DOI: 10.38146/BSZ.2016.11.5

SORBÁN KINGA

A digitális bizonyíték a büntetőeljárásban

„A mai modern világban nehéz elképzelni olyan bűncselekményt, amelynek nincs digitális dimenziója” – írja *Eoghan Casey.*[1] A technológia manapság annyira mélyen áthatja az életünket, hogy észre sem vesszük azt, annak egy részét egy teljesen virtuális környezetben töltjük. Manapság a fejlett országokban már kevés olyan ember él, aki nincs jelen valamilyen közösségi oldalon, vagy nem használ e-mailt. Internetes felületeken kommunikálunk az ismerőseinkkel, munkatársainkkal, sőt bizonyos ügycsoportok tekintetében már a hatóságok sem kívánnak személyes jelenlétet az ügyintézésnél. Számítógépen rendelhetünk ebédet, intézhetjük a banki ügyeinket. A mobileszközök robbanásszerű használatának elterjedésével folyamatosan a zsebünkben van egy miniatűr számítógép, amely mindig tudja, merre járunk éppen. Egy ilyen világban mindenki óhatatlanul digitális nyomok tömegét hagyja maga után, amelyek egy bűncselekmény felderítése vagy nyomozása során akár bizonyíték szintjére is emelkedhetnek. Vannak olyan bűncselekmények, amelyeket kizárólag számítógép felhasználásával, vagy információs rendszer, illetve adat sérelmére lehet elkövetni (tipikusan ilyenek az információs rendszer és adatok elleni bűncselekmények), de emellett figyelmet kell fordítani arra is, hogy manapság a hagyományos bűncselekmények többségének is van valamilyen digitális oldala (például az elkövetők e-mailben beszélik meg a cselekmény elkövetésének részleteit, a zaklató egy közösségi oldalon keresztül igyekszik kapcsolatot teremteni a sértettel stb.). A XXI. században nem számít kirívónak az amerikai *Robert Durall* ügye[2], aki – a böngészője keresési előzményei alapján –, mielőtt megölte a feleségét, olyan kifejezésekre keresett rá, mint „fojtogatás”, „emberölés”, „házastárs + gyilkosság”, „altató + tabletták + halál”. Ezeket a keresési kulcsszavakat a bíróságon arra használták, hogy bizonyítsák velük az előre kiterveltséget.

Az angolszász jog régóta bizonyítási eszköznek tekinti az elektronikusan tárolt információt *(electronically stored information; ESI)* és ismerik az úgynevezett „digitális vagy elektronikus” bizonyíték fogalmát is. A magyar jogban az

1 Eoghan Casey: Digital Evidence and Computer Crime. 3rd edition. Academic Press, 2011, p. 3.

2 Nancy Bartley: A trial of tangled webs. The Seattle Times, May 8, 2000. http://community.seattletimes.nwsource.com/archive/?date=20000508&slug=4019710

elektronikusan tárolt adatok helyzete annak ellenére bizonytalan, hogy a jogirodalomban egyre gyakrabban találkozhatunk ezzel a fogalommal. Mivel az információtechnológia fejlődésének vívmányai a magyar bűnelkövetőket sem kerülték el, hazánkban is egyre sűrűbben fordulnak elő olyan esetek, amelyekben az elkövetett bűncselekménynek technológiai vetülete van. A büntetőeljárásról szóló törvény (Be.) rendelkezéseit vizsgálva megállapítható, hogy az adat és annak hordozója nem feltétlenül alkot szoros és elválaszthatatlan egységet, nem tisztázott viszont annak a kérdése, hogy mely esetekben lehet vagy kell külön kezelni az adatot és az azt tároló információtechnológiai eszközt. A digitális bizonyítékok jogi aspektusaival foglalkozó tudományos munkák száma meglehetősen csekély, noha nagy szükség lenne arra, hogy az elektronikusan tárolt adatok eljárásjogi szerepe és rendszertani elhelyezése tisztázott és egyértelmű legyen.

