ИЗПОЛЗВАНЕ НА ЦИФРОВИ ДОКАЗАТЕЛСТВА ПРИ РАЗСЛЕДВАНЕ НА КИБЕРПРЕСТЪПЛЕНИЯ

Доц. д. н. Драгомир Кръстев
Висше училище по телекомуникации и пощи

INVESTIGATION OF CYBERCRIME THROUGH DIGITAL EVIDENCES

Assoc. Prof. DSc. Dragomir Krastev
University of telecommunications and posts

Резюме: В доклада се разгледани същността и формите на използване на цифрови доказателства при разследването и разкриването на киберпрестъпления. Анализирани са специфичните свойства на цифровите доказателства и особеностите при тяхното събиране. Отделено е внимание и на някои методологии, с които си служи дигиталната криминалистика.

Ключови думи: *киберсигурност, киберпрестъпления, цифрови доказателства, разследване*

Abstract: The manuscript examines the nature and forms of the use of digital evidence in the investigation and detection of cybercrime. The specific properties of digital evidence and the peculiarities of their collection are analyzed. Attention is also paid to some methodologies used by digital forensics.

Key words: *cybersecurity, cybercrime, digital evidence, investigation*

Doi: https://doi.org/10.36997/LBCS2021.332

Въведение

Цифровите доказателства оказват влияние във всеки аспект на правото, включително договорно, трудово, семейно, наказателно, право на интелектуалната собственост и т.н. В крайна сметка няма сфера на правото, която да не е включена и цифровите доказателства придобиват все по-голяма значимост с повсеместното използване на глобалната мрежа – интернет. Очевидно е, че престъпниците и терористите използват дигиталната среда за кражби, изнудване и злоупотреба с малолетни в международен мащаб.

Изложение

Разследването на киберпрестъпления представлява процесът на събиране, анализ, съхраняване и унищожаване на доказателства при инцидент, представляващ заплаха за киберсигурността по начин, който е съобразен с действащите правни актове и може да бъде възприет като годно доказателство в съда.

Наказателно-процесуалният кодекс (НПК) в чл. 104 определя доказателствата като факти на обективната действителност. Във връзка с възприетата легална дефиниция доктрината възприема няколко общи постановки за фактите, които ще послужат като доказателство. Те трябва да бъдат индивидуализирани по време и място, като могат да бъдат предмети, вещи, книжа, документи, действия и бездействия, състояние на човешката психика или вътрешен мир без значение дали са минали, дали са настоящи, постоянни, временни, нововъзникнали или новосъздадени. За да бъдат взети предвид при разкриването на обективната истина, те следва да бъдат приложени към делото или да са възпроизведени по предвидения в закона начин, ако техният размер и естество не позволяват това. Доказателствата следва да се разграничават от доказателствените средства – чл. 105 от НПК предвижда, че доказателствените средства служат за възпроизвеждане в наказателното производство на доказателства или други доказателствени средства. Макар че са предвидени в НПК, заедно с реда за тяхното изготвяне съществуват доказателствени средства, чийто ред за изготвяне не е предвиден в процесуалния закон[1].

Благодарение на технологичния напредък в събирането и обработката на информация, в днешно време правоохранителните органи и специалните служби са в състояние да събират доказателства в хода на разследване чрез много по-ефективни начини, немислими до преди няколко години. Въпреки това действащото приложимо законодателство в много европейски страни е прието преди появата на тези технологии и съответно не взема предвид тези технологични възможности. В резултат на това възникват три много важни проблема:

(1) при допускането от съда на доказателства, извлечени с електронни средства, съществува елемент на несигурност предвид това, че съдиите нямат ясни критерии за тяхната допустимост и степен на

[1] https://www.netlaw.bg/bg/a/mobilnite-ustroistva-v-svetlinata-na-nakazatelniya-proces-i-praktikata-na-evropeiskiya-sd-po-pravata-na-coveka, 20.10.2021.

