БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ
ИНСТИТУТ ЗА ДЪРЖАВАТА И ПРАВОТО

ДОКАЗВАНЕ ЧРЕЗ ТРАФИЧНИ ДАННИ В БЪЛГАРСКИЯ НАКАЗАТЕЛЕН ПРОЦЕС

АВТОРЕФЕРАТ

БОГДАН РАДОСЛАВОВ МЛЪЧКОВ

Докторска програма „Наказателен процес“ (3.6. Право)

Научен ръководител: проф. дюн Гергана Маринова

София, 2026 г.

СЪДЪРЖАНИЕ

I. ОБЩА ХАРАКТЕРИСТИКА..... 3

II. КРАТКО ИЗЛОЖЕНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД..... 6

III. НАУЧНИ ПРИНОСИ В ДИСЕРТАЦИОННИЯ ТРУД..... 27

IV. ПУБЛИКАЦИИ НА АВТОРА ПО ТЕМАТА..... 29

I. ОБЩА ХАРАКТЕРИСТИКА

1. Значение на изследването

Революцията в сферата на информационните технологии доведе до фундаментални обществени промени и не може да съществува каквото и да е съмнение, че те ще стават все по-видими в следващите години, въпреки че наличието им е достатъчно явно и понастоящем. Епохата на информационното общество ни позволява да комуникираме по-лесно отвсякога дори когато сме разделени от десетки хиляди километри, можем да получим мигновено информация за абсолютно всичко, което се случва в която и да е точка на планетата. Класическите стационарни, а и мобилни телефонни услуги бяха изпреварени необратимо от широка палитра от програми, уеб сайтове и приложения, които позволяват обмен на невъобразими количества данни, съдържащи звук, текст, снимки и видео.

Възможностите за откриване на сведения от всякакъв вид чрез компютърните информационни системи, достъпността на информацията и неограничените способности за нейното разпространение, без каквито и да е физически лимити, доведоха до истинска експлозия в количеството данни, налични за всекиго и по всяко време. Ураганът на ерата на информационното общество предизвика уникални по рода си икономически и социални промени. Навлезлите технологични подобрения промениха естеството на работата в редица стопански и не само сектори, увеличиха съществено производителността на труда, намалиха рисковете от допускане на грешки. Новите технологии обаче се оказват сериозно предизвикателство за съществуващите консервативни правни концепции - информационните и комуникационни потоци се движат с невиждана досега скорост, а националните правила, вкл. в областта на наказателния процес, по-скоро се придържат към принципа на териториалността и уреждат предимно отношенията, които се развиват единствено в границите на съответната държава.

Тези промени имат и своя особено „тъмна“ страна: появата на престъпления, извършвани в киберпространството, както и създаването на нови форми на традиционни престъпни прояви, реализирани посредством средствата на информационните технологии. Едно от основните предизвикателства в разследването и разкриването на престъпления с отражение в кибернетичното пространство, особено когато те са извършени чрез помощта на компютърна информационна система, е установяването на самоличността на извършителя. Интернет технологиите позволяват в голяма степен запазването на анонимността на потребителите, които се крият зад всевъзможни псевдоними, а използват и

различни програми, които възпрепятстват компетентните органи при установяването на местоположението им. Допълнително затруднение създава фактът, че данните в електронен формат, необходими за целите на провеждането на наказателното производство, могат да се модифицират, преместват и заличават за части от секундата.

Като един от основните видове електронни доказателства трафичните данни представляват основен 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 следи, без които правоохранителните органи често биха били поставени пред съществени затруднения.

2. Цел, задачи и методология на изследването

Целта на изследването е да представи възможно най-широкообхватен поглед върху темата за съхраняването и събирането на трафични данни и използването им като доказателствен материал в наказателния процес, както и за съпътстващите ги гаранции за спазване на основните права на гражданите. Задачите на дисертационния труд са следните - изясняване на понятието за трафични данни и същността им, вкл. сред останалите видове електронни доказателства; изследване на нормативната уредба в областта на съхраняването и събирането на трафични данни за целите на наказателния процес на национално, европейско и международно равнище; разглеждане на функцията на трафичните данни като доказателство в процеса; проучване на практиката на националните съдилища, Конституционния съд, Съда на Европейския съюз и Европейския съд за правата на човека; идентифициране на основните проблеми, произтичащи от нормативната уредба и съдебната практика; и формулиране на предложения *de lege ferenda* с цел усъвършенстване на правната уредба.

В дисертационния труд се разглеждат особеностите на трафичните данни като един от видовете данни в електронна форма; представят се в синтезиран вид становищата по темата, изразени в доктрината; проследява се развитието на нормативната уредба за съхраняване и събиране на трафични данни и тяхното използване като доказателство в наказателния процес, включително когато то е обусловено от актовете на Европейския съюз и международните договори, както и от решенията на Конституционния съд; и се анализира съдебната практика на българските и наднационалните съдилища. Посредством използваната методология се постигат горепосочените задачи на дисертационния труд, включително предлагането на решения, които да допринесат за постигането на баланс между ефективността на наказателното преследване чрез ползването на

трафичните данни като доказателствен материал и защитата на основните права.

3. Структура на дисертационния труд

Дисертационният труд се състои от 209 страници, включително съдържание и библиография. Броят на бележките под линия е 484. Трудът включва заглавна страница, съдържание, въведение, четири глави с обособена структура, заключение и библиография. Към дисертационния труд е приложена декларация за оригиналност.

II. КРАТКО ИЗЛОЖЕНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД

Въведение

От изобретяването на първия компютър до създаването на съвременния интернет преминават цели четиридесет и две години, а днес изчислителната мощност на приложенията с изкуствен интелект се удвоява приблизително на всеки шест до дванадесет месеца. „Ускоряването на историята“, предизвикано от все по-динамичното развитие на технологиите, ни поставя постоянно пред непознати предизвикателства, но едновременно предоставя и нови възможности.

Досегашните модели за обмен на информация отстъпват пред интернет базирани услуги, социални мрежи и други платформи и приложения, а дори телефонната комуникация, която сама по себе си дълго време беше основен източник на трафични данни и данни за местоположението, постепенно губи актуалност. Тези процеси изискват качествено приспособяване на законодателството, както и повишаване на капацитета и експертните познания на всички участници в наказателния процес, които имат пряко отношение към разкриването на обективната истина - разследващи органи, прокурори, съдии. В противен случай съществува реална опасност обективната истина да не бъде разкрита и по този начин да се компрометират задачите на наказателното производство.

Електронните доказателства, включително трафичните данни, се превръщат със засилен интензитет в основен носител на информация относно поведението и комуникацията на лицата, замесени в престъпни деяния. Повишаването на тяхната значимост е пряка последица от промяната в начина, по който функционира съвременната комуникация: голяма част от обществените отношения, в т.ч. престъпната дейност, се осъществява онлайн, в цифрова среда, в която всеки недобросъвестен потребител с противозаконни намерения би могъл да остави следи, годни да бъдат използвани в рамките на разследването.