Jelen tanulmányom arra keresi a választ, szükséges-e, hogy az elektronikusan tárolt információ önálló bizonyítási eszközként jelenjen meg a magyar büntetőeljárásban. Gyakorlati problémákon keresztül demonstrálom, hogy a büntetőeljárás során milyen nehézségeket vethetnek fel a digitálisan tárolt adatok, illetve milyen következményekkel járhat azok nem megfelelő kezelése, összegyűjtése. Ahhoz, hogy bemutatható legyen az elektronikusan tárolt információk jelentősége, mindenképpen célszerűnek tartom az olyan alapfogalmak tisztázását, mint a digitális bizonyíték, illetve a digitális bizonyítási eszköz. A fogalommeghatározásokon túl a tanulmány bemutatja a bizonyítás hatályos magyar szabályait, különös tekintettel a Be. bizonyításról, valamint kényszerintézkedésekről szóló rendelkezéseire. Mivel az elektronikusan tárolt információ, mint bizonyítási eszköz, angolszász jogterületről származik, indokoltnak tartom bemutatni a témában keletkezett, főként az Egyesült Államokból származó külföldi szakirodalmat.

A digitális bizonyíték fogalma és forrása

A bizonyítás sajátos megismerési folyamat, amelynek célja a múltban történt események lehető legpontosabb feltárása. E megismerés folyamán az eljáró hatóság bizonyítékokat gyűjt, amelyek olyan adatok, amelyek büntetőjogilag releváns tényekre vonatkoznak, és amelyeket a törvény által megengedett forrásokból (bizonyítási eszközökből) szereztek be. A bizonyítási eszköz tehát a bizonyíték hordozója, a bizonyíték pedig az az információ, amelyhez a bizonyítási eszközből jutunk. A leggyakrabban elhangzó példa ennek szemléltetésére a tanú vallomása: ez esetben a tanúvallomás a bizonyítási eszköz, az informá-

ció pedig, amelyet a hatóság a vallomásból szerez, a bizonyíték. Nem ennyire egyértelmű a helyzet azonban információtechnológiai környezetben. Mivel manapság a legtöbb bűncselekménynek van valamilyen technológiai vetülete, a hatóságok a nyomozás során gyakran találkoznak olyan bizonyítékokkal, amelyeket információtechnológiai eszköz hordoz, ez az úgynevezett digitális bizonyíték. Először a digitális bizonyítékokkal foglalkozó tudományos társaság *(Scientific Working Group on Digital Evidence)* tett kísérletet a digitális bizonyíték fogalmának meghatározására 1998-ban. A társaság a következő definíciót alkotta: *„Bizonyító erejű információk, amelyeket bináris formában tároltak, vagy továbbítottak."*[3] E meghatározás egyik fő problémája, hogy csak a bináris formában tárolt információkat tekinti digitális bizonyítéknak, amely kétségkívül az egyik legnépszerűbb ugyan, de korántsem az egyetlen számrendszer. A hexadecimális, azaz a tizenhatos számrendszer használata szintén népszerű az informatikában, az egyes programozási nyelvekben sűrűn fordulnak elő hexadecimális számok. *Máté István Zsolt* kiemelte, hogy ebben a definícióban a hangsúly *„a puszta adatra kerül, s az adathordozót bárminemű is legyen azt elhagyja a meghatározásból"*[4]. Eoghan Casey szerint digitális bizonyíték *„minden olyan adat, amely alátámaszthatja, hogy bűncselekmény történt, vagy amely összekapcsolja a bűncselekményt annak elkövetőjével"*[5]. Hasonló a digitális bizonyíték fogalma a brit jogban is, a Rendőrfőnökök Egyesülete a következőképpen definiálta a fogalmat: *„a számítógép-alapú elektronikus bizonyíték olyan nyomozási értékkel bíró információ és adat, amelyet számítógépen tárolnak vagy számítógép segítségével továbbítottak"*[6]. Az európai szabályozásban szintén nem ismeretlen a digitális bizonyíték. Az Európa Tanács számítástechnikai bűnözésről szóló egyezményének preambuluma rögzíti, hogy *„jelen egyezmény célja, hogy […] lehetővé tegye a bűncselekmények elektronikus formában megjelenő bizonyítékainak összegyűjtését"*[7]. Az

3 Digital & Multimedia Evidence Glossary, 2015. Scientific Working Group on Digital Evidence and Imaging Technology, 2016, p. 7. https://www.swgde.org/documents/Current Documents/2015-05-27 SWGDE-SWGIT Glossary v2.8

4 Máté István Zsolt: Digitális bizonyíték. In: Törő Csaba – Cservák Csaba – Rixer Ádám – Fábián Ferenc – Miskolczi Bodnár Péter – Deres Petronella – Trencsényiné Domokos Andrea (szerk.): IX. Jogász Doktoranduszok Országos Szakmai Találkozója 2013. Károli Gáspár Református Egyetem, 2014, 86–94. o.