достоверност, поради което се стига до нееднакво прилагане на закона, което е недопустимо;

(2) новите технологии могат бързо да се окажат неефективни, след като престъпни организации и/или лица се запознаят с тяхното съществуване и техническите им спецификации и възприемат контрамерки по осуетяване на приложението им;

(3) глобализацията на престъпността изисква пряко сътрудничество между правоохранителните и правораздавателните системи в различни страни: доказателствата, събрани в една държава, трябва да бъдат използваеми и допустими в други страни, като едновременно се спазват основните права и процедурни гаранции, което е предизвикателство с немалка сложност поради липсата на законодателство и стандарти на национално и международно ниво в тази материя[2].

В своята работа експертите си служат със сложен комплекс от правни и етични съображения, когато обработват, анализират и тълкуват цифрови доказателства и когато докладват резултати при разследване на киберпрестъпления (Seigfried-Spellar, K., M. Rogers, D. M. Crimmins 2017: 135-144).

Трябва да се има предвид, че юридическите задължения съществуват като предписания в националното и международното право, докато етичните задължения са доброволно възприети или наложени от държавни институции или частни организации (Sharevski, F. 2015: 39-54).

Към днешна дата няма налични общовалидни процедури за разследване на киберпрестъпления. Всяка държава използва собствени протоколи за разследване. Съществуват обаче някои международни стандарти и добри практики, които могат да бъдат възприети от държавите за разследване на киберпрестъпления.

През последните две десетилетия са разработени различни методологии, които ползва цифровата криминалистика.

Така например през 2002 г. е предложен модел за цифрова криминалистика, базиран на опита на ФБР, наречен: *„Абстрактен модел на цифрова криминалистика“*. Именно този модел се използва най-често в практиката. Той се състои от девет стъпки:

1. Идентификация;

2. Събиране на цифрови доказателства;

---

[2] http://www.libreresearchgroup.org/bg/a/e-justice, 20.10.2021.

3. Получаване на цифрови доказателства;

4. Запазване на цифрови доказателства;

5. Анализ и отчитане;

6. Допустимост на цифрови доказателства;

7. Оценка на цифрови доказателства;

8. Разглеждане на цифрови доказателства и

9. Вземане на решение относно допустимостта на цифрови доказателства.

Цифровите доказателства са крехки и краткотрайни и неправилното боравене с тях може да доведе до изменението им по редица параметри. Поради нестабилността на доказателствата трябва да се следват определени протоколи, за да се гарантира, че данните няма да се променят, докато се обработват. Тези протоколи описват стъпките, които трябва да се предприемат при работа с цифрови доказателства.

Цифровите доказателства създават уникални предизвикателства в процеса на удостоверяването им. Към тях спадат:

- количеството налични данни,

- тяхната скорост (т.е. скоростта, с която са създадени и предадени),

- нестабилност (т.е. те могат бързо да изчезнат, когато бъдат презаписани или изтрити) и

- уязвимост (т.е. те могат лесно да бъдат обработвани, променяни или повредени).

Докато някои държави са въвели правила за доказване, които включват изисквания за удостоверяване, които конкретно се отнасят до цифровите доказателства, други страни използват подобни изисквания за удостоверяване на традиционни доказателства и цифрови такива. Във Франция например както хартиените, така и електронните документи трябва да бъдат удостоверени чрез проверка на самоличността на създателя на документите и целостта на документите (Bazin 2008).

На практика цифровите доказателства обикновено се разглеждат като информация, която се генерира, съхранява и предава чрез използването на електронно оборудване и която може да констатира наличието или липсата на престъпление, да идентифицира лицето, извършило такова престъпление, както и да определи обстоятелствата за разрешаването на даден случай.

Това обхваща информация от регистрите, хронология на интер-

нет трафика, данни от съдържанието, изображения, IP адреси, имейли, електронни документи, цифрови видеофайлове, аудиофайлове и изображения, бази данни, данни от електронни таблици, бисквитки, изходни печатащи устройства, електронно счетоводство, геолокационни данни от GPS, архиви на извършени банкови операции и др.

Събирането, анализът и използването на цифрови доказателства в наказателното производство могат да бъдат от значение не само при престъпления срещу компютри и извършени чрез компютри, но и във връзка с други престъпления, които могат да включват цифрови доказателства.

