватели на електронни съобщителни услуги. Съществуването на големи масиви от данни за електронни съобщения, продължаващото съхраняване и достъп на държавните органи на такива данни по разбираем начин може да породи чувство на уязвимост и беззащитност и да накърни възможността на лицата да се ползват от правото на личен живот и тайната на кореспонденцията, да развиват отношения с други лица и да упражняват други основни права.⁴⁸

Забраната в чл. 15 от ЗЗК за сключването на всякакъв вид споразумения между предприятия, решения на сдружения на предприятия, както и съгласувани практики надве или повече предприятия, които имат за цел или резултат предотвратяване, ограничаване или нарушаване на конкуренцията на съответния пазар, по съществото си не съставлява престъпление, а е административно нарушение. За нарушение на тази забрана не се носи наказателна отговорност, а административнонаказателна отговорност, като е предвидена имуществена санкция за участвалите в тайното споразумение предприятия. Следователно, предвидените в ЗЕС правомощия на КЗК не целят разкриване на престъпления, а на административно нарушение, което не отговаря на изискванията, заложили в КЗПЧОС и практиката на ЕСПЧ за допустимост на сериозната намеса в правата на лицата, гарантирани от чл. 8 от КЗПЧОС. В случая не се преследват цели, които ЕСПЧ да признава като допустими основания за ограничаване на правата на лицата, а именно борба с престъпността или заплахата за обществената сигурност, както и не отговарят на изискванията за справедлив баланс между целите и ограниченията на правата, гарантирани от КЗПЧОС.

УВАЖАЕМИ ГОСПОЖИ И ГОСПОДА КОНСТИТУЦИОННИ СЪДИИ,

Считам, че оспорените разпоредби не съответстват на чл. 32, ал. 1 от Конституцията, защото представляват съществена намеса в личното пространство на гражданите, която не

⁴⁶ *Ibid*, в § 119 и цитираните там решения на ЕСПЧ.

⁴⁷ *Ibid*, в § 124 и цитираните там решения на ЕСПЧ.

⁴⁸ *Ibid*, в § 133 и цитираните там решения на ЕСПЧ.

съответства на гарантираната неприкосновеност на личния живот. Достъпът до данните нарушава и основното право на свобода и тайна на кореспонденцията, гарантирано от чл. 34, ал. 1 от Конституцията, защото засяга възможността на лицата да се ползват от правото на свобода и тайна на кореспонденцията, да развиват отношения с други лица и да упражняват други основни права чрез използване на електронни съобщителни услуги.

Ограничаването на основните права на гражданите не следва да бъде оправдано единствено с улесняване на доказването от страна на КЗК на административни нарушения, независимо от това каква е тяхната тежест. Предвидената съществена намеса в основните права и свободи на гражданите е също така непропорционална, защото не е абсолютно необходима за целите на разкриване и доказване на конкретната категория административни нарушения като съществуват други надеждни и ненарушаващи личното пространство подходи за събиране на електронни доказателства. Поради това оспорените разпоредби като цяло не съответстват на принципа на пропорционалност, а намесата в правата на гражданите е неоправдана с оглед преследваната цел. В заключение считам, че предвидената възможност за достъп до съхранявани трафични данни по реда на ЗЕС за целите на разкриване на административни нарушения по чл. 15 от ЗЗК е опасна тенденция на продължаващи опити за ерозия на основни права, гарантирани от Конституцията.

15 януари 2026 г.
гр. София

Georgi
Todorov
Sulev

Digitally signed
by Georgi
Todorov Sulev
Date: 2026.01.15
18:09:45 +02'00'

адв. Георги Сулев