СПИСАНИЕ
DE JURE

ОФИЦИАЛНО ИЗДАНИЕ НА
ЮРИДИЧЕСКИЯ ФАКУЛТЕТ НА
ВТУ „СВ. СВ. КИРИЛ И МЕТОДИЙ“

Брой 1/2022 (24), ISSN 1314-2593 (Print), ISSN 2367-8410 (Online)

DOI: 10.54664/CTYJ5693

ЕЛЕКТРОННИ ДОКАЗАТЕЛСТВА

Димитър Младенов

ELECTRONIC EVIDENCE

Dimitar Mladenov

Abstract: *The article deals with special characteristics of electronic evidence in criminal procedure, the need for a new type of classification, and the involvement of an expert in seizing and dealing with it. The paper also considers the legal way of seizing such evidence, the distance seizure of computer data, the legal procedure of collecting electronic traffic data, as well as the legal way to handle and accept video records as evidence.*

Keywords: *electronic evidence, criminal procedure.*

Преди двадесет години списание Правна мисъл издаде авангардната и изпреварила времето си статия на проф. Маринова за електронните доказателства[1]. Към момента на написване на статията липсваше каквато и да е правна уредба на електронните доказателства в НПК, не бяха приети специалните компютърни престъпления[2], като единствените правни източници, на които можеше да се позове изследователя на темата бяха различни международни актове. Независимо от това, Маринова ясно дефинира спецификата на електронните доказателства и нуждата от законодателни промени: „Тенденцията в развитието на обществото, свързана с все по-широко използване на компютърни и въобще на електронни технологии е ясна… Това налага и необходимостта от съответни изменения и допълнения в наказателнопроцесуалното ни законодателство, насочени към въвеждане и дефиниране на нов вид доказателства и доказателствени средства за тяхното закрепване и възпроизвеждане в процеса, както и съответните изменения в способите за събиране и проверка на тези доказателства, които да отчетат особеностите им“[3].

Днес, двадесет години по-късно, са формулирани компютърни престъпления в НК[4], приети са специфични процесуални правила свързани с достъпа и изземането на електронни доказателства, но не са преодолени трудностите в събирането и оценката на електронните доказателства. Успехите на прокуратурата и МВР в разкриване на компютърни престъпления и предаване на извършителите им на съд са скромни: За 2020 г. от общо образувани 120 ДП[5] за престъпления по глава 9А НК, в съда е внесен само едни прокурорски

[1] **Маринова, Г**. Електронните доказателства. – Правна мисъл, бр. 3/2002, с. 58–73.

[2] Глава 9А от НК.

[3] **Маринова, Г**. Цит. съч.., с. 72–73.

[4] Под **компютърно престъпление** разбирам специалните компютърни престъпления по глава 9А НК и всяко друго престъпление извършено в дигитална среда или значително улеснено от дигитално устройство.

[5] Досъдебно производство.

акт[6]. Подобна е ситуацията и за предходните години: за 2019 г. за новообразувани 80 ДП, а в съда са внесени 4 прокурорски акта[7]; за 2018 г.- новообразувани 75 ДП, а в съда са внесени 4 прокурорски акта[8]: за 2017 г. новообразувани 75 ДП, а в съда са внесени 0 прокурорски акта[9]. За посочените 4 години са образувани общо 350 ДП, а в съда са внесени общо 9 прокурорски акта, което представлява разкриваемост от 2,57%. Размерът на скритата престъпност, при този род престъпления е огромен. Извън посочените данни остават различни престъпления извършвани основно по електронен път, като компютърната измама по чл. 212А НК, невярно деклариране по електронен път – чл. 313, ал. 3 НК и др., при които успеваемостта на разследващите органи и прокуратурата да разкрият извършителя и да го предадат на съд е малко по-голяма. Подобни ниски нива на противодействие на компютърната престъпност са причинени от неразбиране на нейната специфика и на нуждата от нови методи за противодействие, защото стандартните методи са крайно неефективни.

1.Същност на електронните доказателства

Електронните доказателства, според законовото определение на доказателствата в наказателното производство[10], представляват фактически данни, които са свързани с обстоятелствата по делото, допринасят за тяхното изясняване и са установени по реда предвиден в този кодекс[11]. Поради своята техническа специфика електронните доказателства следва да се дефинират допълнително.

Наличното в теорията определение на Маринова на електронните доказателства отразява до голяма степен тяхната специфика:

„Електронни данни, (т.е. данни които се преобразуват по електронен път, за да бъдат от една страна обект на автоматична обработка от електронни устройства, а от друга – обект годен за възприемане от хората), които са свързани с обстоятелствата по делото, допринасят за тяхното изясняване и са установени по реда на НПК. Казано по друг начин електронните доказателства са фактически данни по чл.84 НПК[12], които имат електронен характер.“[13]

Напълно приемам даденото от Г.Маринова определение. То може да се подобри и прецизира[14], но нищо съществено не липсва в него.

Електронното доказателство представлява дигитален електронен запис в две състояния: логическа 0 и логическа 1, като наличието на напрежение, електромагнитно поле или оптично-отразена светлина се възприема като логическа единица, а липсата на напрежение, на електромагнитно поле или на отразена светлина (поради прогорена дупка в оптичния диск), се третира като логическа нула.

---

[6] Доклад за прилагането на закона и за дейността на прокуратурата и на разследващите органи през 2020 г., с. 40.

[7] Доклад за прилагането на закона и за дейността на прокуратурата и на разследващите органи през 2019 г., с. 36

[8] Доклад за прилагането на закона и за дейността на прокуратурата и на разследващите органи през 2018 г., с. 33.