Ако цифровите доказателства са в интернет или са собственост на доставчици на електронни услуги, от съществено значение е да се осигури сътрудничество с доставчиците на услуги на информационното общество или доставчиците на електронни съобщителни услуги, за да се предоставят необходимите данни и да се предприемат мерки срещу унищожаването и модифицирането на данните.

В контекста на дигиталната криминалистика хората оставят дигитални отпечатъци след използване на информационни и комуникационни технологии (ИКТ) (Antwi-Boasiako, Venter 2017). Поспециално, потребителят на ИКТ може да остави цифрови пръстови отпечатъци, т.е. данни, оставени от потребители на ИКТ, които могат да разкрият информация за тях, включително информация за възраст, пол, раса и етническа принадлежност, гражданство, сексуална ориентация, мисли, предпочитания, навици, хобита, медицинска история и здравословни проблеми, психологически разстройства, трудов статус, принадлежност към която и да е общност, връзка, геолокация, ежедневие и други дейности. Такива цифрови пръстови отпечатъци могат да бъдат активни или пасивни.

Активен цифров пръстов отпечатък се създава от предоставени от потребителя данни, като лична информация, видеоклипове, изображения и коментари, публикувани в приложения, уебсайтове, табла за съобщения, социални мрежи и други онлайн форуми.

Пасивните цифрови пръстови отпечатъци са данни, които хората, които използват интернет и цифровите технологии, по невнимание оставят след себе си (например преглеждане на историята в браузър). Данните, които са част от активни и пасивни цифрови пръстови отпечатъци, могат да се използват като доказателство за престъпление, включително киберпрестъпление (т.е. като цифрови доказателства).

Такива данни могат да се използват и за:

• доказване или опровергаване на констатиран факт;

• потвърждаване или опровергаване на показанията на пострадалия, свидетеля и заподозрения;

• и/или определяне на участието или неучастието на заподозрения в престъплението.

Данните се съхраняват в цифрови устройства (например компютри, смартфони, таблети, телефони, принтери, смарт телевизори и всякакви други устройства, които имат цифрова памет), външни устройства за съхранение (например външни твърди дискове и USB флаш устройства – устройства за съхранение), мрежови компоненти и устройства (напр. маршрутизатори), сървъри и съхранение в облак. Извлечените данни могат да бъдат свързани със съдържание (т.е. думи в писмени съобщения или изговорени думи в аудио файлове; например видеоклипове, текст на имейли, текстови съобщения, незабавни съобщения и съдържание в социалните медии) и несвързани данни, съдържание или метаданни (т.е. данни за съдържанието; например самоличността и местоположението на потребителите и данните за транзакциите, като информация за изпращачи и получатели на телекомуникации и електронни съобщения). Данните, получени онлайн и/или извлечени от цифрови устройства, могат да съдържат голямо количество информация за потребители и събития. Например конзолите за компютърни игри, които действат като лични компютри, съхраняват:

• лична информация за потребителите на устройства (например имена и имейл адреси);

• финансова информация (например информация за кредитни карти);

• информация за историята на сърфирането в интернет (например посетени уебсайтове);

• изображения, видеоклипове и други данни.

Данните, извлечени от игровите конзоли, се използват за разследване на случаи на сексуална експлоатация на деца и онлайн материали за сексуално насилие над деца. Друго цифрово устройство, което натрупва значително количество данни за своите потребители, е Amazon Echo (с гласов асистент Alexa). Данните, събрани от това устройство, могат да съдържат ценна информация за потребители/собственици, като информация за техните интереси, предпочитания,

запитвания, покупки и други дейности, както и тяхното местоположение (за да се определи например дали са вкъщи или извън дома чрез преглед на датчика за време и аудиозаписи на взаимодействия с гласовия асистент Alexa). Данните, извлечени от Amazon Echo, са използвани в САЩ при разследване на убийство. Въпреки че обвиненията срещу заподозрения в крайна сметка са свалени, този случай ясно показа, че данните, събрани с помощта на новите цифрови технологии, неизбежно ще бъдат представени в съда като доказателство (Maras, Wandt 2018). Данните могат да се добиват и използват за генериране на разузнавателна информация и може да бъдат представени в съда като цифрови доказателства. В последния случай цифровите доказателства могат да служат като преки доказателства чрез *„установяване на факта“* или косвени доказателства чрез *„извеждане на истинността на даден факт“* (Maras 2014: 40-41).