Глава първа. Същност и значение на трафичните данни.

В глава първа трафичните данни се разглеждат през призмата на понятието за „електронни доказателства“ съгласно научната литература. Ако то трябва да се дефинира по възможно най-прост начин, то бихме казали, че електронните доказателства представляват данни, съхранени в електронна (цифрова) форма. Електронните доказателства могат да се съхраняват в личните ни компютърни устройства, вкл. мобилни телефони, камери, таблети и др., в сървърите на доставчика на съответната електронна съобщителна услуга или в т. нар. „cloud” платформи (облачни технологии).

В Конвенцията за престъпления в кибернетичното пространство вместо „електронни доказателства“ се използва понятието „компютърни данни“, а формулировката от Конвенцията е възприета изцяло в понятието за „компютърни данни“ в чл. 93, т. 22 от Наказателния кодекс (НК). За разлика от НК в НПК се ползва понятието „компютърни информационни данни“, без обаче в допълнителните разпоредби на кодекса да е налице легална дефиниция. В тази връзка *de lege ferenda* би било полезно двата употребени в НК и НПК термина да се уеднаквят чрез ползването на понятието „електронни доказателства“. По същество за еднакви по съдържание понятия се използват две различни, макар и все пак близки, и остарели формулировки - компютърни данни и компютърни информационни данни.

В тази част от дисертацията се прави и предложение за обособяване на на електронните доказателства като отделна категория доказателствен материал поради специфичното им естество. От гледна точка на класическото разделение на видовете доказателства в наказателноправната теория на веществени и невеществени електронните доказателства не попадат в категорията на веществените, тъй като последните имат материално естество, с което данните в цифров формат не разполагат.

Проф. дюн Гергана Маринова и проф. д-р Веселин Вучков поставят електронните доказателства в групата на невеществените, намирайки, че доколкото те представляват информация в цифров вид, а не вещ, понятието за невеществени доказателства следва да се разшири и допълни със следите от електронно естество. В тази връзка подкрепям тезата на Димитър Младенов, че използването на класификацията на доказателствата на веществени и невеществени не представлява удачен начин за отразяване на спецификата на електронните доказателства. От една страна, както беше посочено по-горе, те нямат материално измерение и поради тази причина не могат да бъдат причислени към веществените доказателства, но от друга страна притежават и съществени особености, които ги отличават от невеществените.

С оглед на цифровата природа на електронните доказателства те задължително се възпроизвеждат чрез устройство или друг носител, който обаче винаги има материален характер, а без подходяща технология съдържанието им е напълно недостъпно. За сравнение, опознаването на фактите от психичния мир на човека като невеществени доказателства е „опосредствено чрез източника им - свидетел или обвиняем“, поради което „съдържанието им зависи от някои личностни фактори“, както посочва проф. д-р Иван Видолов. Поради тази причина при възприемането на електронните доказателства се проявява висока степен на обективност, докато при възприемането на невеществените доказателства е налице силен субективен елемент. Друга съществена отлика е, че електронните

доказателства се събират чрез изземване по реда на чл. 159 и 159а НПК, чрез претърсване и изземване (чл. 163, ал. 6 и 7 НПК) или задържане и изземване на кореспонденция (чл. 165 НПК), а обичайният способ за събиране на невеществените доказателства е разпитът на свидетел или обвиняем. Друга особеност на електронните доказателства се дължи на това, че те са трудно проследими и често могат да бъдат променени с цел прикриване на информация. Поради горните съображения намирам, че електронните доказателства могат да бъдат изведени в отделна категория.

В глава се прави разграничение между понятията „доказателство“ и „доказателствено средство“, като се разглеждат случаите, в които носителят, съдържащ електронни доказателства, представлява веществено доказателство (когато е създаден извънпроцесуално), съответно когато представлява веществено доказателствено средство, изготвено по реда на НПК.

Трафичните данни се разглеждат като един от видовете електронни доказателства заедно с потребителските данни (име, адрес, телефонен номер и др.), данните за местоположението (по-специфична категория, която за улеснение попада в масива „трафични данни“) и данните за съдържанието (текст, глас, звук, изображения или видео). Тези понятия нямат легални дефиниции в НПК, където се използват термините „данни за абоната на компютърно-информационна услуга“ и „данни от предприятия, предоставящи обществени електронни съобщителни мрежи и/или услуги”. В българското законодателство данните за съдържанието не са предмет на самостоятелна уредба - спрямо тях се прилагат разпоредбите относно претърсването и изземването, задържането и изземването на кореспонденция, както и използването на специални разузнавателни средства.

В рамките на наказателното производство потребителските данни са необходими най-вече в две ситуации: за да се установи какви услуги са ползвани или се ползват от даден потребител, чиято самоличност е известна (мобилна или фиксирана телефонна услуга, гласова поща, електронна поща и др.); ако техническият идентификатор (телефонен номер, IP адрес, потребителско име и др.) е известен, то тогава потребителските данни са необходими, за да се установи самоличността на търсеното лице.

Извършва се подробен анализ на понятието за трафични данни, съгласно което трафични са всички данни, свързани със съобщение, преминаващо през компютърна система, произведени от нея като елемент от комуникационна верига, които способстват за проследяването на пътя на съобщението от източника до неговото местоназначение. Поради тази причина трафичните данни могат да се категоризират като спомагателни спрямо извършената комуникация. Данните за трафика 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 (чрез електронна поща, телефонни услуги, приложения за мигновено изпращане на съобщения и др.).

Отделено е и внимание на останалите видове метаданни, различни от трафичните, както и на значението на IP адресите като по-особен вид данни. Въз основа на характеристиките на трафичните данни и с оглед необходимостта от последващо разграничение поради различните изисквания при събирането им се прави и съпоставка между трафичните и останалите видове данни.

Например съществена концептуална разлика между потребителските и трафичните данни е, че трафичните данни, в т.ч. и данните за местоположението, позволяват изграждането на приблизително ясен профил на лицата, за които се отнасят. Това твърдение обаче не е валидно по отношение на данните за абоната (потребителските данни), които не притежават това свойство. Тези данни предоставят на разследващите органи възможност единствено да установят самоличността на лицето, което ползва дадена услуга, или по-скоро на лицето, което е регистрираният ползвател на тази услуга (често множество лица могат да ползват една и съща услуга), без да им позволяват да изградят по-точна картина относно адресатите на неговата комуникация, продължителността ѝ, местата, от които я провежда, и др.

Същевременно, с течение на времето изводите от съпоставката между трафичните данни и данните за съдържанието търпят съществени промени. През 90-те години на двадесети век и в началото на двадесет и първи по-скоро надделява разбирането, че данните за съдържанието са значително по-чувствителни и значими, отколкото трафичните данни. За сравнение, в съвременната практика на Съда на Европейския съюз и на Европейския съд по правата на човека се откроява идеята, че събирането на трафични данни може да накърнява също толкова правата на гражданите, колкото и събирането на данни за съдържанието. Това е така, тъй като ако бъдат получени в цялост, трафичните данни могат да се използват за създаване на подробен профил на дадено лице чрез проследяване на местоположението му, преглед на данните за сърфирането му в интернет, моделите му на комуникация и др.