[9] Доклад за прилагането на закона и за дейността на прокуратурата и на разследващите органи през 2017 г., с. 38.

[10] Виж: чл.104 НПК.

[11] Понятието за доказателствата в наказателното производство е подробно разработено в теорията. Вж.: **Сарановъ, Н**. Българско наказателно-процесуално право. София: Печатница „Художник“,1937, т. 2, с. 183–184; **Павлов,С**. Наказателен процес на НРБ. С.: НИ, 1959, с. 377–405. **Чинова, М**. Досъдебното производство по НПК. С.: Сиела, 2013, с. 498–505.

[12] Чл. 84 от НПК от 1974 г. отм. съответства на чл. 104 от сега действащия НПК и е с идентично съдържание.

[13] **Маринова, Г**. Цит. съч., с.65.

[14] Предлагам следната редакция на понятието за електронните доказателства: Това е специфична група доказателства по смисъла на чл.104 НПК, които представляват **бинарно дефинираната информация**, която се интерпретира, чрез строго дефинирани алгоритми в текст, образ, звук или някакво понятно за човека действие.

Този принцип на дефиниране на информацията се нарича двоичен, защото разполага с две състояния за обозначение и представлява един бит[15]. Думата е създадена като съкращение на binary digit – „двоична цифра“[16]. Това техническо определение на електронните доказателства показва тяхното машинно естество, което е напълно недостъпно за човека в непреработен вид. Бинарно дефинираната информация става достъпна за сетивата и съзнанието на човека, след като се **интерпретира**, чрез строго дефинирани алгоритми в текст, образ, звук или някакво действие.

Именно този преобразуван вид, дигиталната информация може да бъде електронно доказателство. Това показва, че за правилната оценка на електронното доказателство е от съществено значение както първоначалният дигитален запис, така и алгоритъмът за преобразуването му в текст, образ, звук или някакво действие, което може да се възприеме от сетивата и съзнанието на човека посредством периферно устройство (екран, принтер, тонколони и др.) Тези особености на електронните доказателства показват, че те са напълно специфични по своето естество от останалите материални вещи и следва да се третират по различен начин. Те са колкото реални, толкова и виртуални, и поради своята двойнствена природаможе да се приеме, че изграждат собствена специфична дигитална квази реалност.

2.Нова класификация на електронните доказателства.

В своя анализ на естеството на електронните доказателства Маринова правилно отчитайки тяхната специфика ги отделя от веществените доказателства и ги поставя в групата на невеществените[17]. Това разбиране се подкрепя и от Чинова[18]. Намирам за неправилно включването на електроните доказателства в категорията на невеществените доказателства. Според Павлов, невещественси са: „онези доказателствени факти, които се свеждат до следи останали в съзнанието на хората, до факти на вътрешния психичен мир на човека….Невещественните доказателства никога не могат да се възприемат непосредствено от съда и да се приложат по делото. Те се включват в орбитата на доказателствата в процеса всякога посредством възпроизвеждането им.[19]“ Очевидно е, че електронните доказателства не могат да се включат в една категория с невещественните доказателства, които като част от съзнанието на човекаса напълно субективни и за независим достъп, към момента, не разполагаме с обективна технология[20]. Напротив, електронните доказателства могат да бъдат разчетени напълно обективно, да се представят непосредствено в съда и да се приложат по делото в цифров вид и като хартиена разпечатка. От своя страна, електронните доказателства имат веществена страна, която става достъпна за сетивата и съзнанието на човека, след като се **интерпретира**, чрез строго дефинирани алгоритми в текст, образ, звук или някакво действие. Невещественните доказателства нямат подобна веществена страна, която да подлежи на непосредствено обективно изследване и интерпретация.

Поради това, използването на старото деление на доказателствата на веществени и невещественси не е добър начин за отразяване на спецификата на електронните доказателства. С оглед подчертаване на тяхната специфика и самостоятелност е удачно да използваме нова класификация на доказателствата на виртуални (електронни) и реални (материални). Като електронни следва да разбираме всички доказателства базирани на бинарен цифров код, който посредством дефинирани алгоритми се превръща в текст, образ, звук или някакво действие. Всички останали вещи, които нямат подобна бинарна природа, следва

[15] На английски: bit е най-малката информационна единица за измерване на количеството информация от нейното вътрешно представяне в компютрите.

[16] **Захариев, Ганчевски и др**. Разкриване и разследване на компютърни престъпления. (практическо ръководство) София: Сиби, 2006, с. 14–15.

[17] **Маринова, Г.** Цит. съч., с. 66.

[18] **Чинова, М.** Цит. съч., с. 512.

[19] **Павлов, С.** Цит. съч., с. 447.

[20] Практиката с детектор на лъжата да се верифицират свидетелски показания не е законово уредена и не е безспорна от научна гледна точка.

да се отнесат към реалните доказателства. Подобна класификация има свой познавателен и дидактичен смисъл, защото, отделя електронните доказателства от останалите вещи и с това набляга на тяхното специфично естество, което изисква специално третиране. Обособяването на електронните доказателства в отделнагрупа има своята перспектива, защото дигиталните технологии завземат нови и нови сфери на дейността на човека и създават специфична дигитална реалност.

3. Задължително участие на специалист – технически помощник при изземането на електронни доказателства.

Изземане на компютърни информационни данни при претърсване и изземане се извършва с извършва със **задължителното участие на специалист – технически помощник** – чл. 162, ал. 6 НПК.