Важно е да се отбележи, че правилата за доказателствата са приложими в еднаква степен за цифровите доказателства и за материалните доказателства, получени от други източници. Винаги на отговарящото за конкретния случай длъжностно лице се пада отговорността да гарантира спазването на законите, по-конкретно, че използваните процедури за изземване на имущество се изпълняват в съответствие с действащото законодателство.

Операционните системи и другите програми често променят или добавят данни към съдържанието на дигиталните носители на информация. Това може да се случи автоматично, без непременно потребителят да разбере, че данните са променяни.

Изключително важно е в съда доказателствата да бъдат изложени в тяхната последователност и цялост. Също така е необходимо да се покаже как доказателствата са били записани, като се демонстрира процесът, чрез който те са придобити. Доказателствата следва да бъдат запазени до такава степен, че трето лице да може да повтори същия процес и да получи същия резултат като този, представен пред съда.

Заключение

Нормативната база, която регламентира статута на каквито и да е било електронни устройства, имащи качество като доказателствен материал в наказателния процес, е слабо уредена у нас. Необходимо

е да се вземе предвид практиката на органите на досъдебното производство и тази на съда, за да се уеднакви разбирането какъв е характерът на цифровите доказателства в българското наказателнопроцесуално право.

Липсата на граници в киберпространството поражда особени предизвикателства за правоприлагащите и съдебните органи. Цифровите доказателства, които днес са от решаващо значение за разследванията и съдебните органи, могат за секунди да се съхранят, променят и заличат от всяка точка на земята.

Специалистите, които разследват киберпрестъпления, трябва да се придържат към националните политики и насоките за най-добри практики, за да гарантират допустимостта на цифровите доказателства в съдилищата. Тези принципи включват техническите и правните изисквания, които трябва да бъдат изпълнени, за да се гарантира допустимостта на доказателствата. В допълнение към тези изисквания, хармонизирането на практиките за разследване на киберпрестъпления и цифрова криминалистика в различните държави е от съществено значение за разследвания, които често пъти включват множество юрисдикции.

Използвана литература

1. Antwi-Boasiako, A., Venter, H. (2017). A Model for Digital Evidence Admissibility Assessment. // Peterson, G., Shenoi, S. (eds.). Advances in Digital Forensics.

2. Bazin, P. (2008). An Outline of the French Law on Digital Evidence. // Digital Evidence and Electronic Signature Law Review, Vol. 5, pp. 179-182.

3. Maras, M-H. (2014). Computer Forensics: Cybercriminals, Laws, and Evidence. Jones and Bartlett, pp. 40-41

4. Maras, M-H, Wandt, A. (2018). IoT Data Collection and Analytics. Presentation for FBI, DHS, and Secret Service agents and members of the National Cyber-Forensics & Training Alliance, at John Jay College of Criminal Justice, City University of New York (2 May 2018).

5. Seigfried-Spellar, K., Rogers, M., Crimmins, D. M. (2017). Development of A Professional Code of Ethics in Digital Forensics. // Annual ADFSL Conference on Digital Forensics, Security and Law, pp.135-144.

6. Sharevski, F. (2015). Rules of professional responsibility in digital forensics: A comparative analysis. // Journal of Digital Forensics, Security and Law, Vol. 10(2), pp. 39-54.

7. http://www.libreresearchgroup.org/bg/a/e-justice, 20.10.2021.

8. https://www.netlaw.bg/bg/a/mobilnite-ustroistva-v-svetlinata-na-nakazatelniya-proces-i-praktikata-na-evropeiskiya-sd-po-pravata-na-coveka, 20.10.2021.

За контакти: доц. д. н. Драгомир Кръстев
Висше училище по телекомуникации и пощи
drago.krastev@gmail.com