5 Eoghan Casey: i. m. 7. o.

6 Good Practice Guide for Computer-based Electronic Evidence. Association of Chief Police Officers, March, 2012, p. 6.

7 2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt számítástechnikai bűnözésről szóló egyezményének kihirdetéséről. http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0400079.TV

egyezmény eljárásjogi szabályai emellett több esetben szólnak elektronikus bizonyítékról (14., 23., 25., 35., 46. cikk), ellenben nem definiálják, hogy mit értenek elektronikus bizonyítékon. A magyar jogirodalomban szintén találhatunk kísérletet a digitális bizonyíték definiálására. *Peszleg Tibor* szerint a digitális bizonyíték *„olyan számítástechnikai eszközről beszerzett adat, amelyet bűncselekménynél valamilyen formában számítástechnikai eszközön tároltak, vagy amelyek feldolgoztak információkat a bűncselekményekkel kapcsolatban”*[8].
Az iménti definícióknak két közös elemük van:

1. Az információk, adatok a büntetőjogilag releváns tényekre vonatkoznak.
2. Olyan információkról, adatokról van szó, amelyeket számítógép (információs rendszer) tárol, vagy továbbít. E pont tekintetében van némi különbség az egyes meghatározások között, hiszen a digitális bizonyítékokkal foglalkozó tudományos társaság definíciója az adathordozóknak a számítógépnél tágabb körét öleli fel.

A digitális bizonyítékok számos olyan kérdést felvetnek, amelyekre még nem született egységes és kielégítő válasz. Ahogy arról már korábban esett szó, a bizonyíték fogalmának egyik kulcseleme, hogy az információ megszerzése törvény által megengedett forrásból, azaz bizonyítási eszközből történjen. A digitális bizonyítékok esetében azonban nem teljesen egyértelmű, hogy mit tekintsünk a bizonyíték forrásának. A szakirodalmat és a vonatkozó jogszabályi rendelkezéseket vizsgálva megállapítható, hogy e tekintetben két elmélet létezik: az egyik szerint a digitális bizonyítékok forrása minden esetben az a tárgy (adathordozó), amely a bizonyítékot tartalmazó adatot (amely lehet szöveges, kép-, videofájl vagy akármilyen program, illetve alkalmazás) tárolja. E szerint az elmélet szerint a digitális bizonyítékokat minden esetben olyan tárgyi bizonyítási eszközök hordozzák, amelyek képesek elektronikus formában létező adatok rögzítésére, tárolására, továbbítására. Ilyen eszközök lehetnek a desktopok (asztali számítógépek), laptopok, táblagépek, játékkonzolok, okostelefonok, CD-k, DVD-k, pendrive-ok, nyomtatók. A másik elmélet, amely főleg angolszász területen honosodott meg, ennél jóval komplexebb képet fest. E szerint az elmélet szerint a bizonyítékforrás az elektronikusan tárolt adat (szövegfájl, táblázat, képfájl, videofájl, hangfájl, naplófájlok, metaadatok stb.), hiszen a hatóságok közvetlenül ezekből szerzik a releváns információt, a hardver csupán olyan szerepet tölt be, mint egy iratokat tároló szekrény. Nem mindegy azonban, hogy ez az információ milyen viszonyban