Хронологично се представя подробна информация относно Директива 2002/58/ЕО и Директива 2006/24/ЕО като правни основания за съхраняването на данни за целите на наказателния процес в държавите членки на Европейския съюз. Съхраняването на трафични данни от страна на доставчиците на електронни съобщителни услуги (и мрежи)

представлява основен стълб в борбата срещу престъпността, защото в изключително голям брой случаи разследващите органи се нуждаят от информация в цифров формат, за да могат успешно да разкрият извършването на престъпно деяние.

Преди влизането в Европейския съюз през 2007 г. в България не съществува правна рамка за съхраняването на трафични данни за целите на наказателния процес. Още през 2002 г. е приета Директива 2002/58/ЕО относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации („E-Privacy“), в която се създава изрично правно основание за съхраняването на трафични данни за целите на борбата срещу престъпността. Директивата е транспонирана в българското законодателство с изменения и допълнения в Закона за електронните съобщения.

През 2006 г. на основание чл. 15, пар. 1 от Директива 2002/58/ЕО 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. С нея се цели създаването на хармонизиран режим относно задълженията на доставчиците на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи за съхраняването на данни, за да се гарантира, че тези данни ще бъдат достъпни за целите на разследването на тежки престъпления. Директивата предвижда, че данните се съхраняват за срок, не по-кратък от шест месеца и не по-дълъг от две години, считан от датата на предаването на съобщението.

През 2014 г. обаче тя е обявена за недействителна от Съда на Европейския съюз с решение по съединени дела C-293/12 и C-594/12 (“Digital rights”), тъй като съдът намира, че Директивата непропорционално ограничава правото на личен живот и правото на защита на личните данни, като поставя на обсъждане редица спорни въпроси относно съхраняването на трафични данни и използването им като доказателство в наказателния процес.

Въпреки отмяната ѝ от Съда на Европейския съюз Директива 2006/24/ЕО оставя съществена нормативна следа в правните рамки за съхраняването на трафични данни на държавите членки, особено по отношение на категориите данни за съхраняване, които в значителна степен остават непроменени и до днес. В тази връзка разпоредбите на Закона за електронните съобщения и на Наказателно-процесуалния кодекс не правят изключение, като е изключително важно отново да се отбележи, че с транспонирането на Директива 2006/24/ЕО за първи път в българското законодателство се предвижда задължение за доставчиците на съобщителни услуги и мрежи за съхраняване на трафични данни.

Глава втора. Основни положения в съхраняването на трафични данни на европейско равнище.

Глава втора е посветена на основните положения в съхраняването на трафични данни, изведени в съдебната практика на Съда на Европейския съюз - съвместимостта им с правото на неприкосновеност на личния живот, правото на защита на личните данни, правото на свобода на изразяване на мнение и др.

В решението по делото „Digital rights" от 2014 г., с което Директива 2006/24/ЕО е обявена за недействителна от Съда на Европейския съюз, се посочва, че въпреки липсата на информация за съдържанието на съобщенията данните, разгледани в съвкупност, позволяват да се изведат много точни заключения относно личния живот на лицата, навиците им в ежедневието, мястото, където пребивават, пътуванията им, упражняваните дейности, социалните им връзки и кръговете, в които се движат.

Съдът отбелязва, че 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. 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.

Тази теза на Съда на Европейския съюз, развита по-късно и в решението по делото „Tele2/Watson", не може да бъде споделена. Не е разумно да се очаква, че е възможно 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. Дори впоследствие в рамките на наказателно производство, инициирано благодарение на други сведения, разследващите органи да издадат заповед за съхраняването на такива данни, ще бъде изгубена ценна информация, която може да има решаващо значение за изхода на делото.

Поради тези причини е далеч по-целесъобразно тази преценка да се извършва на етапа на получаването на достъп от страна на разследващите органи до запазените данни. Така ще се гарантира целостта на данните и ще се противодейства на всякакви злоупотреби с оглед незаконосъобразното им използване. Сходни 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 позволи извършването на злоупотреби от страна на лица с престъпни намерения.

Според Съда на Европейския съюз 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.

В заключение според Съда на Европейския съюз Директива 2006/24/ЕО не предвижда ясни и конкретни правила, които да определят обхвата на намесата в основните права, провъзгласени в Хартата на основните права. 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, и го обявява за недействителен.

Съдът развива своите разсъждения в областта на съхраняването на трафични данни и в решението по делото „Tele2/Watson" от 2016 г., в което приема, че правото на Европейския съюз не допуска приемането на национална правна уредба, която за целите на борбата срещу престъпността предвижда всеобщо съхраняване на всички трафични данни и данни за местоположение на всички абонати на всички електронни съобщителни средства; не ограничава достъпа на компетентните национални органи до съхранените данни единствено за целите на борбата срещу тежката престъпност, не го подчинява на предварителен съдебен контрол или на контрол от страна на независима административна юрисдикция и не изисква разглежданите данни да се съхраняват на територията на Съюза.

Преповторено е и становището от решението по делото „Digital rights", според което в повечето случаи засегнатите лица не са в ситуация, която би могла да бъде повод за започването на наказателно преследване, а освен това не се установяват и изключения за лица, чиито съобщения представляват професионална тайна съгласно националното право. Не се изисква и наличие на връзка между данните, които трябва да бъдат съхранени, и извършването на престъпление. Предвиденото съхраняване не е насочено единствено към данни, отнасящи се до определен период от време, определена географска област или определен кръг от лица, за които се предполага, че са участвали в извършването на престъпна дейност или които биха могли да допринесат за разкриването или преследването на тежки престъпления. Съответно, изразената критика към тази част от

становището на Съда на Европейския съюз по делото „Digital rights” е изцяло валидна и приложима и спрямо изводите по делото „Tele2/Watson”.

Все пак съдът дава указания какви параметри би следвало да притежава дадена правна уредба, за да може да отговори на изискванията на Директива 2002/58/ЕО и на относимите разпоредби от Хартата. Според съдиите запазването трябва да се извършва въз основа на обективни критерии, които да установяват връзка между подлежащите на съхраняване данни и преследваната цел. Тези условия ще ограничат обхвата на мярката, както и броя на засегнатите лица. Съдът допълва, че подобно ограничаване може да се постигне и чрез въвеждането на географски критерий, когато въз основа на обективни обстоятелства компетентните национални органи установят, че в една или в няколко географски области съществува повишен риск от извършване на тежки престъпни деяния.