Според мен, тази норма е със задължителен характер и нарушаването й е съществено процесуално нарушение, което опорочава законосъобразното изземане на електронните доказателства. Участието на специалист в хода на претърсване и изземане, които са с принудителен характер доказва, че данните са иззети правилно, в пълен обем и без промени, и е гаранция за правата на засегнатите лица, срещу които тези данни може да се използват като доказателство. Друг е въпросът доколко разследващите органи разполагат с толкова голям брой специалисти, които да се включат в извършените от тях претърсвания и до колко тези специалисти действително са експерти в компютърната област. Поради огромните възнаграждения в бизнеса, които получават действителните експерти в областта на компютърните науки, едва ли разследващите органи ще могат да си позволят наемането на истински експерти. Това представлява риск, за правилното изземане и съхраняване на електронните доказателства.

Подобна норма липсва, когато данните се предават доброволно – чл. 159, ал. 1 НПК. Това е неправилно. Компютърен специалист следва да участва при всеки случай, в който се борави с електронни доказателства по какъвто и да е повод, защото за правилното изземане и съхранение на данните са нужни специални знания и умения.

Нужно е не просто да се предвиди задължително участие на компютърен специалист при работата с електронни доказателства, нужно е детайлно да се дефинират в закона ползваните от него програми и методи за изземане, съхранение и ползване на електронни доказателства, което ще гарантира достоверността и липсата на манипулации с иззетите данни[21]. Компютърният експерт, участващ в производството като технически помощник или вещо лице следва да използва само определените в закона програми и методи за изземане или анализ на електронни доказателства, като тези нормативно зададени методи ще гарантират достоверността и правилната оценка на електронните доказателства[22]. В момента, всеки експерт може да ползва каквито си поиска програми и методи, а това създава риск за правилното изземане на данните и не дава никаква възможност за защита на засегнатите лица. Само така може ясно да се отграничат действията на ползвателя на електронната система, от тези на хакери проникнали в нея дистанционно със зловреден софтуеър. Възможността инкриминираните електронни доказателства да са създадени не от ползвателя на системата, а от хакери, които са завладели ползвания компютър или друго устройство задължително следва да се провери[23].

---

[21] Например използвания от множество правоохранителни агенции – **Triage**. Вж: **Василев, Димитров**. Методика за разследване на киберпрестъпления. Електронни подписи-същност и правни проблеми. Н. Сл. С, София, 2015, с. 100–102.

[22] Най-широко използваните програми за анализ са **Forensic Toolkit (FT**K) и **EnCase**, които извличат текстови файлове, електронна поща, история от сърфирането в интернет и др.,възстановяват изтрити файлове, в някои случаи и след форматиране на твърдия диск. Виж: **Василев, Димитров.** Цит. съч., с. 134.

[23] Разследващите органи следва да са наясно, че това е основаната защитна позиция при обвинение в компютърно престъпление и ако желаят да докажат евентуално обвинение насочено срещу ползвателя, подобна възможност следва да се обори категорично.

При изземане на електронни доказателства рискът от грешки[24] е особено голям, като присъствието на поемни лица не дава никакви гаранция за защита срещу злоупотреби, ако поемните лица не са компютърно грамотни и непрекъснато не наблюдават действията на експерта по изземане на данните. В този смисъл, при извършване на принудителни действия свързани с изземане на електронни доказателства следва да се въведе изискването за компютърна грамотност на поемните лица. Електронна поща се иззема по реда за изземане на кореспонденция-чл.165,ал.6 НПК, като за това е нужно отделно съдебно разрешение.

Основният стремеж, според авторите на цитираната методика, при провеждане на изследването е по възможност да се запазят електронните данни в техния оригинален вид. Поради тази причина, вещото лице не следва да работи върху оригиналния твърд диск на иззетата компютърна система, а върху предварително изготвеното с помощта на специализиран софтуер и хардуер копие /имидж/. В този смисъл, повдигания понякога в практиката спор какво следва да бъде обект на изследване - оригинал или цифрово копие е безпредметен. Изследването се провежда върху създадено по определен ред пълно цифрово копие на информационния носител. Поради способността на електронните доказателства да се мултиплицират, това копие е идентично с оригинала. Този метод на изследване дава възможност на независими трети лица да повторят тези действия и да получат същите резултати.[25]

От особено значение за разкриване на действителния автор на компютърното престъпление е установяване на неговата мотивация[26].

4. Компютърните информационни данни задължително се записват на хартиен и на електронен носител.

При изземане на компютърни информационни данни, които не могат да се отделят от мястото на което са намерени, задължително се изготвят две веществени доказателствени средства:

а/запис на специализиран електронен носител-чл.125,ал.1 НПК.

б/запис на хартиен носител-чл.135 НПК.

Тези две общи правила за изземане на компютърни информационни данни са допълнително разширени при извършване на претърсване и изземване-чл.163,ал.7 НПК, като са въведени специални правила за запечатване на електронния носител, подписване на всяка разпечатана страница от всички участници в претърсването и специални правила за разпечатване и ползване на електронния носител (само с разрешение на прокурора в ДП или съда в съдебната фаза, в присъствие на поемни лица само на ДП и специалист-технически помощник).