8 Peszleg Tibor: Interneten, számítógépen történő nyomrögzítés. Ügyészek Lapja, 2005/1., 25. o.

van az őt hordozó fizikai komponenssel, bizonyos esetekben ugyanis az információ kizárólag a hardverrel együttesen vizsgálható és értékelhető. Az Egyesült Államokban igen részletes és precedenseken alapuló szabályok határozzák meg azt, mikor szükséges a hardvert az adattal együtt vizsgálni és mikor van szükség csupán a tárolt adatok információtartalmára. A két elmélet közötti legmarkánsabb különbség az, hogy míg az első az adatra és annak tárolójára elválaszthatatlan egységként tekint, addig a második lehetőséget ad arra, hogy a hatóság az adatot és az azt tároló hardvert egymástól függetlenül kezelje, aminek az adat megismerésére irányuló kényszerintézkedések során van nagy jelentősége. Magyarországon a gondot jelenleg az jelenti, hogy sem a Be. rendelkezéseiből, sem a szakirodalom vizsgálatából nem szűrhető le egyértelmű állásfoglalás az iménti kérdésben. A Be. ugyanis a bizonyítási eszközök taxatív felsorolásában nem nevesíti külön az elektronikusan tárolt adatot, a későbbiekben a kényszerintézkedések szabályai között azonban már igen, és több helyen is rendelkezik olyan adatokról, amelyek bizonyítási eszközök. Ha ragaszkodunk ahhoz, hogy a Be. 76. §-ában felsorolt bizonyítási eszközök rendszere kötött, a digitális bizonyíték forrása csak a tárgyi bizonyítási eszköz lehet, amely lehet bármely *„olyan tárgy, amely műszaki, vegyi vagy más eljárással adatokat rögzít”*[9]. Úgy tűnik azonban, hogy a helyes értelmezés az, hogy a Be. 76. §-ában található felsorolás nem taxatív, ugyanis a Be. több szakasza említést tesz olyan információs rendszerben tárolt adatról, amely maga is bizonyítási eszköz (lásd lefoglalás). Ha utóbbi feltevést vesszük alapul, a digitális bizonyíték forrása nem az adathordozó mint tárgyi bizonyítási eszköz, hanem az információs rendszerben tárolt adat. *Tremmel Flórián* szerint *„egyre több bizonyítási mód önálló jelentőségre tesz szert, s egyszersmind sui generis eljárási szabályozás révén legalizálódik”*[10]. A következetesség hiánya különösen a Be. azon rendelkezései kapcsán okoz problémát, amelyek a digitális bizonyítékok, illetve az azokat hordozó bizonyítási eszközök megszerzését és megőrzését szolgáló kényszerintézkedésekre vonatkoznak. A digitális bizonyítékok forrásának tisztázása azért kiemelkedően fontos feladat, mert a jelenlegi szabályozási és értelmezési bizonytalanságok a jogbiztonságot, illetve az eljárásban részt vevő személyek jogait veszélyeztetik. A következő részben azokat a dilemmákat mutatom be részletesen, amelyek amiatt vetődhetnek fel, hogy nem tisztázott, milyen bizonyítási eszközhöz rendeljük a digitálisan tárolt adatot.

9 Be. 115. § (2) bek.

10 Tremmel Flórián: Bizonyítékok a büntetőeljárásban. Dialóg Campus Kiadó, Budapest–Pécs, 2006, 67. o.

A digitális bizonyítékok megszerzése és megőrzése

A magyar büntetőeljárás számos olyan lehetőséget ad a nyomozó hatóságok számára, amelyek által a digitális bizonyítékok megismerhetők, megszerezhetők, illetve megőrizhetők. Ezeket a lehetőségeket a Be., valamint a rendőrségről szóló törvény tartalmazza. A digitális bizonyíték megismerhető:

– megkereséssel (Be. 71. §);
– az adathordozónak, illetve az adatnak a lefoglalásával (Be. 151. §);
– információs rendszerben tárolt adatok megőrzésére kötelezéssel (Be. 158/A §);
– titkos információgyűjtéssel (1994. évi XXXIV. törvény a rendőrségről 63. §); illetve
– titkos adatszerzéssel (Be. 200–202. §).

Speciális jellegük miatt jelen tanulmány nem tárgyalja a titkos információgyűjtéssel és a titkos adatszerzéssel kapcsolatos dilemmákat.

A megkeresés

A megkeresés jogintézménye az egyik legjobb példa a hardver és az adat elválaszthatóságára. Ha a nyomozó hatóság egy hírközlési szolgáltatótól igényli egy felhasználó azonosításához szükséges adatokat, fel sem vetődik kérdésként, hogy a hatóság részére azt az információs rendszert, illetve adathordozót kellene megküldeni, amelyen az eredeti adat található. A nyomozó hatóság általában megelégszik az adatok CD-n vagy DVD-n megküldött duplikátumával. Ennek oka, hogy az eljárás szempontjából az adat és annak a tartalma a lényeges, nem pedig az, milyen adathordozón tárolták.