По този начин в решението по делото „Tele2/Watson” съдът изгражда т.нар. концепция за „целенасочено съхраняване на данни“, която търпи сериозни критики в практиката. Несъгласието със становището на съда се основава на факта, че целенасоченото съхраняване позволява единствено запазването на „бъдещи“ данни, вследствие на възникнало за националните правоохранителни органи обосновано предположение за вече извършено престъпление или за опасност от извършването на такова, благодарение на информация, получена по друг начин. Този подход гарантира, че безвъзвратно изгубени, макар и от полза за разследването, ще бъдат всякакви данни в цифров формат, които са генерирани преди възникването на обоснованото предположение, въз основа на което доставчикът на услуги ще бъде задължен да започне да съхранява данни за определен потребител, определена категория лица или в рамките на определена географска област.

Практиката на Съда на Европейския съюз се развива чрез приемането на решението по съединени дела C-511/18, C-512/18 и C-520/18 от 2020 г. В него съдът потвърждава досегашното си становище, според което Директива 2002/58/ЕО следва да бъде тълкувана в смисъл, че не допуска национална правна уредба, която създава задължение за доставчиците на услуги за всеобщо съхраняване на трафични данни. Освен това съдът потвърждава и разбирането си за принципа за „целенасочено“ съхраняване на данни, но за разлика от решенията по делата „Digital rights” и „Tele2/Watson” съдът не абсолютизира тези изводи и извежда някои важни изключения, свързани със защитата на националната сигурност и с IP адресите като по-особена категория данни.

Изтъква се, че целта „защита на националната сигурност“ надхвърля като значение останалите цели, посочени в чл. 15, пар. 1 от Директива 2002/58/ЕО, вкл. противодействието на тежката престъпност и защитата на

обществената сигурност. Поради тази причина съдът намира, че Директива 2002/58/ЕО във връзка с чл. 7, чл. 8 и чл. 11 от Хартата допуска правна уредба, която оправомощава 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. Тази мярка може да бъде приложена, в случай че съществуват достатъчно убедителни основания да се приеме, че съответната държава членка е изправена пред сериозна заплаха за националната сигурност.

Същевременно, в решението се посочва, че IP адресите се генерират и извън рамките на определена електронна комуникация и в тези случаи служат най-вече за установяването на физическото лице - притежател на крайното оборудване, чрез което се осъществява интернет връзката. Ако се съхранява единствено IP адресът на източника на съобщението, но не и IP адресът на получателя, не се разкрива каквато и да е информация за трети лица, които са били в контакт с него. Поради тази причина следва да се приеме, че тази категория данни е с по-ниска степен на чувствителност, отколкото останалите трафични данни. В съответствие с горните разсъждения съдът постановява, че се допуска приемането на нормативна уредба, която предвижда всеобщо съхраняване на IP адреси, разпределени на източника на дадено съобщение.

В последната част на главата детайлно са изследвани различните възможности за последващи действия с цел изменение, допълнение и прецизиране на европейската и българската нормативна уредба в следствие на решенията на Съда на Европейския съюз.

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 приложим, вкл. за България, инструмент, който да установява конкретни правила за съхраняването на трафични данни за целите на наказателния процес. Поради тази причина понастоящем държавите членки прилагат множество фрагментирани режими, което води до сериозни трудности за националните органи при разследването и разкриването на престъпления с трансграничен елемент.

С оглед на това подходите, около които в България и в останалите държави членки на Европейския съюз de lege ferenda е възможно да се гради нова нормативна уредба (или да се измени настоящата), могат да се разделят в две основни категории: ограничено съхраняване на данни и подновяеми заповеди за съхраняване.

При ограниченото съхраняване по подобие на сега действащия режим запазването 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 важно значение за ефективното изпълнение на концепцията 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. Освен това би могла да се съкрати продължителността на сроковете за съхраняване, както и да се предвидят различни срокове за отделните категории данни в зависимост от степента им на чувствителност.

Ограниченото съхраняване на трафични данни за целите на наказателния процес цели значително намаляване на интензитета на намесата в личното пространство на засегнатите лица.

Моделът, основан на подновяеми заповеди за съхраняване, би имал за правно основание Директива 2002/58/ЕО и националното право, защото понастоящем липсва всеобщ европейски инструмент за съхраняването на трафични данни. Препоръчително е подновяемите заповеди да предвиждат задължение за съхраняване на данни от (почти) всички доставчици на услуги, тъй като оставянето на част от тях извън обхвата на приложената мярка може да доведе до вредни последици, ограничаващи възможностите за провеждане на ефективно разследване. В противен случай ще се създадат „сиви“ зони, в рамките на които извършителите на престъпни деяния ще действат, без да бъде възможно техните данни да попаднат законосъобразно в ръцете на компетентните национални органи.

Все пак може да се обмисли вариант, при който някои доставчици да бъдат изключени от кръга на задължените да съхраняват данни лица - въз основа на броя на техните потребители, когато той е твърде малък, или когато предоставят единствено определени специализирани услуги. Съдебният контрол следва да бъде задължителен елемент от производството, като в тази връзка трябва да се предвидят и правила относно обжалването на заповедите.

Необходимостта от издаването на заповедите следва да произтича от детайлна оценка на риска, която да спомогне за определянето на данните, които са строго необходими за целите на борбата срещу престъпността и които трябва да се съхраняват, както и на доставчиците, които генерират такива данни в процеса на своята дейност. Недостатък на модела, основан на подновяемите заповеди за съхраняване, е, че при включване в кръга на задължените лица на всички доставчици на услуги, на всички категории данни и при постоянно подновяване на заповедите той може да репликира всеобщото и неизбирателно съхраняване на трафични данни, отхвърлено в цялост от Съда на Европейския съюз.

Глава трета. Съхраняването и събирането на трафични данни в Република България.

В глава трета се акцентира върху функцията на трафичните данни като доказателство в процеса - значението им за разследването нараства все повече и повече, защото все по-голям брой престъпни деяния оставят следа в кибернетичното пространство под една или друга форма. Тези данни са основополагащи за разкриването на т.нар. „същински“ компютърни престъпления по Глава девета „а“ от Наказателния кодекс, а при множество други престъпления стойността на този вид данни също е особено висока. В случай на разследване на престъпно деяние трафичните данни са съществено важни с цел откриването на първоизточника на дадено съобщение, което от своя страна позволява събирането и на по-нататъшни доказателства. Получаването на трафичните данни, свързани с вече изпратени съобщения, може да бъде от значение с оглед определянето на източника или адресата на съобщението, което би могло да спомогне и за установяването на самоличността на лице, за което се предполага, че е извършило или ще извърши (тежко) престъпление. Доколкото обаче тези данни се съхраняват единствено за сравнително кратки периоди от време в съответствие с правилата за защита на данните и за тяхната неприкосновеност, компетентните разследващи и съдебни органи следва да действат възможно най-бързо.

Трафичните данни рядко служат като единствени доказателства - те по-често представляват първа стъпка към откриването на други следи, доказващи вината (или невиновността) на предполагаемия извършител. Освен това данните биха могли да послужат за целите на изясняването на определени факти - местоположението на дадено лице, дали то е било във връзка с друг заподозрян и др.