Този сложен ред за изземане на компютърни информационни данни поставя въпроса дали ще е законосъобразно изземане на самите носители на тези данни[27] в хода на претърсване, оглед или доброволно предаване, като на същите в последствие ще се възложи компютърно-техническа експертиза за извличане на нужните данни. На този въпрос следва да се отговори положително, защото не се изземат никакви данни, а вещи в които се предполага наличие на тези данни. В практиката въпросът дали ще се иззема цялото електронно оборудване или само данните без материалните носители, чрез изготвяне на огледално копие (имидж) на носителя на данните е уреден с вътрешен акт на Н.Сл.С.[28] за всички следователи. Условията да се пристъпи към изземане на самото оборудване са: да са налице малък брой системи и устройства, нужно е за пресичане на престъпната дейност или има риск от последващо въздействие вър-

[24] При оглед, претърсване и изземане, не се стартират програми и не се отварят никакви файлове, тъй като това би довело да промяна на характеристиките им – например часът и датата на последен достъп до файла и модификацията му, виж: Василев, Димитров. Цит. съч., с. 108.

[25] **Василев, Димитров.** Цит. съч., с. 138.

[26] За мотивите за извършване на компютърно престъпление виж: **Василев, Димитров.** Цит. съч., с. 117–119.

[27] Твърди дискове, таблети, телефони, флашки и др.

[28] Виж: чл. 8.6.1 и 8.6.2, от **Правила** за претърсване и изземване на компютърни информационни системи и компютърни информационни данни, утвърдени със заповед № з-75/26.05.2016 г. на Директора на НСл. С г-н Е. Диков.

ху носителите на данните, да липсва риск от финансови загуби на трета страна[29]. Изземането на електронните устройства от офиса на търговец може да доведе съответна търговска дейност до невъзможност да се продължи и до фалит. Поради това, евентуалните щети за легалната търговска дейност следва винаги да се имат предвид, когато се решава дали да се изземат електронни устройства, които се използват за търговски цели.

Вещите носители на компютърни информационни данни, следва да се изземат и съхраняват по начин, с който да е невъзможно да се манипулират данните. Ако това не е направено и на експерта са предадени за анализ незапечатани носители или такива с нарушена запечатка, възниква съмнението, че данните може да са променяни след момента на изземане. Действията на експерта по извличане на данните и анализ следва също да се документират по начин, който да удостовери, че не са правени промени в хода на самото изследване.

Винаги, когато в хода на претърсване се заварят работещи електронни устройства, преди изземането им, следва да се запишат по указания начин данните, които са свързани с енергозависимата памет (RAM), които ще се унищожат при изгасяне на устройството. Ако електронните устройства са заварени изключени, те не се включват, защото това също може да доведе до загуба на данни или промени[30].

Възниква въпросът и как на практика ще се изпълни изискването на закона за разпечатване на данните на хартиен носител. В някои от случаите, това може да е невъзможно, защото самите данни са в голям обем или са със строго техническо естество. При всички случаи, разследващият орган следва да разполага с преносим принтер (което едва ли е така на практика) и на място да извърши разпечатване на данните с оглед подписване на разпечатаните листа от поемните лица. При това положение, считам, че е много по-удачно изискването за разпечатване на хартия на данните да не еабсолютно, а да може да се замени с изготвяне от страна на експерта на пълно дигитално копие на данните, които ще се изземат преди записване на електронния носител. Така ще са налице два независими един от друг носителя на данните и между тях може да се правят сравнения по спорните моменти (какъвто е смисълът на хартиеното копие). Носителите на които се записват данните следва да не съдържат никакви други стари данни, за да не се получи смесване на иззетите със стари електронни данни.

Засегнатите при претърсване лица следва да получават копие на иззетите данни, което да бъде записано по начин недопускащ промени. Така те ще имат възможност да оспорят всяка промяна в оригиналните носители, ако тя не е била налична към момента на изземане.

5. Дистанционно събиране на компютърни информационни данни, чрез прилагане на СРС под формата на електронно наблюдение/претърсване.

Чл. 172,ал.1 и ал.3 НПК допуска използване на СРС[31] под формата натайно наблюдение, проследяване, проникване (дистанционно), белязване (чрез проследяващи източника на сигнала програми) с обект компютърна информация, без да се налага физическо проникване в помещенията, където се намират съответните сървъри. При **тайното телекомуникационно наблюдение** се прихваща и записва в реално време трафика на компютърни данни[32] без знанието и разрешението на заинтересованите лица. Поради непълния достъп до информация, е възможно да се наложи извършване на **тайно дистанционно претърсване** на компютърна система, база данни или сайт, като скрито се проникне в системата и тайно от администратора се извлекат данни, които да се запишат на полицейски сървъри за последващ анализ.

---

[29] Например: юридическото лице в което работи извършителя.

[30] Вж.**Василев, Димитров**.Цит. съч., с.100–102.

[31] Относно общите положения при употребата на СРС виж: **Маринова, Г**. Особености на специалните разузнавателни средства, като способ на доказване в българския наказателен процес. – De jure, №2, 2021 (23), с. 269–276.

[32] Данните обичайно са в криптирана форма, поради което достъпът до тях е затруднен.

Възможността да се извършва тайно телекомуникационно наблюдение или тайно дистанционно претърсване на различни бази данни, интернет сайтове и др. и изземане на данни, следва да се уреди изрично, като се предвидят стриктни условия за прилагането на тези способи и гаранции срещу злоупотреби, каквато е европейската практика[33]. Поради скрития си и таен характер подобни действия не могат да се извършват по друг ред, освен като СРС. Доколко към момента нормите на чл. 5 и на чл. 8 от ЗСРС[34] са достатъчна законова основа за извършване на подобни тайни дистанционни дигитални наблюдения или прониквания ще се реши от практиката. Според мен, поради спецификата на тези действия в електронна среда следва да се предвиди изричен специален ред за провеждането им, включително и когато са налице подобни искания на чуждестранни власти по реда за ЕЗР[35]. Средствата, с които подобни СРС ще се прилагат следва да са законово регламентирани и обект на обществен контрол, за да не се стига до международни скандали за тайното използване на програми от типа на **софтуера Pegasus**[36].

