Препоръчан начин за цитиране на публикацията:

Млъчков, Б. Съхраняването на трафични данни в Република България. // Предизвикай правото!, 2024, № 2, с. 1–1

Автор: **Богдан Млъчков**

Съхраняването на трафични данни в Република България

Ключови думи: съхраняване, трафични, данни, разследване, престъпления, доставчици, услуги, електронни, съобщения, България.

Резюме: Трафичните данни са един от основните видове електронни доказателства, както и особено важен инструмент в процеса по наказателно преследване на извършителите на престъпления. Поради това темата за съхраняването на трафичните данни от доставчиците на електронни съобщителни услуги е особено чувствителна. Тя е редовна предпоставка за значителни обществени вълнения, тъй като засяга в съществена степен редица въпроси, свързани с неприкосновеността на личния живот на гражданите. Статията представя развитието на българската нормативна уредба в тази област, вкл. в светлината на приложимите европейски актове и на практиката на Конституционния съд и на Съда на Европейския съюз.

Въведение

Трафичните данни[1], т.е. свързаните с провежданата комуникация данни, наричани още метаданни[2] или комуникационни данни, представляват един от основните видове електронни доказателства и са съществено важен инструмент в процеса по наказателно преследване на извършителите на престъпления. Те не са в състояние да докажат извършването на дадено престъпно деяние без събирането на допълнителен доказателствен материал, но предоставят необходимите първоначални

[1] Трафичните данни по-конкретно включват: източника (изпращач) на съобщението, неговото местоназначение (адресат), пътя, времето на изпращане, датата на изпращане, размера, продължителността на проведената комуникация, както и неуспешните опити за повикване и обема на информацията, ако става дума за изпращане на данни. За улеснение данните за местоположението, т.е. данните, които се обработват в електронните съобщителни мрежи за определяне на географското местоположение на крайното устройство на потребителя, също са включени в понятието „трафични данни“, освен ако не е посочено друго.

[2] Според Брус Шнайер метаданните са „прозорец към личността ни“. Виж **Schneier, B.** Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World (W.W. Norton and Co., 2015), p. 24.

следи, без които правоохранителните органи често биха били поставени пред съществени затруднения.

Темата за трафичните данни и събирането им от разследващите органи винаги е била особено чувствителна. Тя е редовна предпоставка за значителни обществени вълнения, тъй като засяга в съществена степен редица въпроси, свързани с неприкосновеността на личния живот на гражданите посредством информацията за лицата, с които комуникират, или местата, които посещават. Граждани и неправителствени организации реагират незабавно във всеки случай, в който се почувстват застрашени, и често предизвикват премисляне и промени в първоначалните планове на изпълнителната и законодателната власт[3]. Основният проблем се корени в липсата на доверие и в съмненията, че със събраната информация ще се злоупотреби. Това от своя страна създава множество подозрения и опасения, че е възможна намеса в личния живот на засегнатите лица и създаване на своеобразен „Биг Брадър“, в който антиутопията на Джордж Оруел ще се превърне в реалност.

Директива 2006/24/ЕО – крайъгълният камък на съхраняването на трафични данни

Материята относно съхраняването на трафични данни е предмет на уредба в правото на Европейския съюз, като през 2006 г. на основание чл. 15, пар. 1 от Директива 2002/58/ЕО[4] е приета Директива 2006/24/ЕО за запазване на данни, създадени или обработени във връзка с предоставянето на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи. Директива 2006/24/ЕО се основава и на принципите за защита на личните данни, предвидени в Директива 95/46/ЕО[5], която е в сила към момента на приемането на Директива 2006/24/ЕО. Директивата цели създаването на хармонизиран режим относно задълженията на доставчиците на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи за съхраняването на данни[6], за да се гарантира, че тези данни ще бъдат достъпни за целите на разследването на тежки

[3] В този смисъл България не прави изключение, виж https://www.mediapool.bg/obedinen-protest-sreshtu-sledeneto-na-trafichni-danni-i-gmo-news162006.html.

[4] 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.

[5] Директива 95/46/ЕО относно защитата на физическите лица при обработването на лични данни и за свободното движение на тези данни. Директивата е отменена от Общия регламент за защита на данните (Регламент (ЕС) 2016/679).

[6] Необходимо е да се уточни, че освен за целите на разследването на престъпления данни се съхраняват и за целите на фактурирането и плащането на сметки, както и за да се гарантира мрежовата сигурност или за други търговски цели, например маркетинг (в последните два случая само със съгласието на клиентите).

престъпления (съгласно съответната дефиниция в националното право на държавата членка)[7].

Директива 2006/24/ЕО се прилага за данни, създадени или обработени вследствие на изпращането на съобщение чрез електронна съобщителна услуга, като от обхвата ѝ е изключено съдържанието на изпратените съобщения[8]. В приложното поле на акта са включени трафичните данни, данните за местоположението и свързаните с тях данни, необходими за идентифицирането на регистрирания потребител (т. нар. потребителски данни[9]).

Решението по делото „Digital rights“ – краят на Директива 2006/24/ЕО

През 2014 г. Директива 2006/24/ЕО е обявена за недействителна[10] от Съда на Европейския съюз с решение по съединени дела C-293/12 и C-594/12 („Digital rights“)[11] на основание, че непропорционално ограничава правото на личен живот и правото на защита на личните данни на гражданите[12]. Според съда Директива 2006/24/ЕО не предвижда ясни и конкретни правила, които да определят обхвата на намесата в основните права, провъзгласени в чл. 7 и 8 от Хартата. Поради това се констатира, че от акта произтича твърде обширна за правния ред на Съюза намеса, без да са налице достатъчно гаранции, че при постигането на заложените цели тя се свежда единствено до строго необходимото. С приемането на този акт законодателят на Съюза надхвърля границите, наложени от зачитането на принципа за съразмерност с оглед прилагането на чл. 7, 8 и чл. 52, пар. 1 от Хартата, поради което съдът обявява Директива 2006/24/ЕО за недействителна.

Съдът по-конкретно посочва и че въведеното задължение за съхраняване на практически всички трафични данни при предаването на съобщения по фиксирани или мобилни телефонни мрежи, при интернет достъп и интернет телефония[13] означава, че се създава намеса в основните права на почти всички граждани на територията на

[7] Предложението за Директива е публикувано от Европейската комисия през септември 2005 г. вследствие на терористичните атаки в Мадрид (2004 г.) и Лондон (2005 г.). Виж **Feiler, L.** The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection. – European Journal of Law and Technology (2010), vol. 1, No. 3, p. 1.

[8] Чл. 5, пар. 2 от Директивата.

[9] Име, дата на раждане, адрес, данни, свързани с избрания начин на плащане и извършените и дължимите плащания, телефон, електронна поща, дата и час на регистрацията и др.