Разглежда се развитието на българската правна рамка за съхраняването на трафични данни от 2008 г. до днешни дни, като се отделя особено внимание на решението на Конституционния съд от март 2015 г. 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, но законосъобразността ѝ е оспорена пред Върховния административен съд, като чл. 5 от Наредбата, който урежда достъпа до съхранените данни от разследващите органи, е отменен поради противоречие с Конституцията. След решението на Върховния административен съд през 2009 г. в чл. 251 ЗЕС са приети изменения и допълнения, които „оцеляват“ до обявяването му за противоконституционен с Решение № 2 на Конституционния съд от март

2015 г. Конституционните съдии посочват, че макар да са въведени като средство за постигането на легитимна цел от общ интерес, разглежданите мерки за съхраняване и събиране на трафични 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 (достъп до трафични данни за разследването на престъпления, които не са тежки; прекомерно дълъг срок за съхраняване; липса на съдебен контрол в определени хипотези; липса на мотивационна част като отделен реквизит на искането). Поради тази причина цялата оспорена уредба в Закона за електронните съобщения е обявена за противоконституционна.

Представя се и приложимата национална правна уредба в областта на събирането на трафични данни за целите на разкриването, разследването и наказателното преследване на престъпления (Наказателно-процесуален кодекс (НПК) и Закон за електронните съобщения (ЗЕС)) след постановяването на посоченото решение на Конституционния съд. Още в края на март 2015 г. в Закона за електронните съобщения са приети изменения, като 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. 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; 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.

В Наказателно-процесуалния кодекс е създадена нова специална разпоредба (чл. 159а), която извежда в отделна норма задължението за предоставяне на данни от страна на доставчиците на обществени електронни съобщителни мрежи и/или услуги. Новата разпоредба въвежда специален режим и завишени изисквания относно събирането на трафични данни и данни за местоположението - доставчиците на услуги следва да предоставят данни, създадени при осъществяване на тяхната дейност, по искане на съда в съдебното производство или въз основа на мотивирано разпореждане на съдия от съответния първоинстанционен съд, постановено по искане на наблюдаващия прокурор в досъдебното производство.

В съответствие с чл. 159а, ал. 2 достъп до трафичните данни е възможен единствено когато това се налага за целите на разследването на тежки умишлени престъпления. По този начин законодателят дори отива отвъд изискванията на Конституцията, като лишава компетентните органи от възможността да получават достъп до трафични данни и данни за местоположението с оглед разкриването на извършени по непредпазливост тежки престъпления, преценявайки, че тяхната обществена опасност също не е достатъчно висока, за да оправдае съществената степен на намеса в личния живот на гражданите при предоставянето на изискваните данни на разследващите органи. Приемам аргументацията за изключването на непредпазливите деяния от приложното поле на разпоредбата, защото в общия случай обществената им опасност е по-ниска поради липсата на намерение за причиняване на противоправни последици.

От друга страна, не бива да се забравя, че в наказателноправния ни мир съществуват достатъчно престъпни състави, при които настъпилият резултат от извършеното по непредпазливост деяние е достатъчно значителен (например пътнотранспортно произшествие с множество пострадали). Важно е да се отчете, че за разлика от НПК при събирането на трафични данни извън рамките на наказателно производство ЗЕС не изключва от приложното поле на режима за достъп до такива данни тежките престъпни деяния, извършени по непредпазливост. Намирам, че *de lege ferenda* подходът в двата закона следва да бъде уеднаквен - не съществува причина, която да обосновава необходимост от разминаване в обхвата на двата набора от разпоредби.

Правят се и други конкретни предложения за усъвършенстване на нормативната уредба, вкл. по отношение на въпросите, свързани със спазването на основните права на гражданите при (незаконосъобразен) достъп до техните данни от страна на съдебните и разследващите органи. В съответствие с юриспруденцията на Съда на Европейския съюз и Европейския съд по правата на човека, както и с оглед ефективното прилагане на горепосочените средства за защита в НПК, е необходимо да се предвиди и съдът в съдебното производство и наблюдаващият прокурор в досъдебното производство да уведомяват лицето, за което са изискани данни по реда на чл. 159а, когато това няма да затрудни провеждането на наказателното производство. По този начин това лице ще може да защити правата си в съответствие с чл. 177а и 177б НПК, като подаде частна жалба в тридневен срок от узнаване на извършеното процесуално-следствено действие. В случаите, в които съдът прецени, че правата на лицето са засегнати незаконосъобразно, е налице нарушение по смисъла на чл. 2, ал. 1, т. 9 ЗОДОВ. Намирам, че по сходен начин уведомяване на засегнатото от събирането на трафичните му данни лице следва да се предвиди и

когато действието е извършено по реда на Закона за електронните съобщения.

Извършва се анализ на предоставянето на трафични данни от страна на доставчиците на услуги като един от способите на доказване, предвидени в НПК, с оглед систематичното му място в раздел „Претърсване и изземване“. Подкрепям тезата на проф. д-р Иван Видолов, че чл. 159 НПК урежда способа за доказване „изземване“, тъй като способите на доказване са предварително определени в кодекса, а сред изброените в чл. 136 НПК не присъства друг способ, чиито характеристики да описват начина за събиране на доказателства по чл. 159. Освен това разпоредбата систематически се намира в раздел „Претърсване и изземване“, в който не са уредени други способи за доказване освен претърсване и изземване. Смятам, че всички изводи, направени по отношение на чл. 159 НПК, са напълно валидни и спрямо събирането на трафични данни по чл. 159а, защото и в двата случая става въпрос за действия с идентични характеристики - съдът или органите на досъдебното производство задължават даден субект да предостави данни (или предмети), които се намират в негово притежание.

Въпреки това е необходимо да се отбележи, че изземването по чл. 159 и 159а НПК притежава някои значителни особености в сравнение с (претърсването и) изземването по чл. 161 – 163 НПК. При последното процесуално-следствените действия се извършват непосредствено от органите по разследването, докато по чл. 159 и 159а НПК доставчиците на услуги (или други субекти) се задължават да предоставят съответните (трафични) данни. Друга принципна разлика е, че в неотложни случаи претърсването и изземването могат да се извършат и без предварително съдебно разрешение, като протоколът от извършеното действие се представя за одобрение от съдията в 24-часов срок. Подобна възможност не е предвидена в НПК по отношение на събирането на трафични данни от предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги.