Електронните доказателства са сложни за оценка, защото за правилното им анализиране са нужни специални знания. Обвинението или осъдителната присъда не следва да се базират само на електронни доказателства, които по своята природа се явяват лесни за манипулация или погрешна интерпретация.

6. Събиране на данни за трафика на електронна комуникация.

Информация за трафика на информационни данни за целите на наказателното производство се получава след съдебно разрешение по реда на чл. 159А от НПК. Данните за трафика може да бъдат установени и в хода на полицейска проверка по реда на чл. 251Г, вр. с чл. 251В от ЗЕС. Основният проблем при изискване на справка за трафика е свързан с краткия 6 месечен срок, в който може да се иска тази информация, съответно в който тя следва да се съхранява от оператора на данните. След изтичане на този срок, операторът на данните е задължен да ги унищожи, ако не е получил съдебно разрешение за достъп и преодставяне – чл. 251Ж, ал.1 ЗЕС. Поради мудното действие на полицията в голяма част от случаите 6 месечният срок[37] изтича и данните се унищожават автоматично, което прави практически невъзможно разкриването на повечето компютърни престъпления, за които тези данни са ключови. Въпрос на организация и инициативност е при всеки сигнал за компютърно престъпление първо да се подсигурят тези данни, защото в противен случай ще бъдат унищожени. Друг проблем е че и в двата режима за разкриване на данните се изисква предмет на разследване да е тежко престъпление, като повечето компютърни престъпления по глава 9А от НК не са тежки и

[33] Вж. чл.100а и 100в от Германския Наказателнопроцесуален закон.

[34] При проникването чрез използване на технически средства се установяват фактически данни, намиращи се в помещения, и вещи, ползвани от контролирани лица.

[35] Например: **казус ID 67235 (DE/BG)** на националното бюро на България в Евроджъст.

[36] Налице са множество оплаквания за незаконно проникване в мобилни телефони на шпионския софтуеър: Pegasus.Този продукт е уникален, защото за разлика от общите случаи на заложени в интернет компютърни шпионски софтуери, които са адресирани към неограничен кръг от хора и целят случайна кражба на данни, Pegasus се насочва към точно определени хора от специфични професии, боравещи с чувствителна информация (журналисти, активисти за правата на човека, опозиционни лидери) и **тайно** прониква в мобилното устройство, като дистанционно може да активира камерата, микрофона, GPS локатор и др. и пренасочва данните към избран сървър. Източник: **Forensic methodology report:** How to catch NSO Group’s Pegasus, Amnesty International, p. 33. (налично на : https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/)

[37] Срокът за съхранение на данните чл.16,ал.2 от Конвенцията за престъпления в киберпространството подписана в гр.Будапеща на 23.11.2001г., в сила за РБ от 01.08.2005 г. е до 90 дни. Това налага данните да са изискат експедитивно. След като максималният срок по конвенцията е около 3 месеца, националният по-дълъг срок от 6 месеца му противоречи и не следва да се прилага на основание чл. 5,ал.4 от Конституцията.

на практика не е възможно изобщо да се иска разкриване на данните.

В свое решение КС[38] е приел, че е налице е противоречие с Конституцията на разпоредбата на чл. 250а, ал. 2 ЗЕС, относно целта на съхраняването на данни от трафика, а именно за нуждите на разкриването и разследването на престъпления по чл. 319а – 319е от Наказателния кодекс (НК), както и за издирване на лица. Изключението по чл. 34, ал. 2 от Конституцията е допустимо само когато интервенцията в сферата на неприкосновеността на свободата и тайната на кореспонденцията и на другите съобщения се налага за разкриване и предотвратяване на тежки престъпления и то не може да бъде тълкувано и прилагано разширително. Следователно, разпоредбата в частта ѝ „и престъпления по чл. 319а – 319е от Наказателния кодекс“, които не са тежки по смисъла на чл. 93, т. 7 НК, с изключение само на това по чл. 319а, ал. 5 НК, доколкото предвидените в санкционните части на съответните норми на особената част на НК за тях наказания не са лишаване от свобода за повече от пет години, доживотен затвор или доживотен затвор без замяна, е противоконституционна.

Според мен, в случая КС неправилно приема, че конституционното разбиране за тежко престъпление е идентично с определението на тежко престъпление по смисъла на НК (чл. 93, т. 7 НК). Тези две понятия са различни. От конституционна гледна точка, тежко ще бъде всяко престъпление, което засяга конституционно гарантираните основни права, независимо от неговата наказуемост и разбиранията на наказателното право. По тази логика, компютърните престъпления по глава 9А НК са конституционно тежки, защото засягат основни права на човека-личният живот на гражданите (чл. 32 от Конституцията), свободата и тайната на кореспонденцията (чл. 34, ал. 1 от Конституцията), правото на собственост (чл. 17, ал. 1 от Конституцията) и др. Независимо от изложеното, единствения начин да изпълним въпросното решение на КС и едновременно с това да стане възможно разследване на компютърните престъпления по глава 9А НК е наказуемостта на всички тях да бъде завишена и те да станат тежки. Не е добро решение да се завишава наказуемост, само за да се преодолее процесуална пречка за събиране на трафични данни, но в тази ситуация е единствено възможното.