[10] Съгласно чл. 263 ДФЕС Съдът на Европейския съюз осъществява контрол относно законосъобразността на законодателните актове на основание липса на компетентност, съществено процесуално нарушение, нарушаване на Договорите или на всякаква правна норма, свързана с тяхното изпълнение, или злоупотреба с власт. За повече относно основанията за отмяна виж **Костов, С.** Актовете на Съда на Европейския съюз – правни последици. С.: Сиби, 2011, с. 66–68.

[11] https://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=BG&mode=lst&dir=&occ=first&part=1&cid=4591634.

[12] Двете дела имат за предмет преюдициални запитвания относно валидността на Директивата и са отправени на основание чл. 267 ДФЕС от High Court (Ирландия) и Verfassungsgerichtshof (Конституционен съд) (Австрия) с актове съответно от януари и ноември 2012 г.

Европейския съюз[14]. Обикновено лицата, чиито данни се съхраняват, не се намират, дори и непряко, във връзка с каквото и да положение, което би могло да даде повод за наказателно преследване. Освен това Директивата се прилага и за лица, чиито съобщения представляват професионална тайна съгласно националното право. Тя не изисква наличието на каквато и да е връзка на данните, които следва да бъдат запазени, с потенциална заплаха за обществената сигурност или с извършването на престъпление. Предвиденото съхраняване не е насочено единствено към данни, касаещи определен период от време, определена географска зона или определен кръг от лица, за които може да се предполага, че са участвали в извършването на престъпна дейност, или само към данни, които биха могли да допринесат за предотвратяването, разкриването или преследването на тежки престъпления. По този начин Съдът на Европейския съюз поставя основите на концепцията за т.нар. *„целенасочено“ съхраняване на данни*, която е доразвита в решението по делото „Tele2/Watson“ (съединени дела C- 203/15 и C-698/15) от декември 2016 г.[15].

Въпреки че цялостното решение на Съда на Европейския съюз за обявяване на Директива 2006/24/ЕО за недействителна безспорно има своите основания[16], представената в предходния абзац теза не може да бъде споделена. Не е разумно да се

---

[13] Според съда в приложното поле на задължението попадат всички широко разпространени електронни съобщителни средства, както и всички абонати и регистрирани ползватели, без да се въвежда каквото и да е разграничение, ограничение или още по-малко – изключение (виж т. 56 от решението). Изводът на съда по този въпрос не е напълно прецизен, доколкото извън задължението за съхраняване на трафични данни по Директива 2006/24/ЕО остават редица платформи, социални мрежи и други средства за предаване на съобщения (например Skype), които масово се използват към момента на постановяването на решението.

[14] Бившият министър на правосъдието на Федерална република Германия Забине Лойтхойсер-Шнаренбергер посочва, че цялостното съхраняване на трафичните данни може да подпомогне правоохранителните органи и особено да улесни работата на прокурорите, които са хронично претоварени. Въпреки това тя намира, че то не е решаващо за защитата на обществената сигурност, както често се твърди – следователно е непропорционално с оглед значителната намеса в основните права на гражданите. Виж **Leutheusser-Schnarrenberger, S.** Goodbye Vorratsdatenspeicherung: https://verfassungsblog.de/goodbye-vorratsdatenspeicherung/.

[15] Както метафорично изтъква Жулиета Мандажиева, решението по делото „Digital rights“ залага експлозив в основите на построените върху Директива 2006/24/ЕО национални закони, вменяващи задължения за съхраняването на данни, който избухва с решението по делото „Tele2/Watson“. Виж **Мандажиева, Ж.** „Запазване и достъп на „службите“ до трафичните данни на абонати на публични електронни съобщителни услуги в България и ЕС“: https://digrep.bg/new/safety-vs-security/.

[16] Съдът посочва, че Директива 2006/24/ЕО не предвижда какъвто и да е обективен критерий, който да позволи ограничаването на достъпа на компетентните национални органи до съхранените данни, доколкото в нея се съдържа единствено общо препращане към дефиницията за тежко престъпление съгласно вътрешното право на държавата членка. Освен това Директивата не урежда и материално- или процесуалноправни изисквания за събирането на данните от разследващите органи. Съдът добавя, че в акта не се предвижда и никакъв критерий, който да позволи ограничаването до строго необходимото на броя на лицата, които биха могли да получат разрешение за достъп до запазените данни и за последващото им използване. Още по-значителна критика е изразена по отношение на факта, че достъпът до данните не се предоставя след предварителен контрол от страна на съд или независима административна юрисдикция. Доколкото настоящата статия разглежда темата за съхраняването на данните, въпросите, свързани със събирането и достъпа до трафични данни, няма да бъдат предмет на обсъждане в нея.

очаква, че е възможно (дори от техническа гледна точка) доставчиците на услуги автоматично да съхраняват единствено данни, за които изначално е налично съмнение за връзка с извършването на определена престъпна дейност. Това е така, тъй като ако не е предвидено друго, данните следва да бъдат заличени незабавно след завършването на предаването на съобщението[17].

Същите разсъждения са в още по-голяма степен валидни и по отношение на съхраняването на данни, които попадат под закрилата на националните разпоредби за професионалната тайна, тъй като към момента на съхраняването доставчикът на услуги не би могъл да прецени кои данни имат именно такъв характер. Следва да бъде зададен въпросът как доставчикът предварително ще установи кои разговори адвокат или лекар провежда в професионално и кои – в лично качество, доколкото в правоотношението между клиент и доставчик професията на първия е ирелевантна и не се отразява по никакъв начин в договора между двете страни (ако такъв въобще е наличен).

Подобни аргументи биха могли да бъдат изтъкнати и с оглед ограничаването на съхраняването на данни до определени категории лица или до определена географска област, тъй като подобен подход ще отвори широко вратите за злоупотреби от страна на лица с престъпни намерения (например обажданията биха могли да се извършват единствено от зони извън обхвата на задълженията на доставчиците, телефонните номера биха могли да бъдат регистрирани на лица, които не попадат в приложното поле на задължението за съхраняване на данни и др.).

Първият опит за транспониране на Директива 2006/24/ЕО в българското законодателство

Първият опит за въвеждане в българското законодателство на разпоредбите на Директива 2006/24/ЕО е направен с Наредба № 40 от 7 януари 2008 г. за категориите данни и реда, по който се съхраняват и предоставят от предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, за нуждите на националната сигурност и за разкриване на престъпления[18]. С Наредбата се определят категориите данни за съхраняване; редът за съхраняването на данните; правилата за защитата и сигурността им, както и редът за достъп до тях. Категориите следват списъка в Директива 2006/24/ЕО[19], а според чл. 2 от Наредбата данните се съхраняват за срок от дванадесет месеца.

Съгласно чл. 5 от Наредбата за нуждите на оперативно-издирвателната дейност доставчиците на услуги осигуряват на дирекция „Оперативно-техническа информация“

[17] Чл. 6, пар. 1 от Директива 2002/58/ЕО.

[18] Издадена от министъра на вътрешните работи и председателя на Държавната агенция за информационни технологии и съобщения, обн. ДВ, бр. 9 от 29.01.2008 г., на основание чл. 251, ал. 2 от Закона за електронните съобщения, приет през 2007 г.