Разгледани са проверката и оценката на данните като доказателствен материал, които представляват основни етапи в процеса на доказване. Така например информацията от клетките на мобилните оператори може да се провери с други доказателства чрез извършването на следствен експеримент, чрез който да се установи дали е възможно дадено лице да се придвижи достатъчно бързо, за да пристигне (или избяга) на/от местопрестъплението за определено време. От своя страна, оценката е етапът на процеса, в който се правят изводи по отношение на допустимостта (относимост и законност), достоверността и достатъчността на събрания доказателствен материал. Относимостта на доказателствата изисква наличието на свързаност с предмета на доказване и възможност да

допринесат за разкриването на обективната истина. Съгласно чл. 159а, ал. 6 НПК, когато предоставената от доставчика справка съдържа данни, които нямат отношение към обстоятелствата по делото и не допринасят за тяхното изясняване, по мотивирано писмено предложение на наблюдаващия прокурор съдията, издал разрешението, разпорежда тяхното унищожаване. В седемдневен срок от получаването на разпореждането доставчикът и наблюдаващият прокурор предоставят на съдията протоколите за унищожаването на данните. Нормата е императивна и засяга всички неотносими данни, предоставени по реда на чл. 159а НПК. Наличието ѝ е необходимост, тъй като по всяка вероятност далеч не са редки случаите, в които справката съдържа значителен брой данни, които не са свързани с предмета на доказване по съответното дело.

В съответствие с чл. 105, ал. 2 НПК изискването за законност ще бъде спазено, ако трафичните данни са събрани при съблюдаване на предпоставките, посочени в чл. 159а. Важно е да се отбележи, че даденото разрешение от съда в досъдебното производство впоследствие не може да ограничи задължението на съда, който се произнася по въпросите за вината и отговорността, да извърши самостоятелна преценка относно допустимостта на всяко едно доказателство и доказателствено средство, представено от прокуратурата. Същевременно, не считам, че липсата на някой от изброените в чл. 159а, ал. 3 и 4 реквизити на искането или съдебното разпореждане (например посочване на разследващия орган, на който да се предоставят данните) задължително следва да води до изключване на предоставените данни от доказателствената съвкупност.

Анализира се и възможността трафичните данни, събрани извън рамките на наказателно производство по реда на ЗЕС, да бъдат включвани в доказателствената съвкупност в процеса, без да е налице необходимост от повторното им събиране. Този подход значително ще облекчи работата на правораздавателните и правоохранителните органи, доколкото ще премахне необходимостта от двукратното извършване на една и съща дейност. То е абсолютно излишно, още повече че след 2015 г. процедурите по изискването и предоставянето на данните по реда на ЗЕС покриват в необходимата степен всички стандарти за гарантиране на основните права на гражданите (съдебен контрол, срокове, съдържание, реквизити на исканията и т.н.). По този начин би се избегнал и рискът от последващо заличаване на информацията в промеждутъка между осъществяването на двете процедури.

Накратко се обръща внимание и на Закона за специалните разузнавателни средства, тъй като той урежда способи за прихващане на трафични данни в реално време. Макар че прихващането на данни в реално време не представлява основен способ за събирането на трафични данни, трябва да се обърне внимание на факта, че в някои държави използването на

специални разузнавателни средства (по ЗСРС) и предоставянето на трафични данни (по ЗЕС) се осъществяват по реда на една и съща нормативна процедура, като съществуват предложения този подход да бъде възприет и у нас. Смятам, че *de lege ferenda* подобен вариант е напълно мислим, но въпреки редицата прилики в процедурите за събиране на трафични данни по ЗЕС и използването на специални разузнавателни средства по реда на ЗСРС намирам, че пълното уеднаквяване на двата режима няма да представлява удачен подход поради различията в особеностите на трафичните данни и на кореспонденцията (данни за съдържанието), която преимуществено се прихваща чрез специалните разузнавателни средства.

Глава четвърта. Събирането на трафични данни в трансгранични случаи.

Последната четвърта глава се концентрира върху събирането на трафични данни в трансгранични случаи и в нея се представят принципите, произтичащи от международните актове в областта на сътрудничеството по наказателноправни въпроси, по които Република България е страна, както и от инструментите на правото на Европейския съюз, които имат отношение към въпросите, свързани с предоставянето на достъп до трафични данни за целите на противодействието на престъпността. Предмет на разглеждане е еволюцията на моделите на международно сътрудничество в областта на наказателния процес - от традиционния, при който данните се обменят единствено между компетентните държавни органи, към подход, в рамките на който се осъществява непосредствена комуникация с частни субекти - доставчици на услуги, установени в друга държава, които следва да предоставят изисканите доказателства, необходими за разкриването на обективната истина в наказателното производство.

В почти две трети от случаите, в които е необходимо събирането на електронни доказателства (65%), следва да се изпрати молба за правна помощ или друг вид искане за предоставяне на информация до доставчик на услуги със седалище или място на стопанска дейност извън територията на държавата, където се води разследването. Обобщено, статистиката показва, че в цели 55% от всички разследвания е налице необходимост от предоставянето на трансграничен достъп до електронни доказателства. Тази необходимост постепенно, но неизбежно повишава и усилията в посока на подобряване на правната уредба, която да позволи възможно най-ефективно събиране на електронни доказателства при спазване на всички гаранции за основните права на човека.

В главата се прави преглед на Конвенцията, съставена от Съвета в съответствие с чл. 34 от Договора за Европейския съюз (ДЕС), за взаимопомощ по наказателноправни въпроси между държавите членки на

Европейския съюз (известна като Конвенция 2000), която е първият акт на Съюза, който урежда взаимната правна помощ по наказателноправни въпроси и в частност - прихващането на данни в реално време, както и на Директива 2014/41/ЕС относно Европейската заповед за разследване по наказателноправни въпроси.

Специално внимание се обръща на Конвенцията за престъпления в кибернетичното пространство от 2001 г., която е ратифицирана от почти всички държави членки на Съвета на Европа, както и от множество страни извън организацията. В българска среда действията по ратифицирането на Конвенцията през 2005 г. водят до редица допълнения в българския правен ред: дефиницията за „компютърни данни“ в НК; задължението за предоставяне на данни за абоната на компютърно-информационна услуга и на трафични данни (чл. 159 и 159а НПК); текстовете относно претърсването и изземването на компютърна информационна система и на компютърни информационни данни в чл. 162 и 163 НПК; задължението за доставчиците на компютърно-информационни услуги да подпомагат съда и органите на досъдебното производство при събирането и записването на компютърни информационни данни чрез прилагане на специални технически средства и др.

Поради всеобщата необходимост от приемането на мерки, които да ускорят трансграничния обмен на електронни доказателства за целите на наказателното производство, в рамките на Съвета на Европа през 2017 г. беше инициирано разработването на Втори допълнителен протокол към Конвенцията от 2001 г. Чрез разпоредбите на протокола се цели и създаването на по-голяма правна сигурност по отношение на условията, при които доставчиците на услуги могат да отговарят на непосредствени искания, отправени от правоохранителните органи за целите на предоставянето на достъп до конкретни данни в цифров формат. Вторият допълнителен протокол представлява в известна степен революция в международното сътрудничество по наказателноправни въпроси, защото за първи път позволява директна комуникация между компетентните органи на една държава с доставчик на услуги, който се намира на територията на друга.