С решение на СЕС[39] се приема, че ЕЗР издадена по ДП от български прокурор за придобиване на трафични данни в друга държава членка на ЕС, противоречи на чл. 2, б. В, подточка i, от Директива 2014/41/ЕС[40], защото е неправомерно да се изпълнява заповед на прокурор, при положение, че за сходен национален случай разпореждането за достъп до трафичните данни е от изключителната компетентност на съдия. Това решение на СЕС налага да се приемат съответни промени в ЗЕЗР, които да предвидят съдебно потвърждаване на издадена от национален прокурор ЕЗР с предмет събиране на трафични данни, защото в противен случай разкриване на компютърни престъпления извършени от територията на държава членка на ЕС ще стане напълно невъзможно. Към момента няма как да се иска национално разрешение за достъп до трафични данни в чужбина, защото на чужда територия българския съд няма компетентност да разрешава каквото и да е.

7.Приобщаване и оценка на видеозаписи.

Множество обществени места и обекти[41], търговски помещения, болници, банкомати, банкови салони и др. са оборудвани

[38] Реш. № 2 от 12.03.2015 г. на КС по к. д. № 8/2014 г., обн. „Държавен вестник“, бр. 23/2015 г.

[39] Решение на четвърти състав от 16.12.2021г. по дело С-724/19г., с предмет преюдициално запитване на българския Специализиран наказателен съд.

[40] ДИРЕКТИВА 2014/41/ЕС НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА от 3 април 2014 годинаотносно Европейска заповед за разследване по наказателноправни въпроси.

[41] Например: От 2007 г. до 2016 г., включително, системата за видеонаблюдение на Столична община обхваща над 220 училища и детски заведения и над 130 публични площи общинска собственост, в това число пешеходни зони, подлези, градски градини, паркове, гробищни паркове, паметници, уязвими точки от инфраструктурата на Столична община и др. Изградени са и 4 локални центъра за видеонаблюдение. За осигуряване на нормалното функциониране на системата за видеонаблюдение в обектите общинска собственост и на своевременна реакция на сигналите, генерирани от системата, се води дежур-

със системи за видеонаблюдение, които могат случайно да запишат поведението на лице извършило престъпление.

Съгласно легалната дефиниция на пар.1, т. 3 от ЗЧОД[42] „Видеонаблюдение“ е техническа форма на обработка и съхранение в предвидения в закона срок[43] на лични данни, извършвани при спазване на изискванията за защита на личните данни и на разпоредбите и на този закон, свързани с изискванията при обработката на лични данни, включваща заснемане на лица в охраняван обект и запис на получените данни. Тези записи могат да послужат като доказателство в наказателното производство, но ползването им поставя някои въпроси.

Най-важният от тях е свързан с това какво е значението за наказателния процес на това дали записът е направен законно, т.е. според изискванията на различни специални закони, които уреждат възможността да се записват лица, независимо от тяхното съгласие или въпреки тяхното несъгласие?Според чл. 32, ал. 2 от Конституцията, никой не може да бъде фотографиран, филмиран или записван, без негово знание или въпреки неговото изрично несъгласие, освен в предвидените в закона случаи. Непосредственото действие на Конституцията налага извода, че подобен запис може да се ползва в наказателния процес, само ако е направен в съответствие със съответния специален закон, допускащ изключение от посочената принципна забрана за заснемане[44].

Във всички случаи следва да се прецени законността на видеозаснемането и в контекста на защита на личните данни. Позицията на Комисията за защита на личните данни[45] по въпроса за законността за видеозаснемането от гледна точка на защита на личните данни, които са събрани с този запис е да приеме заснемането за непротиворечащо на закона, при определени условия. Обработката на лични данни, чрез видеозаснемане не винаги може да се счете за необходимо и за да е допустимо, много внимателно следва да се направи преценка за баланса на интересите на администратора и на заснемани и записвани субекти. Освен това е нужно, да се преценява, доколко адекватни и пропорционални са целите, за които се събират тези данни и дали тези цели не могат да се постигнат по друг начин. Видно от изложените критерии всеки случай трябва да се изследва самостоятелно,- за да се прецени дали видеозаснемането е законно от гледна точка на защита на личните данни. Ако видеозаснемането се приеме за незаконно[46], то по силата на чл. 32, ал .2 от Конституцията то не може да се използва в наказателния процес, защото засяга конституционно установеното право и не е налице визираното в Конституцията изключение. Това означава, че преди да разгледаме записа като доказателство, следва да се произнесем дали не е направен в нарушение на закона, което би го направило недопустим в наказателния процес. Недопустимостта на запис направен в нарушение на някой от специалните закони не е уредена в НПК, но следва от приложението на посочената норма на Конституцията. В практиката този въпрос понякога се игнорира и не се проверява задълбочено, до колко из-

---

ство 24 часа в денонощието, 7 дни в седмицата, в ОДЦВ на Столична община. Изградена е отделна оптична линия за пренос на информация между Оперативния дежурен център и видеонаблюдение (ОДЦВ) на Столична община и Оперативния център за видеонаблюдение на Столична дирекция на вътрешните работи (СДВР). Двете системи са напълно съвместими, което е важна предпоставка за повишаване ефекта от дейността на общинската система за видеонаблюдение и осигуряване на бърза и адекватна реакция от компетентните полицейски органи. Източник: https://www.sofia.bg/closed-circuit-television.