[19] Чл. 5, пар. 1 от Директивата.

при Министерството на вътрешните работи пасивен технически достъп чрез компютърен терминал до съхраняваните от тях данни. Съответно, за целите на наказателния процес доставчиците предават съхраняваните данни по писмено искане на разследващите органи, прокурора или съда.

Законосъобразността на Наредбата е оспорена пред Върховния административен съд от фондация „Програма достъп до информация“. Жалбоподателят посочва, че Наредбата е приета в нарушение на чл. 32 от Конституцията на Република България[20] и чл. 8 от Европейската конвенция за правата на човека (ЕКПЧ), които предвиждат подобни въпроси да се уреждат единствено с акт на законодателната власт, а чл. 5 от Наредбата[21] противоречи и на чл. 34 от Конституцията[22]. Фондацията твърди, че Наредбата надхвърля и обхвата на делегацията по чл. 251, ал. 2 от Закона за електронните съобщения (ЗЕС)[23], както и че в разпоредбите на подзаконовия нормативен акт не са предвидени каквито и да е изисквания за осъществяването на достъпа до съхранените данни от страна на оправомощената дирекция при Министерството на вътрешните работи.

С Решение № 8786 от 16 юли 2008 г. Върховният административен съд отхвърля изцяло жалбата срещу Наредбата като неоснователна, посочвайки, че актът е издаден от компетентен орган в рамките на предоставената от закона делегация. Не са открити причини и за отмяната на чл. 5 – съдът отбелязва, че предоставянето на запазените данни единствено на компетентни национални органи по тяхно писмено искане в специфични случаи представлява достатъчна гаранция. В първоинстанционното решение обаче е допуснат сериозен пропуск, тъй като по никакъв начин не са разгледани твърденията за противоречие на Наредбата с чл. 32 и 34 от Конституцията и чл. 8 от ЕКПЧ.

Фондация „Програма за достъп до информация“ подава жалба пред петчленен състав на Върховния административен съд, който с Решение № 13627 от 12 ноември 2008 г. отменя чл. 5 от Наредбата и потвърждава решението на първата инстанция в останалата му част.

---

[20] Чл. 32. (1) Личният живот на гражданите е неприкосновен. Всеки има право на защита срещу незаконна намеса в личния и семейния му живот и срещу посегателство върху неговата чест, достойнство и добро име.

(2) Никой не може да бъде следен, фотографиран, филмиран, записван или подлаган на други подобни действия без негово знание или въпреки неговото изрично несъгласие освен в предвидените от закона случаи.

[21] Жалбоподателят моли, в случай че не бъде уважена жалбата срещу Наредбата в цялост, да се обяви най-малко нищожността на чл. 5.

[22] Чл. 34. (1) Свободата и тайната на кореспонденцията и на другите съобщения са неприкосновени.

(2) Изключения от това правило се допускат само с разрешение на съдебната власт, когато това се налага за разкриване или предотвратяване на тежки престъпления.

[23] Чл. 251. (Обн., ДВ, бр. 41 от 2007 г.) (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.

Според касационната инстанция изводът в оспореното решение, че посоченият в Наредбата „пасивен технически достъп“ до съхранените данни е възможен единствено след подаването на писмено искане, е неправилен. В действителност разпоредбата не поставя такива ограничения по отношение на данните, до които се осъществява достъп, а изразът „за нуждите на оперативно-издирвателната дейност“ е твърде общ и не предоставя необходимите гаранции с оглед спазването на Конституцията и по-конкретно – неприкосновеността на личния живот на гражданите. От своя страна, уредената възможност за разследващите органи, прокуратурата и съда да изискват достъп до данни само след представяне на писмено искане не поставя условия, които да възпрепятстват възможната злоупотреба с конституционно гарантираните права на гражданите[24].

Намирам, че решението на петчленния състав за отмяната на чл. 5 от Наредбата е правилно, доколкото чл. 34, ал. 2 от Конституцията изисква във всички случаи разрешение на съдебната власт, за да се дерогира общият принцип за неприкосновеността на тайната на кореспонденцията, и то само когато това се налага за целите на разследването и разкриването на тежки престъпления – ограничение, което също не се съдържа в отменената норма от Наредбата. От своя страна, предвиденият „пасивен технически достъп чрез компютърен терминал“ създава неоправдано висок риск от нарушаване на чл. 32, ал. 2 от Конституцията, тъй като съответните служители на дирекция „Оперативно-техническа информация“ при Министерството на вътрешните работи биха могли произволно да получават достъп до съхраняваните от доставчиците данни.

След решението на Върховния административен съд през 2009 г. в чл. 251 ЗЕС[25] са приети изменения и допълнения, които „оцеляват“ до обявяването му за противоконституционен с Решение № 2 на Конституционния съд от март 2015 г.[26]

Решение № 2 на Конституционния съд от 2015 г.

Като последствие от решението на Съда на Европейския съюз по делото „Digital rights“ режимът за съхраняването на трафични данни в ЗЕС, с който в българското законодателство е транспонирана Директива 2006/24/ЕО, е обявен за противоконституционен с Решение № 2 на Конституционния съд от 2015 г. (конституционно дело № 8/2014 г.)[27]. Делото е образувано по искане на омбудсмана на Република България, като Конституционният съд е сезиран да установи

[24] В Наредбата не е посочен нито един реквизит на писменото искане, вкл. мотиви за представянето му.

[25] Приет е и нов чл. 251а. През 2010 г. са приети и нови членове 250а – 250е.

[26] Изрично е премахната възможността за издаване на наредби, а Наредба № 40 е практически мълчаливо отменена след влизането в сила на измененията и допълненията в ЗЕС. През август 2024 г. Наредбата е отменена и изрично по предложение на министъра на вътрешните работи и министъра на транспорта и съобщенията поради отпадналото правно основание за издаването ѝ (ДВ, бр. 69 от 16.08.2024 г.).

[27] Обн., ДВ, бр. 23 от 27.03.2015 г.

противоконституционността на чл. 250а – чл. 250е[28], чл. 251[29] и чл. 251а[30] ЗЕС. В искането си омбудсманът посочва, че тези разпоредби противоречат на чл. 4, ал. 2, чл. 5, ал. 4, чл. 32, ал. 1 и чл. 34 от Конституцията и твърди, че съхраняването на данни по уредения в закона начин представлява неоправдана и несъразмерна намеса в личния живот на гражданите, както и нарушение на провъзгласената на конституционно равнище закрила на свободата и тайната на кореспонденцията[31].

В становището си по делото Съюзът на юристите в България заявява, че атакуваните текстове от ЗЕС не попадат в приложното поле на чл. 32 и чл. 34 от Конституцията, доколкото не става дума за огласяване или създаване на каквато и да е публичност по отношение на данните, свързани с личния живот на гражданите. Още по-малко съхраняването на такива данни би могло да бъде окачествено като нарушение на тайната на кореспонденцията.