Приемането на Втория допълнителен протокол към Конвенцията от Будапеща представлява стъпка напред в повишаването на ефективността на наказателноправното сътрудничество, поради което *de lege ferenda* намирам, че ратифицирането му от страна на България ще допринесе значително за подобряването на възможностите на националните ни органи във връзка със събирането и достъпа до електронни доказателства за целите на наказателния процес. За да се осигури прилагането на Протокола е необходимо приемането на някои допълнения в Наказателно-

процесуалния кодекс, в Закона за Министерството на вътрешните работи, в Закона за електронните съобщения и в Закона за електронната търговия.

Въпреки наличието на редица инструменти на европейското и на международното право за правна помощ по наказателни дела, предоставящи възможност за осъществяването на трансграничен обмен на електронни доказателства, вкл. трафични данни, разследващите органи са изправени пред множество трудности, които възпрепятстват бързото и навременно предоставяне на данни, необходими за предотвратяването, разкриването и разследването на престъпни деяния. Основно затруднение в тази насока представлява прекалената тромавост на процедурите, провеждането на които често изисква твърде дълги срокове (седмици, месеци, понякога дори повече).

След задълбочено и продължително обществено обсъждане с всички заинтересовани страни през април 2018 г. Европейската комисия представи две законодателни предложения, които целят подобряването на трансграничния достъп до електронни доказателства - предложение за Регламент и Директива. В сърцевината на двата акта стоят повишаването на скоростта на презграничния обмен на електронни доказателства, облекчаването на компетентните органи в осъществяването на този процес, гарантирането на правна сигурност за доставчиците на услуги, които вече ще прилагат единен и опростен режим с ясни, точни и конкретни правила, както и спазването на основните права на човека чрез предоставянето на ефективни правни средства за защита.

В Регламент (ЕС) 2023/1543 се въвежда специален режим (европейски заповеди за предоставяне и запазване на данни), съгласно който разследващите органи на държавите членки могат да се обръщат директно към доставчиците на услуги на територията на Европейския съюз във връзка с предоставянето и запазването на данни, необходими за целите на наказателния процес. Следва да се отбележи, че непосредствено приложимият и в България Регламент не заменя Европейската заповед за разследване и инструментите на международната правна помощ, а създава допълнителна алтернатива, която следва да гарантира ускорения достъп до електронни доказателства на европейско равнище.

Европейските заповеди могат да се издават само за целите на наказателното производство и за изпълнението на наказание лишаване от свобода или на мярка за задържане за срок не по-малък от четири месеца, вследствие на наказателно производство. Задължени по смисъла на Регламента са следните видове доставчици на услуги: доставчици на електронни съобщителни услуги; доставчици на имена на домейни, регистър на имена на домейни и др.; доставчици на услуги на информационното общество. Регламентът се прилага спрямо всички

доставчици, които предлагат услуги на територията на Съюза, вкл. доставчици, чиито седалища се намират извън Европейския съюз.

Компетентните национални органи могат да изискват от доставчиците на услуги да предоставят и запазват, както в рамките на досъдебното производство, така и в съдебната фаза на наказателния процес, следните видове данни: потребителски данни; данни, поискани единствено с цел идентифициране на ползвателя; трафични данни; данни за съдържанието. В българска среда въвеждането на категория „данни, поискани единствено с цел идентифициране на ползвателя“ може да създаде проблеми при прилагането на Регламента, защото сходна категория не съществува в националното ни право. Възможно решение *de lege ferenda* може да бъде създаването на нова алинея в чл. 159а НПК, в която да се посочи, че ал. 1 - 6 на същия член не се прилагат, когато данните по ал. 1, т. 1, 3 и 5 се изискват само с цел установяването на самоличността на потребителя и не са свързани с осъществяването на повиквания или предаването на съобщения, като целта трябва задължително да се посочи в искането.

В случаите, в които съгласно Регламента заповедта за предоставяне освен на доставчика на услуги се изпраща и на компетентен орган на държавата членка, в която доставчикът е установен, този орган може в десетдневен срок след получаване на уведомлението да се позове на някое от предвидените основания за отказ от изпълнение. Предвижда се изпълнението на заповедта да може да бъде отказано, когато трафичните данни са защитени от имунитет или привилегия съгласно правото на изпълняващата държава или попадат в приложното поле на правила относно определянето или ограничаването на наказателната отговорност, свързани със свободата на изразяване, които възпрепятстват изпълнението на заповедта.

Необходимо е да се отбележи, че в Наказателно-процесуалния кодекс не е предвидена изрична забрана за предоставянето на трафични данни за лице с имунитет, произтичащ от Конституцията на Република България. Съгласно чл. 220, ал. 1 НПК наказателното преследване срещу лице с имунитет се възбужда след отпадането на имунитета, но подобно ограничение не е уредено във връзка със събирането на доказателства и по-конкретно по чл. 159а НПК. Въпреки това в Решение № 12 от 2020 г. Конституционният съд посочва, че „изразът „*не може да бъде възбудено наказателно преследване*“ не е пречка по досъдебно производство да се извършват всички действия по разследването, стига те да не представляват по естеството си насочване на обвинение към лица с имунитет. Поради горните съображения намирам, че *de lege ferenda* следва да се обмисли предвиждането на изрично ограничение на непосредственото събиране на доказателства, вкл. трафични данни, по отношение на лице с имунитет (освен в случаите, в които лицето с имунитет е пострадал от извършеното

престъпно деяние), доколкото в противен случай наказателната му неприкосновеност, произтичаща от имунитета, би се оказала лишена от съдържание.

Представят се и особеностите на Директива (ЕС) 2023/1544, която има спомагателен характер спрямо Регламент (ЕС) 2023/1543 и установява правила за определянето на представител на доставчиците, които предлагат услуги на територията на Европейския съюз, който да получава и изпълнява заповедите за предоставяне и запазване на данни. Целта на Директивата е намаляване на правната несигурност чрез въвеждането на общоевропейско решение. То премахва необходимостта от приемането на индивидуализирани и некоординирани подходи на национално равнище по отношение на определянето на оправомощени лица, които да изпълняват заповедите за предоставяне и запазване на данни. Задължението за определяне на представител се отнася до всички доставчици, предоставящи услуги на територията на Съюза, без значение от това къде се намира тяхното седалище - в държава членка или в трета държава.

В българското законодателство Директива (ЕС) 2023/1544 следва да бъде въведена чрез допълнения в Закона за електронните съобщения, който урежда дейността на доставчиците, предоставящи обществени електронни съобщителни мрежи или обществени електронни съобщителни услуги, както и в Закона за електронната търговия, който установява правила относно дейността на доставчиците на услуги на информационното общество.

Разглежда се и темата за сътрудничеството с доставчиците на електронни съобщителни услуги със седалище в САЩ, както и със съответните американски компетентни органи, тъй като огромна част от необходимите за целите на разследването данни се намират именно в притежание на американски доставчици поради значителния им пазарен дял.