[42] ЗАКОН за частната охранителна дейност, обн., ДВ, бр. 10 от 30.01.2018 г., в сила от 31.03.2018 г.,

[43] Според чл. 56, ал. 4 ЗЧОД Записите от техническите средства за видеонаблюдение се съхраняват в регистър „Видеонаблюдение“ два месеца след изготвянето им. Унищожаването им се удостоверява от ръководителя на охранителната дейност.

[44] Специалните закони уреждащи видеозапис на публични места са: чл.165, ал. 2, т. 7 от ЗДП; чл. 16 от ЗООРПСМ; ЗСРС; чл. 30 от ЗЧОД и Наредба I-171/2001г. на МВР и БНБ.

[45] Виж: Становище № П-272 от 16.10.2014 г. на КЗЛД

[46] Видеозаснемането е в нарушение на нормата на някой специален закон, например: поставена е камера в общите части на етажна собственост, без съответно решение на Общото събрание.

общо е било законно да се монтират камери и да е извършва видеозаснемане, което представлява грубо игнориране на нормата на чл. 32, ал. 2 от Конституцията, която по принцип забранява такова поведение, освен за случите и начините, които са изрично разрешени в закон.

Извършването на инцидентен запис с мобилен телефон и друго записващо устройство се отличава от посочения по-горе метод на регулярно видеозаснемане, защото цели да документира конкретна ситуация свързана с лицето изготвящо записа, с оглед защита на негови права. Тази дейност не е законово уредена по принцип, но изразява конституционно прогласената в чл. 41 от Конституцията свобода за търсене, получаване и разпространяване на информация. Поради това, подобни записи не могат да се приемат за незаконни, освен ако с тях не се нарушава норма на специален закон[47].

Най-трудна е преценката за законност на тайно направени видео и аудио записи от разследващи журналисти, с използване на скрити камери и микрофони. Тези записи на практика се доближават до СРС поради тайния с характер и цел: разкриване и документиране на престъпление. Възможността журналисти да използват подобни методи следва да се уреди в закон, защото иначе е налице незаконно СРС[48] и подобно поведение, макар да е ръководено от високи морални подбуди, може да се разгледа като престъпление по чл. 145А, ал.1 НК. Липсата на законова уредба към момента на подобни журналистически разследвания, води до това, че законността на подобни тайни записи е много съмнителна и употребата на тези записи в наказателното производство може да се изопачи. Вместо те да се ползват като доказателство за извършено престъпление или конфликт на интереси, те могат да се превърнат в доказателство срещу техните автори за незаконно прилагане на СРС и основание за предявяване на деликтен иск[49]. При липсата на законова уредба на журналистическо разследване проведено с таен запис на поведение на набелязаното лице, единственият начин на защита на журналиста е, да се позове на института на крайната необходимост (чл.13 от НК), упражнена в защита на държавен (разкриване на престъпление) или обществен интерес (осигуряване на обществен достъп до информация). За да избегне наказателна отговорност за незаконно прилагане на СРС разследващият журналист следва да докаже, че е била налице непосредствена опасност от извършване на престъпление и че причинените от деянието вреди са по-малко значителни от предотвратените. Слабият момент в подобна защита е свързан с обстоятелството, че воден от професионална амбиция, разследващият журналист сам провежда свое разследване, а не уведомява компетентните държавни органи, което обстоятелство прави института на крайната необходимост трудно приложим. Поради това, докато подобни журналистически разследвания не получат законова регламентация[50], преценката дали са законни или не остава мъглява и неясна, а това се отразява на статута на направения видеозапис.

Ако забраната на чл. 32, ал. 2 от Конституцията е преодоляна в съответствие със закона и записът е допустим, то възможни са следните начини за законно приобщаване на записи от видеонаблюдение:

а) доброволно предаване

[47] Например: запис в съдебна зала от лице от публиката или страна, без изрично разрешение на председателя на състава нарушава нормата на чл. 266 НПК.

[48] Под СРС (чл.2 от ЗСРС) се разбира както техническите средства (миниатюрни камери/скрити микрофони) така и оперативните способи за прилагането им-наблюдение и заснемане.

[49] Решение № 56 от 26.02.2009 г. на ВКС по гр. д. № 5814/2007 г., I г. о., ГК.

[50] Законовата регламентация е нужна както за гарантиране свободата на журналиста да провежда разследване, резултатите от което да документира със видео или аудио запис, така е нужно да се гарантират и правата на разследваното лице, че няма да бъде обект на провокация или манипулация, с цел добиване на сензационен материал. Нормата на чл. 16, ал. 1 от ЗРТ (Доставчиците на медийни услуги зачитат правото на личен живот и спазват законодателството за защита на личните данни на гражданите, като вземат предвид баланса между правото на личен живот и правото на свобода на изразяването и информацията) е прекалено обща, касае само някои електронни медии и не разрешава проблема с тайното заснемане.

Записът се прехвърля на материален носител от съответния служител и се прилага в хода на разследването по реда на чл.159,ал.1 НПК обичайно с протокол за доброволно предаване[51] или като приложение към протокол за разпит на свидетел.

б) принудително изземане

При отказ да се предостави записа доброволно, същият се иззема принудително с претърсване и изземане. Важно е да се съобрази, че повечето системи за запис на видеонаблюдение са автоматично програмирани за изтриване на записа в по-кратък от законния срок, обичайно един месец, което налага спешно да се поиска запазване на записа за периода, който е предмет на разследване.