Считам, че тази теза не е основателна. Неприкосновеността на личния живот и на тайната на кореспонденцията попадат под закрилата на Конституцията и без задължително да е налице огласяване на съответните данни от страна на лицата, които ги обработват. Стеснителното тълкуване на понятието „тайна на кореспонденцията“ по никакъв начин не би могло да отговори на целите, заложени в конституционната норма, като го сведе единствено до неприкосновеност на съдържанието на разменените съобщения. Както правилно посочва Съдът на Европейския съюз, съхраненият набор от данни позволява изграждането на точен профил на засегнатите лица[32]. Чувствителността на трафичните данни се доближава до чувствителността на

---

[28] Нови – ДВ, бр. 17 от 2010 г., в сила от 10.05.2010 г., обявени за противоконституционни от КС на РБ – бр. 23 от 2015 г.

[29] Изм. – ДВ, бр. 17 от 2009 г., бр. 17 от 2010 г., в сила от 10.05.2010 г., обявен за противоконституционен от КС на РБ - бр. 23 от 2015 г.

[30] Нов – ДВ, бр. 17 от 2009 г., обявен за противоконституционен от КС на РБ – бр. 23 от 2015 г.

[31] В подкрепа на искането на омбудсмана по делото са постъпили становища от президента на Република България, Върховния касационен съд, Върховния административен съд, главния прокурор, Комисията за защита на личните данни и др. Изтъква се, че чл. 34, ал. 2 от Конституцията допуска изключение при упражняването на установеното по силата на ал. 1 основно право на гражданите на неприкосновеност на свободата и тайната на кореспонденцията и на другите съобщения само когато това се налага за разкриване или предотвратяване на тежки престъпления, докато в оспорената норма на чл. 250а ЗЕС е предвидено доста по-широко приложно поле. Посочва се, че предвиденият режим представлява сериозно вмешателство в личния живот на лица, които никога и по никакъв начин не са участвали и не са били съпричастни към извършването на каквито и да е било престъпления.

Обратно, Министерството на вътрешните работи и Националното бюро за контрол на специалните разузнавателни средства твърдят, че оспорваните разпоредби на ЗЕС отговарят на изискванията за съразмерност, а срокът от дванадесет месеца е разумен и осигурява ефективност на въведената със закона ограничителна мярка, доколкото с нея се постига легитимна цел – защита на обществената сигурност. Освен това в становището им се отбелязва, че са предвидени механизми за контрол, които създават необходимите гаранции срещу възможни злоупотреби (например административнонаказателната отговорност за длъжностни лица или предприятия, предоставящи електронни съобщителни мрежи и/или услуги, в случай на нарушаване на предвидено задължение или злоупотреба с данни).

[32] Виж решение на Съда на Европейския съюз по съединени дела C-203/15 и C-698/15 („Tele2/Watson“), т. 99.

съдържанието на съобщенията, доколкото чрез тях може да се създаде детайлна картина относно адресатите, времето, а и мястото на проведените разговори.

В решението си Конституционният съд отбелязва, че с искането се оспорва закон, с който се засягат основни права на гражданите, провъзгласени в Конституцията и в редица европейски и международни актове[33]. Обявяването на Директива 2006/24/ЕО за недействителна няма за последица автоматичната отмяна на правните норми, с които тя е транспонирана във вътрешното право, а единствено прекратява задължението на държавите членки да въведат нейните изисквания в националното си законодателство. Поради тази причина приетият закон продължава да бъде в сила до момента, в който бъде отменен или изменен от Народното събрание или бъде обявен за противоконституционен от Конституционния съд.

Според конституционните съдии предвиденият в ЗЕС режим за съхраняване, достъп и унищожаване на трафични данни безспорно представлява намеса в конституционно защитени права на гражданите и следователно трябва да се третира като изключение от правилата, предвидени в чл. 32, ал. 1 и чл. 34, ал. 1 от Конституцията. В решението се посочва изрично, че съгласно изискванията на чл. 32, ал. 2 и чл. 34, ал. 2 от Конституцията изключенията следва да бъдат уредени в закон, да се допускат само с разрешение на съдебната власт и само когато това се налага за разкриването и предотвратяването на тежки престъпления.

Оспорената уредба изпълнява първото конституционно изискване, тъй като е създадена със закон. Налице е обаче противоречие на чл. 250а, ал. 2 ЗЕС[34] с Конституцията, тъй като той позволява предоставянето на достъп до трафични данни за нуждите на разкриването и разследването на престъпни деяния по чл. 319а – 319е от Наказателния кодекс (НК) (глава девета „а“ Компютърни престъпления), които към момента на разглеждането на конституционното дело не представляват тежки престъпления[35] по смисъла на чл. 93, т. 7 НК[36] (в тях не се предвижда наказание лишаване от свобода за повече от пет години).

Според Димитър Младенов Конституционният съд неправилно приема, че конституционното разбиране за тежко престъпление е идентично с дефиницията по чл. 93, т. 7 НК. Той застъпва тезата, че от конституционна гледна точка тежко ще бъде всяко престъпление, което засяга конституционно гарантираните основни права, независимо от неговата наказуемост и постулатите на наказателното право. По тази

---

[33] Всеобщата декларация за правата на човека (чл. 12), Международният пакт за граждански и политически права (чл. 5 и чл. 17), Хартата на основните права на Европейския съюз (чл. 7, чл. 8 и чл. 52, пар. 1) и Европейската конвенция за правата на човека (чл. 8).

[34] Чл. 250а. (Обявен за противоконституционен от КС на РБ – бр. 23 от 2015 г.) (2) Данните по ал. 1 се съхраняват за нуждите на разкриването и разследването на тежки престъпления и престъпления по чл. 319а – 319е от Наказателния кодекс, както и за издирване на лица.

[35] Към датата на постановяването на решението на Конституционния съд изключение прави единствено престъпният състав по чл. 319а, ал. 5, в който се предвижда наказание лишаване от свобода от една до осем години.

[36] Чл. 93, т. 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.

логика компютърните престъпления по глава „девета а“ НК също са тежки, тъй като засягат основни права на човека – личния живот на гражданите, свободата и тайната на кореспонденцията, правото на собственост и др.[37]

Намирам, че при аргументирането на тази позиция не е взето предвид еднозначното дефиниране на понятието „тежко престъпление“ в националното законодателство. То не се използва в друг нормативен акт с различна дефиниция и смятам, че не съществува причина, поради която да е налице необходимост да бъде тълкувано по различен начин. В тази връзка е важно да се отбележи, че съгласно чл. 37, ал. 1 от Указ № 883 от 24.04.1974 г. за прилагане на Закона за нормативните актове думи или изрази с утвърдено правно значение се използват в един и същ смисъл във всички нормативни актове.