Заключение

Анализът в дисертационния труд показва, че успешното използване на трафичните данни като доказателствен материал в наказателния процес изисква модернизирана нормативна рамка, съобразена със съвременното технологично развитие и със стандартите за защита на основните права на човека. Ето защо се предлага усъвършенстване на понятийния апарат в Наказателно-процесуалния кодекс, който към момента не отразява спецификите на електронните комуникации. Наред с това на национално равнище следва да бъде ясно регламентирано ограничаването на непосредственото събиране на доказателства, включително трафични данни, по отношение на лица с имунитет, освен ако те не са пострадали от престъплението, за да се избегне обезсмисляне на предоставената им наказателна неприкосновеност. Наложително е да се предвиди и

отговорност на държавата за вредите, причинени на граждани от разследващите органи, прокуратурата или съда, във всички случаи на незаконосъобразен достъп до трафични данни.

В международен и европейски план, вкл. по отношение на усъвършенстването на българското законодателство, централно място в предложените в изследването промени заема принципът на „ограничено съхраняване“ на трафични данни, който съчетава нуждите на разследването с изискванията за защита на основните права на гражданите. Неговото прилагане би гарантирало ефективност на наказателното преследване, без да се нарушава принципът на съразмерност. Ратифицирането на Втория допълнителен протокол към Конвенцията за престъпленията в кибернетичното пространство от страна на Република България също би представлявало значим напредък. То ще разшири възможностите за по-бързо и ефективно трансгранично събиране на електронни доказателства и ще укрепи международното сътрудничество, което е ключово в настоящите социално-икономически условия. В изследването се предлагат и множество мерки във връзка с осигуряването на прилагането на Регламент (ЕС) 2023/1543, както и за въвеждането на Директива (ЕС) 2023/1544 - водещите инструменти на правото на Европейския съюз в областта на събирането на електронни доказателства за целите на наказателното производство.

Използването на трафичните данни като доказателствен материал в българския наказателен процес изисква комплексен, модерен и балансиран подход, съобразен както с националните, така и с европейските и международните реалности. Технологичните промени не просто предизвикват развитие на правната уредба - те го правят напълно неизбежно. Създаването на адекватно законодателство в наказателноправната област, усъвършенстването на процесуалните гаранции и повишаването на компетентността у всички участници в процеса по отношение на боравенето с електронни доказателства са ключът към осигуряване на ефективно правосъдие и постигане на основната цел на наказателното производство - разкриване на обективната истина при зачитане на основните права и свободи на гражданите.

Библиография

Броят на използваните литературни източници е 84, от които 34 на български език и 50 - на английски, немски и френски език.

III. НАУЧНИ ПРИНОСИ В ДИСЕРТАЦИОННИЯ ТРУД

Дисертационният труд е първото детайлно изследване относно доказването чрез трафични данни и ролята им в българския наказателен процес.

1. Уеднаквяване на понятийната система в Наказателния (НК) и Наказателно-процесуалния кодекс (НПК) по отношение на термините и „компютърни данни“ и „компютърни информационни данни“ чрез ползването на „електронни доказателства“, тъй като по същество за еднакви по съдържание понятия понастоящем се използват различни, макар и близки, и остарели формулировки.

2. Обособяване на електронните доказателства като отделна категория доказателствен материал (сравнение с веществените и невеществените доказателства) поради специфичното им естество.

3. Предложения за подобряване на нормативната уредба на българско и европейско равнище в областта на съхраняването на трафични данни чрез ползването на два подхода, които биха могли да се прилагат както алтернативно, така и кумулативно: ограничено съхраняване на данни и подновяеми (периодични) заповеди за съхраняване.

4. Уеднаквяване на предпоставките за събиране на трафични данни по реда на Наказателно-процесуалния кодекс и Закона за електронните съобщения, тъй като не съществува причина, която да обосновава необходимост от разминаване в обхвата на двата набора от разпоредби.

5. Приемане на допълнение в Закона за отговорността на държавата и общините за вреди (ЗОДОВ) - отговорност за вреди, причинени на граждани от разследващите органи, прокуратурата или съда, в случай на незаконосъобразен достъп до трафични данни.

6. Приемане на допълнение в Наказателно-процесуалния кодекс, в което да се предвиди, че съдът в съдебното производство и наблюдаващият прокурор в досъдебното производство уведомяват лицето, за което са изискани данни по реда на чл. 159а НПК, когато това няма да затрудни провеждането на наказателното производство (в съответствие с юриспруденцията на Съда на Европейския съюз и Европейския съд по правата на човека). По сходен начин уведомяване следва да се предвиди и когато действието е извършено по реда на Закона за електронните съобщения.

7. Хармонизиране на нормативната процедура за използването на специални разузнавателни средства (по Закона за специалните разузнавателни средства) и предоставянето на трафични данни (по Закона за електронните съобщения) при вземане предвид на особеностите и

чувствителността на трафичните данни и на кореспонденцията (данни за съдържанието) като видове електронни доказателства.

8. Ратифициране на Втория допълнителен протокол към Конвенцията за престъпленията в кибернетичното пространство от 2001 г., което ще допринесе значително за подобряването на възможностите на националните ни органи във връзка със събирането и достъпа до електронни доказателства за целите на наказателния процес.

9. Приемане на допълнения в Наказателно-процесуалния кодекс, Закона за Министерството на вътрешните работи, в Закона за електронните съобщения и в Закона за електронната търговия, с оглед осигуряването на прилагането на Втория допълнителен протокол.

10. Приемане на допълнение в чл. 159а от Наказателно-процесуалния кодекс с оглед осигуряването на прилагането на понятието по чл. 3, т. 10 във връзка с чл. 4, пар. 2 от Регламент (ЕС) 2023/1543 „данни, поискани единствено с цел идентифициране на ползвателя“.

11. Приемане в Наказателно-процесуалния кодекс на изрично ограничение на непосредственото събиране на доказателства, вкл. трафични данни, по отношение на лице с имунитет (освен в случаите, в които лицето с имунитет е пострадал от извършеното престъпно деяние), доколкото в противен случай наказателната му неприкосновеност, произтичаща от имунитета, би се оказала лишена от съдържание (в съответствие с практиката на Конституционния съд).

IV. ПУБЛИКАЦИИ НА АВТОРА ПО ТЕМАТА НА ДИСЕРТАЦИОННИЯ ТРУД

1. “Съхраняването на трафични данни в Република България” - статия, публикувана на интернет страницата „Предизвикай правото“;

2. „Събирането на трафични данни в Република България“ - статия, публикувана на интернет страницата https://news.lex.bg;

3. “Същност на трафичните данни и значението им като доказателствен материал в наказателния процес” - доклад за научна конференция „Знание, наука, иновации, технологии“, 28 март 2025 г., публикуван в сборника от конференцията;

4. “Директно сътрудничество с частни субекти - (р)еволюция в трансграничното събиране на електронни доказателства” - доклад за научна конференция „Знание, наука, иновации, технологии“, 12 декември 2025 г., публикуван в сборника от конференцията.