Записи от видеонаблюдение, които са приложени фактически по делото, без да е установен техния източник по посочения по-горе ред, не могат да се ползват като доказателство, защото са с неясен произход и това внася непреодолими съмнения за тяхната относимост и възможна манипулируемост, за която няма лице-депозант, което да носи отговорност.

Правилната оценка на записа от видеонаблюдение е от съществено значение, защото в много случаи това е единственото доказателство срещу извършителя[52]. Оценката на доказателствената стойност на запис от видеонаблюдение не може да бъде еднозначна, а зависи от неговото качество и възможността да се идентифицира самоличността на записаното лице по категоричен начин. Годността на записа следва да се преценява самостоятелно и отделно от годността на сравнителния материал за изследване, който ако е негоден или частично годен, следва да се изземе нов, което не е възможно за самия запис. Техническата преценка на годността на записа се прави от вещо лице в рамките на техническа експертиза, защото за нея се изискват специални знания и оборудване.

Възможни са следните варианти на оценка на самия запис:

а. Записът е негоден за идентификация.

Поради лошо качество на самия запис (ниска резолюция), лош ъгъл на заснемане, лоша осветеност или маскиране на извършителя същият не може да бъде идентифициран. Такъв запис е едно косвено доказателство с минимална стойност, защото само потвърждава извършеното престъпление, но няма никаква доказателствено значение за установяване на неговия автор.

б. Записът е частично годен и идентификацията е със степен на вероятност.

В тази ситуация, поради различни дефекти на записа, възможността за идентификация е частична. В тази ситуация, записът представлява косвено доказателство, като за правилната му оценка следва много внимателно да се анализира заключението на вещото лице, което използва различни думи за да означи степента на съвпадение на записаното лице с конкретна личност. Думите: „възможно“, „вероятно“ или „сигурно[53]“ показват различни степени на вероятност и поради това подобен запис винаги е косвено доказателство.

в. Записът е напълно годен и идентификацията е категорична.

В тази ситуация записът е напълно годен, а при идентификация на лицето, вещото лице използва думата категорично, поради което записът е пряко доказателство. Много е важно правилно да се разчете заключението на вещото лице, което не следва да има никакви съмнения при идентификация на лицето, защото всяко негово колебание води до загуба на категоричност. Дори най-малкото съмнение или колебание на вещото лице при идентификация на извършителя или годността на

[51] НПК не урежда доброволното предаване като отделен способ за доказване (поради това не са нужни поемни лица), но за него задължително следва да се състави протокол, в който да се отразят изявленията на предаващото лице. В този смисъл виж: Решение № 362 от 21.01.2011 г. на ВКС по н. д. № 334/2010 г., III н. о., НК.

[52] Например: престъпление по чл. 249, ал. 1 НК свързано с незаконно ползване на чужда банкова карта на банкомат.

[53] За повечето вещи лица сигурно не е синоним на категорично, а най-високата степен на вероятност.

записа, води до различна оценка на записа, а ако това е единственото пряко доказателство при трансформацията му в косвено, изискванията за доказване на обвинението и постановяване на осъдителна присъда с косвени доказателства са напълно различни от тези с преки доказателства. Идентификацията на човека обикновено е лицева, защото лицето съдържа множество специфични белези, но е възможна категорична идентификация и по други признаци: очен ирис, специфична татуировка или малформация.

Категорично може да се каже, че априорното отхвърляне на тези записи, като негодни, с мотив, че не са изготвени по реда на НПК е неправилно и незаконосъобразно. Всички следи от извършеното престъпление (в случая електронни данни) могат да бъдат доказателство в процеса – чл.104 НПК. Освен това, те не могат да бъдат изготвени по реда на НПК, защото към момента на създаването им не е имало разследване, защото те са отразили непосредствено самото престъпление в процеса на извършване, а разследването винаги започва в последствие.

Заключение

Електронните доказателства имат своя уникална природа, която налага да се отнасяме към тях по нов начин, различен от отношението към другите доказателства, с които сме свикнали да боравим и оценяваме. Събирането и оценката на електронните доказателства налага използването на нови подходи, като киберразследващите следва да са не само юридически грамотни, но и компютърно грамотни и да са обезпечени с нужната техника и софтуеър. Липсата на специализирано киберразследване и на специални методи за събиране и оценка на електронните доказателства води до практическа невъзможност да се разкрият и докажат извършените в електронна среда престъпления. Колкото по-рано осъзнаем, че сме изправени пред напълно нов феномен в областта на наказателния процес, толкова по-бързо ще вземем нужните адекватни мерки за провеждане на професионално и ефективно разследване на престъпленията извършени в електронна среда и събирането на годни и достатъчни електронни доказателства.

БИБЛИОГРАФИЯ / REFERENCES

Сарановъ, Н. Българско наказателно-процесуално право. С.: Печатница „Художник“, 1937, т. 2.

Павлов, С. Наказателен процес на НРБ. С.: НИ, 1959.

Чинова, М. Досъдебното производство по НПК. С.: Сиела,2013г.

Захариев, Ганчевски и др. Разкриване и разследване на компютърни престъпления. (практическо ръководство). С.: Сиби, 2006.

Маринова, Г. Електронните доказателства. – Правна мисъл, № 3, 2002.

Маринова, Г. Особености на специалните разузнавателни средства, като способ на доказване в българския наказателен процес. –DE JURE, № 2/2021 (23).

Василев, Димитров. Методика за разследване на киберпрестъпления. Електронни подписи-същност и правни проблеми. НСлС, София, 2015.

Доклади за прилагането на закона и за дейността на прокуратурата и на разследващите органи през 2020; 2019; 2018; 2017.