Конституционният съд подчертава, че съобразяването с установения конституционен стандарт и критериите за законосъобразното ограничаване на основните права включват не само основанието, но и органите и процедурите, по които ще се изпълнява съответната мярка. Според съда законодателят твърде много е разширил кръга на субектите, които имат право да искат извършване на справка за данните[38], включвайки звена, които не разполагат с компетентност за разкриване и разследване на тежки престъпления, т.е. правомощия, свързани пряко с преследваната по закон цел[39].

Все пак в решението изрично се изтъква, че само по себе си съхраняването на трафични данни не представлява дейност, забранена от Конституцията, и не може изначално да бъде отречено като несъвместимо с основните права на гражданите. Конституционният съд посочва, че редица престъпления не биха могли да бъдат разследвани пълноценно без изследване и анализ на трафичните данни.

Въпреки това запазването на толкова значителен обем данни (кой, с кого, кога, как, с кое конкретно устройство и къде точно е осъществявал комуникация) за фиксирания в закона продължителен срок от дванадесет месеца по отношение на

---

[37] Виж **Младенов, Д.** Електронни доказателства. // De jure, 2022, № 1, с. 70.

[38] Чл. 250б. (Обявен за противоконституционен от КС на РБ 2022 бр. 23 от 2015 г.) (1) Право да искат извършване на справка за данните по чл. 250а, ал. 1 съобразно тяхната компетентност имат ръководителите на:

1. специализираните дирекции, териториалните дирекции и самостоятелните териториални отдели на Държавна агенция „Национална сигурност“;

2. Главна дирекция „Национална полиция“, Главна дирекция „Борба с организираната престъпност“ и териториалните й звена, Главна дирекция „Гранична полиция“ и териториалните й звена, дирекция „Вътрешна сигурност“, Столичната дирекция на вътрешните работи и областните дирекции на Министерството на вътрешните работи;

3. службите „Военна информация“ и „Военна полиция“ към министъра на отбраната;

4. Националната разузнавателна служба.

[39] Освен това изискването за съдебен контрол напълно отсъства в производството, уредено в хипотезата на чл. 250а, ал. 5 ЗЕС, в която органът, отправил искане за достъп, контактува директно с доставчика на услуги и без съответно разрешение практически удължава срока на съхраняването с още шест месеца – срок, който сам по себе си е значителен особено ако се добави към дванадесетте месеца по чл. 250а, ал. 1.

неопределен кръг лица дава възможност да се направят аргументирани заключения за личния живот на лицата, навиците им, социалната среда, местопребиваването, пътуванията им и т.н. При подробен анализ на генерирания трафик могат да се изведат и съдържателни изводи за интимния живот на гражданите, сексуалната им ориентация, здравословното им състояние, професионалната или политическата принадлежност, дори личните предпочитания, склонности, увлечения и слабости. По този начин се осигурява реална възможност за съставянето на ясен профил на засегнатите лица, не само без тяхното изрично съгласие, но и без те въобще да имат представа или да подозират, че се извършва подобна дейност.

Съдът намира, че преследването на формулираната цел не може да бъде извършвано на цената на толкова съществена намеса в основните права на гражданите. Дисбалансът няма как да бъде отречен, доколкото на съхраняване подлежат комуникационните данни на всички лица, а не само на тези, които по някакъв начин участват в престъпна дейност.

В пълно противоречие със Съда на Европейския съюз обаче Конституционният съд специално отбелязва, че не съществува друг способ, който, от една страна, би могъл да бъде насочен единствено към тези, чието поведение е предмет на наказателно преследване, а от друга – да може да осигури необходимите за целите на разследването сведения, и то отнасящи се основно за времето, предшестващо извършеното престъпно деяние.

Ако оспорената мярка, вменяваща изначално задължение за съхраняване на трафични данни, не съществува, то запазването и анализирането на данните по отношение на конкретно лице биха могли да започнат едва след извършването на престъплението. В този случай става невъзможно да се събере голяма част от информацията, свързана с подготовката, организацията, извършването на изпълнителното деяние и евентуалните съучастници, доколкото съхраняването на данните ще обхваща единствено последващия период, следователно няма как да

обслужи целите на наказателното преследване. Поради тази причина може да се приеме, че сама по себе си въведената мярка е необходима и подходяща.

Подкрепям тезата на Конституционния съд, тъй като ако се следва изцяло подходът на Съда на Европейския съюз, например ще възникне ситуация, при която две или повече лица се готвят да извършат престъпление с висока обществена опасност, използвайки средства за предаване на електронни съобщения. Престъплението е извършено, от него настъпват значителни вреди, започва разследване и в процеса на събиране на доказателства възниква съмнение за наличието на вина у лицата, които в действителност са извършили деянието. На доставчиците на електронни съобщителни услуги е наложено последващо задължение за съхраняване на трафични данни, отнасящи се до тези лица, но данните, създадени преди датата на връчването на заповедта за съхраняване, са загубени, което не позволява на разследващите органи да докажат по несъмнен начин вината на заподозрените лица.

Сходна теза по отношение на заличаването на трафичните данни споделят и Адам Юшчак и Елиза Сасон[40], които допълват, че ако предложенията на Съда на Европейския съюз се приложат стриктно, съществуват изключително големи трудности да се определи кои данни следва да бъдат съхранени, без да се наруши принципът на недискриминация[41]. Освен това според тях подобна категоризация може да бъде несъвместима и с презумпцията за невиновност[42].

Конституционният съд обаче счита, че дванадесетте месеца по чл. 250а, ал. 1 ЗЕС[43] са твърде продължителен срок, който съществено надхвърля необходимото за

---

[40] **Juszczak, A., E. Sason.** Recalibrating Data Retention in the EU: The Jurisprudence of the CJEU – Is this the End or the Beginning? – Eucrim, 2021, No. 4, p. 253–254: https://eucrim.eu/articles/recalibrating-data-retention-in-the-eu/.

[41] Рискът от дискриминация се отчита и при Цану и Карида, които посочват, че ефектът от подобен модел на съхраняване на данни ще се усети основно от по-бедните и непривилегировани слоеве на обществото. Виж **Tzanou, M., S. Karyda.** Privacy International and Quadrature du Net: One step forward two steps back in the data retention saga? – European Public Law 28, No. 1, p. 139–140: https://eprints.whiterose.ac.uk/198992/.

[42] Т. нар. „целенасочено“ съхраняване на данни е трудно осъществимо и по технически причини. Например според решение № 393099 на френския Държавен съвет от 21 април 2021 г. (https://www.legifrance.gouv.fr/ceta/id/CETATEXT000043411127?isSuggest=true) то се поставя в зависимост и от редица препятствия от техническо естество, които компрометират неговото въвеждане. Когато целенасоченото съхраняване се основава на географски критерий, следва да се има предвид, че местоположението на клетките на мобилните оператори е индивидуално за всеки оператор, а обхватът им не е обвързан с предварително определена географска зона. Освен това информацията за местоположението на съответната клетка не се включва автоматично в събраните данни – доставчиците са в състояние да установят връзката между клетката, до която се отнасят данните, и географското местоположение на тази клетка само за конкретен случай – във връзка с искане на компетентните съдебни или разследващи органи.

[43] Чл. 250а. (Обявен за противоконституционен от КС на РБ – бр. 23 от 2015 г.) (1) Предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, съхраняват за срок от 12 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;

постигането на дефинираните цели. Натрупването на едногодишна база данни позволява не само изготвянето на подробен личностен профил, но и създаването на ясна представа за трайните, обичайните и дори инцидентните прояви на конкретното лице, неговите контакти (лични, служебни, професионални, културни), систематизирането на местата, които посещава, както и идентификация на лицата, с които го прави. Поради тези съображения конституционните съдии преценяват, че прекомерно дългият срок за съхраняването на данните самостоятелно компрометира конституционосъобразността на приетата мярка, тъй като тя се явява особено несъразмерна[44].

В заключение Конституционният съд посочва, че макар да са въведени като средство за постигането на легитимна цел от общ интерес, разглежданите мерки безспорно представляват съществена намеса в личния живот на гражданите и следва да бъдат уредени по начин, съобразен с най-високите стандарти за сигурност, каквито посочената уредба не осигурява. Поради тази причина съдът правилно приема, че не отделните разпоредби – предмет на искането на омбудсмана, а цялата оспорена уредба в ЗЕС следва да бъде обявена за противоконституционна.

Всички обсъдени норми са систематично, логически и функционално свързани и като такива в цялост изграждат структурата на разгледаната правна регламентация на съхраняването и събирането на трафични данни. Те формират единна система, която цялостно не удовлетворява установените европейски и международни стандарти за гарантиране на конституционно закрепените основни права на гражданите.

Съдът отбелязва, че прегледът на практиката на различни европейски конституционни съдилища показва, че националните нормативни актове на редица други държави членки, с които е транспонирана Директива 2006/24/ЕО, също са обявени за противоконституционни (изцяло или частично). Основните съображения на конституционните съдии в Германия, Румъния, Чехия, Словения, Австрия, Полша се оказват твърде сходни, а някои и напълно идентични, с изводите на българския Конституционен съд[45]. Допълва се, че пороците и несъвършенствата на самата

---

4. идентифициране на типа на връзката;

5. идентифициране на крайното електронно съобщително устройство на потребителя или на това, което се представя за негово крайно устройство;

6. установяване на идентификатор на ползваните клетки.

[44] Конституционният съд цитира и решението на Федералния конституционен съд на Германия от 2 март 2010 г. „1 BvR 256/08, 1 BvR 263/08 и 1 BvR 586/08“, с което той се е произнесъл по конституционосъобразността на аналогични разпоредби във вътрешното законодателство на страната, отнасящи се до съхраняването на трафични данни. Германският съд прави заключението, че запазването на данни поначало не е неоправдано, когато е в границите на поставената легитимна цел и спазва изискванията на принципа за съразмерност.

[45] Юдит Раухофер и Дайти Мак Ситхай правилно прогнозират, че решението по делото „Digital rights“ е способно да „промени играта“ („game changer“) в областта на съхраняването на трафични данни. Виж **Rauhofer, J., D. Mac Sithigh.** The Data Retention Directive Never Existed. – SCRIPTed (2014), vol. 11, No. 1, p. 127.

Директива често не само са механично пренесени във вътрешното законодателство, но в редица случаи се оказват и задълбочени, какъвто пример е налице и със ЗЕС.

Конституционнните съдии заключават, че обратният фрагментиран подход чрез обявяването на частична противоконституционност би довел до възникването на правна несигурност в регулирането на обсъжданата материя.

Съхраняването на трафични данни след измененията в ЗЕС от март 2015 г.

Вследствие на решението на Конституционния съд, с което уредбата, въвеждаща Директива 2006/24/ЕО, е обявена за противоконстуционна, и отчитайки в цялост неговите препоръки, българският законодател предприема необходимите действия по привеждането на нормативната база в съответствие с акта на съда. Още в края на март 2015 г. в ЗЕС са приети изменения, които целят постигането на баланс между обществения интерес за ефективното предотвратяване, разкриване и преследване на престъпни прояви и защитата на неприкосновеността на личния живот и на кореспонденцията на гражданите.

Съгласно сега действащия чл. 251б, ал. 1 ЗЕС срокът за съхраняване на данните е намален на шест месеца в сравнение с дванадесетте месеца, предвидени в уредбата, обявена за противоконституционна. Тезата на Димитър Младенов[46], че шестмесечният срок противоречи на чл. 16, ал. 2 от Конвенцията за престъпления в кибернетичното пространство[47], не може да бъде подкрепена, тъй като Конвенцията не урежда въпроси, свързани с всеобщото съхраняване на трафични данни от доставчиците на услуги. Посоченият във въпросната разпоредба 90-дневен срок се отнася до продължаването на запазването[48] на вече съхранени данни и е необходим, за да могат съответните разследващи или съдебни органи да поискат тяхното предоставяне чрез молба за правна помощ или друг инструмент.

Предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, следва да съхраняват данните[49], създадени или обработени в процеса на тяхната дейност и необходими за:

- <u>проследяване и установяване на източника на връзката:</u> при услуга за гласови съобщения – телефонния номер на викащия и данни за идентифициране на

---

[46] Виж **Младенов, Д.** Цит. съч., с. 69.

[47] В България Конвенцията е ратифицирана със закон, приет от 39-то Народно събрание на 1 април 2005 г., обн. ДВ, бр. 29 от 5 април 2005 г., като е в сила за страната от 1 август 2005 г.

[48] Важно е да се отбележи, че в контекста на събирането на трафични данни понятието „запазване на данни“ (data preservation) следва да се разграничава по смисъл от понятието „съхраняване на данни“ (data retention), въпреки че двете са практически синоними на български език. „Запазването“ означава продължаване на пазенето на данни, които вече са съхранени, чрез което се цели предотвратяване на изменението на тяхното качество и съдържание, вкл. възпрепятстване на тяхното заличаване. Съответно, под „съхраняване“ следва да се разбира запазването на данни, които се генерират в момента, вкл. за целите на изпълнението на нормативно задължение, съгласно което определени категории данни подлежат на съхраняване.

[49] Чл. 251и ЗЕС.

крайния ползвател[50]; при интернет достъп, електронна поща и интернет телефония – идентификатор (IP адрес), определен за крайния ползвател, 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;

- идентифициране на направлението на връзката: при услуга за гласови съобщения – набран телефонен номер, вкл. номера, към който е пренасочено повикването, и данни за идентифициране на крайния ползвател; при електронна поща и интернет телефония – идентификатор на крайния ползвател или телефонен номер на получателя на интернет телефонно повикване, данни за идентифициране на крайния ползвател и идентификатор на получателя, за когото е предназначено съобщението;
- идентифициране на датата, часа и продължителността на връзката: при услуга за гласови съобщения – дата и час на началото и края на връзката; за интернет достъп, електронна поща и интернет телефония – дата и час на влизане и излизане в/от услугата интернет достъп, заедно с IP адреса (динамичен или статичен), определен от доставчика, и идентификатора на крайния ползвател, дата и час на влизане и излизане в/от услугата електронна поща или интернет телефония;
- идентифициране на типа на връзката: вида на използваната услуга за гласови съобщения; използваната услуга при електронна поща или интернет телефония;
- идентифициране на крайното устройство на потребителя или на това, което се представя за негово крайно устройство: при фиксирана (стационарна) услуга за гласови съобщения – викащия и викания телефонен номер; при услуга за гласови съобщения, предоставяна чрез мобилна наземна мрежа – викащ и викан телефонен номер; международен идентификатор на викащия и викания мобилен краен ползвател (IMSI[51]); международен идентификатор на викащото и виканото мобилно крайно устройство (IMEI[52]); в случай на предплатени услуги – дата и час на началното активиране на услугата, както и местоположението и идентификатора на клетката, от която е активирана услугата; при интернет достъп, електронна поща и интернет телефония – викащия телефонен номер за комутируем достъп[53], цифрова абонатна линия (DSL) или друга крайна точка на инициатора на връзката;

---

[50] Съгласно чл. 248, ал. 2, т. 2, б. „а“ ЗЕС данните за абоната са необходими за изготвянето на сметките на потребителя, като включват: за физически лица – трите имена, единен граждански номер и адрес, а за чуждестранни лица – личния номер; за юридически лица и физически лица – еднолични търговци – наименование, седалище, адрес на управление и единен идентификационен код.

[51] IMSI номерът е поредица от максимум 15 цифри, която идентифицира мобилния абонат.

[52] IMEI номерът се състои от 15 цифри и служи за идентификация на мобилния телефон.

[53] Комутируем достъп (dial-up) е телефонна услуга, която позволява на компютър, снабден с модем, да се свърже с друг компютър по телефонната мрежа за предаване на данни (например за достъп до интернет).

- установяване на идентификатор на ползваните клетки (данни за местоположението)[54]: административни адреси на клетки на мобилна наземна електронна съобщителна мрежа, от които е генерирано или в които е завършено повикване[55].

Съгласно чл. 251б, ал. 2 ЗЕС данните се съхраняват:

- за нуждите на националната сигурност;
- за предотвратяването, разкриването и разследването на тежки престъпления, в т.ч. за целите на предотвратяването на тежки престъпления в рамките на оперативно-издирвателната дейност по реда на глава девета от Закона за противодействие на корупцията[56];
- 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 не е отложено и която не е приведена в изпълнение, или което е изпаднало или може да изпадне в положение, поставящо в риск живота или здравето му.

Изключение от този принцип се прави единствено по отношение на данните за местоположението, които се запазват и за осъществяването на издирвателни операции и спасяването на лица в случаите по чл. 38, ал. 3 от Закона за защита при бедствия[57].

Като съществена гаранция за неприкосновеността на личния живот на гражданите е предвидено задължение доставчиците на услуги да унищожават данните след изтичането на сроковете за съхраняване[58], като ежемесечно представят на Комисията за защита на личните данни (КЗЛД) протоколи за унищожените през предходния месец данни.

Заключение

---

[54] Поради пандемията от COVID-19 с § 41 от преходните и заключителните разпоредби на *Закона за мерките и действията по време на извънредното положение, обявено с решение на Народното събрание от 13 март 2020 г., и за преодоляване на последиците* в чл. 251б, ал. 2 и някои свързани разпоредби от ЗЕС беше направено допълнение, съгласно което данните за установяване на идентификатор на ползваните клетки се съхраняват и за нуждите на принудителното изпълнение на задължителната изолация и болничното лечение на лица по чл. 61 от Закона за здравето, които са отказали или не изпълняват задължителна изолация и лечение. Допълненията в ЗЕС бяха обявени за противоконституционни с Решение № 15 на Конституционния съд от 17 ноември 2020 г. поради противоречие с чл. 32 от Конституцията.

[55] Както и в Наредба № 40, категориите данни по чл. 251и ЗЕС изцяло следват списъка по чл. 5, пар. 1 от Директива 2006/24/ЕО.

[56] Глава девета „Противодействие на корупцията чрез разкриване и разследване на корупционни деяния, извършени от лица, заемащи публични длъжности“.

[57] Чл. 38 (3) (Нова – ДВ, бр. 97 от 2016 г., в сила от 6.12.2016 г.) При постъпил сигнал за физическо лице, което е изпаднало или може да изпадне в положение, поставящо в риск живота или здравето му, предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, извършват справка за данните по чл. 251б, ал. 1, т. 6 от Закона за електронните съобщения. Достъпът до данните се осъществява при условията и по реда на Закона за електронните съобщения.

[58] Чл. 251ж, ал. 1 ЗЕС.

След обявяването на Директива 2006/24/ЕО за недействителна с решението на Съда на Европейския съюз по делото „Digital rights“ в правния мир на европейско равнище не съществува инструмент, който да установява правила за съхраняването на трафични данни за целите на наказателния процес. В тази връзка трябва да се има предвид и решението на Съда на Европейския съюз по делото „Tele2/Watson“ (съединени дела C-203/15 и C-698/15)[59], в което съдът приема, че съгласно чл. 15, пар. 1 от Директива 2002/58/ЕО във връзка с чл. 7, чл. 8 и чл. 52, пар. 1 от Хартата на основните права не се допуска приемането на национална правна уредба, която за целите на борбата срещу престъпността предвижда всеобщо[60] съхраняване на всички трафични данни и данни за местоположение на всички абонати на всички електронни съобщителни средства.

Съдът потвърждава забраната за всеобщо съхраняване на данни и в решението си от 17 ноември 2022 г. по „българското“ дело C-350/21 (преюдициално запитване, отправено от Специализирания наказателен съд). В него също се посочва, че чл. 15, пар. 1 от Директива 2002/58/ЕО не допуска национално законодателство, което за целите на борбата срещу тежката престъпност и предотвратяването на сериозни заплахи за обществената сигурност предвижда общо и неизбирателно съхраняване на трафични данни дори ако посоченото законодателство ограничава във времето това съхраняване до период от шест месеца и предвижда определени гаранции при съхраняването и достъпа до съответните данни[61].

Както беше посочено и по-горе, Съдът на Европейския съюз предлага като алтернатива т.нар. *„целенасочено съхраняване на данни“*. При него запазването на данните следва да се извършва единствено въз основа на обективни критерии и едва след установяване на предварителна взаимовръзка между подлежащите на съхраняване данни и извършването на тежко престъпление. Съдът добавя, че съхраняването може да бъде допълнително ограничено – по отношение на конкретна географска област или спрямо определена категория лица.

Този подход обаче страда от съществени слабости, тъй като става невъзможно да се събере значителна част от информацията, свързана с подготовката за извършването на престъплението, доколкото запазването на данните ще обхваща единствено последващия период. Ще бъдат изгубени големи обеми от данни, генерирани преди възникването на обоснованото предположение за необходимост от съхраняване, които вече ще са заличени от доставчика в съответствие със задълженията му по Директива

---

[59] https://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=BG&mode=lst&dir=&occ=first&part=1&cid=409367.

[60] Марчин Ройшчак използва и понятието „превантивно съхраняване (*preventive retention*)“. Виж **Rojszcak, M.** The uncertain future of data retention laws in the EU: Is a legislative reset possible? – Computer Law & Security Review 41, p. 3: https://www.sciencedirect.com/science/article/pii/S0267364921000455.

[61] Вече е налице и съдебна практика на българските съдилища, съгласно която се отказва достъп до съхранени трафични данни въз основа на позоваване на решението по дело C-350/21. Виж например Разпореждане № 12813 от 17.10.2023 г. на Софийския районен съд по ч. н. д. № 14021/2023 г. и Разпореждане № 12965 от 19.10.2023 г. на СРС по ч. н. д. № 14136/2023 г.

2002/58/ЕО, а в българската действителност – и съгласно разпоредбите на ЗЕС. Тази теза се подкрепя и в решението на Конституционния съд от 2015 г. (виж по-горе).

Поради тази причина de lege ferenda намирам, че подход, около който е възможно да се градят изменения в настоящата нормативна уредба, е т. нар. *„ограничено“ съхраняване на данни*. При този модел по подобие на настоящия съхраняването също започва от момента на генерирането на данните, но в допълнение се основава на ограничаването (намаляването) на броя на категориите данни за съхраняване.

От изключително значение за ефективното ѝ изпълнение е да се подберат категориите, които са от първостепенно значение за разследващите органи при упражняването на техните правомощия по предотвратяването, разследването, разкриването и преследването на престъпни деяния, както и тези данни, които биха могли спокойно да се изключат от обхвата на модела, доколкото степента им на полезност би могла да бъде подложена на съмнение. Така например се приема, че съхраняването на данни, свързани с предаването на съобщения чрез фиксирани телефонни услуги (при стационарните телефонни апарати), не е толкова наложително, доколкото тези услуги вече се използват доста по-рядко, съответно на разследващите органи по-рядко се налага да изискват от доставчиците подобни данни[62].

Освен това би могла да се съкрати продължителността на сроковете за съхраняване, както и да се предвидят различни срокове за отделните категории данни с оглед степента им на чувствителност[63]. Прекомерно дългият срок позволява създаването на огромни масиви от данни, което се явява несъразмерно на заложената цел за борба срещу престъпността. Съгласно доклада на КЗЛД за 2023 г.[64] времето, изтекло от началната дата на съхраняването, до датата, на която компетентните органи са поискали предаването на данните, е преимуществено до три месеца – в 59% от всички случаи[65]. Тази информация би могла да бъде от полза при прилагането на концепцията и евентуалното намаляване на срока за съхраняване. Все пак (въпреки извода на Съда на Европейския съюз по дело C-350/21) смятам, че настоящият шестмесечен срок е умерено продължителен особено ако се вземе предвид дължината на срока в редица други държави членки на Европейския съюз[66].

---

[62] Същото в голяма степен важи и за интернет телефонията.

[63] Например в Швеция данните за местоположението от мобилните оператори се съхраняват за два месеца, трафичните данни, свързани с интернет достъп – за десет месеца, а всички останали трафични данни – за шест месеца. Виж https://www.ejnforum.eu/cp/e-evidence-fiche/378/0.

[64] https://cpdp.bg/wp-content/uploads/2024/03/Annual-report_2023_CPDP.pdf (стр. 140).

[65] Трябва да се отчете, че „възрастта“ на данните зависи пряко от вида на разследваното престъпление. Самият факт на извършването на определени престъпни деяния (например някои компютърни престъпления) се установява по-трудно и бавно.

[66] В Белгия, Франция, Унгария, Испания, Естония, Португалия и Дания срокът за съхраняване на данните е дванадесет месеца, а в Латвия – осемнадесет месеца. В Италия данните от обществени телефонни услуги се съхраняват за две години, а данните от интернет услуги – за дванадесет месеца. Виж https://www.ejnforum.eu/cp/e-evidence-fiche/230/0 и съответната информация за другите държави членки в падащото меню.

Крайната цел на въвеждането на модела на ограниченото съхраняване е намаляването на интензитета на намеса в личното пространство на засегнатите лица[67]. Все пак при определянето на категориите данни за съхраняване следва да се ползва технологично неутрален подход, тъй като с развитието на техниката характеристиките им биха могли да се изменят със забележителна скорост.

Друг възможен вариант е прилагането на констатациите на Съда на Европейския съюз от решението по съединени дела C-511/18, C-512/18 и C-520/18 от 6 октомври 2020 г.[68], съгласно което Директива 2002/58/ЕО във връзка с чл. 7, чл. 8 и чл. 11 от Хартата на основните права допуска правна уредба, която упълномощава компетентните органи да издадат разпореждане, съгласно което доставчиците на електронни съобщителни услуги са длъжни да съхраняват трафични данни и данни за местоположението на всички потребители, в случай че съществуват достатъчно убедителни основания да се приеме, че съответната държава членка е изправена пред сериозна заплаха за националната сигурност[69].

Особено важно е да се посочи, че съгласно чл. 4, пар. 2 от Директива (ЕС) 2016/680[70] обработването на данните за цел, различна от целта, за която те са събрани, ще бъде позволено, ако администраторът е оправомощен да обработва данните за втората цел в съответствие с правото на Съюза или правото на държава членка и обработването е необходимо и пропорционално. Това означава, че Директивата позволява използването на данни, съхранени с оглед защитата на националната сигурност, за целите на борбата срещу тежката престъпност, стига горните условия да бъдат изпълнени, с оглед на което предложеният вариант за промени в националното законодателство ще бъде в съответствие с европейското право.

Въпреки това намирам, че този подход не е достатъчно устойчив, доколкото изисква периодичното издаване на съответни разпореждания, и то за цел, различна от тази за борбата срещу престъпността, и по-скоро би могъл да се прилага по изключение. За сравнение моделът, основан на ограниченото съхраняване на данни, притежава редица предимства – стабилност чрез предвиждането му в нормативен акт, правна сигурност за доставчиците на услуги, чиито задължения ще бъдат предварително установени, както и намален обем на информацията, която се съхранява.

---

[67] Например само евентуалното скъсяване на срока за съхраняване от шест на три месеца автоматично ще намали обема на съхраняваните данни наполовина.

[68] https://curia.europa.eu/juris/document/document.jsf?text=&docid=232084&pageIndex=0&doclang=BG&mode=lst&dir=&occ=first&part=1&cid=4602373.

[69] Виж т. 137–139 от решението. Разпореждането трябва да обхваща ограничен период от време, а при необходимост от неговото подновяване следва да се издаде ново. В допълнение, задължението за съхраняването на данните не трябва да се налага систематично.

[70] Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни, и за отмяна на Рамково решение 2008/977/ПВР на Съвета.