A lefoglalás

A digitális bizonyítékok említett megismerési lehetőségei közül a lefoglalás okozza a legtöbb problémát, és ez a kényszerintézkedés jelenik meg a leggyakrabban a médiában is, amikor informatikai bűncselekmények nyomozásáról esik szó. Ez a kényszerintézkedés tükrözi a leginkább a digitális bizonyítékok forrásával kapcsolatos polémiát. A Be. 151. §-ának (2) bekezdése kimondja, hogy: *„A bíróság, az ügyész, illetve a nyomozó hatóság elrendeli – az ingatlan kivételével – annak a dolognak, információs rendszernek, ilyen rendszerben tárolt adatokat tartalmazó adathordozónak* vagy adatnak *a le-*

foglalását, amely a) bizonyítási eszköz." Az idézett rendelkezés szerint tehát a digitális bizonyíték háromféleképp is lefoglalható:

– a teljes információs rendszer lefoglalásával;
– csak az érintett adatot tartalmazó adathordozó lefoglalásával;
– csak az adatnak a lefoglalásával;

A teljes információs rendszer lefoglalása sok esetben nem szerencsés. Egyrészt a teljes rendszer számtalan olyan egységből áll, amelyek a büntetőeljárás szempontjából nem releváns hardverkomponensek (például videokártya, hangkártya, tápegység). Ezek a komponensek igen gyakran azonban nagyobb értékkel bírnak és a technológia rohamos fejlődésének következtében gyorsan amortizálódnak, így a lefoglalás elszenvedőjének súlyos anyagi kárt okozhat, ha a hatóság az adathordozóval együtt ezeket az eszközöket is lefoglalja. A teljes konfiguráció lefoglalása személyiségi jogi aggályokat is felvet. Az adatvédelmi biztos 2009-es beszámolója[11] alapján számtalan esetben előfordul, hogy a lefoglalt számítógép olyan személyes adatokat is tartalmaz, amelyek semmilyen összefüggésben nincsenek a büntetőeljárással. Ezek a személyes adatok sok esetben hosszú hónapokig maradnak a nyomozó hatóságnál, ami a személyes adatok védelméhez fűződő jog sérelmét jelentheti. Az információs rendszer nemcsak egy különálló számítógép lehet, hanem az adatok automatikus kezelését, tárolását, továbbítását biztosító, egymással kapcsolatban lévő berendezések összessége is, vagyis akár egy céges hálózat összes számítógépére/szerverére kiterjeszthető a lefoglalt dolgok köre. (Sőt, ezen az úton elindulva, ha egy számítógép az internethez csatlakozik, az összes internethez csatlakoztatott eszközt tekinthetnénk egy információs rendszernek.) A cég működéséhez szükséges eszközök lefoglalása azonban veszélyezteti a kényszerintézkedéssel érintett cégek üzletszerű működését. Egy webhosting szolgáltatást nyújtó vállalkozás például működésképtelen a szerverei nélkül, hiszen az általa nyújtott szolgáltatás lényege éppen az, hogy tárhelyet kínál a felhasználóinak. A felhasználók számára is előnytelen következményekkel járhat egy szerver lefoglalása: egy-egy szerver ugyanis általában több felhasználó számára nyújt tárhelyet, így a lefoglalással vétlen harmadik személyek weboldalai válhatnak elérhetetlenné, illetve e személyek személyes adatai kerülnek szükségtelenül a nyomozó hatósághoz. A teljes konfiguráció lefoglalásának tagadhatatlanul vannak azonban bizonyos

11 Az adatvédelmi biztos beszámolója 2009, 35. o. http://www.naih.hu/files/Adatvedelmi-biztos-beszamoloja-2009.PDF

előnyei is. A legnagyobb az, hogy kevés szakértelmet igényel, ezért a lefoglaláshoz nem szükséges szaktanácsadó igénybevétele, azt a nyomozó hatóság tagjai is el tudják végezni. További előnye, hogy ezáltal a szükséges vizsgálatok laboratóriumban kontrollált körülmények között végezhetők el, valamint biztosítható, hogy a lefoglalás után az eredeti adatokban semmilyen változás ne következzen be.

A második lehetőség, hogy a hatóság csak az érintett adatot tartalmazó adathordozót foglalja le. Az adathordozó lefoglalásának kétségtelen előnye, hogy a lefoglalás elszenvedőjének nem okoz a szükségesnél nagyobb sérelmet, valamint ez a módszer is lehetővé teszi az adathordozó későbbi, kontrollált környezetben történő vizsgálatát. Hátránya ellenben, hogy az adathordozó szakszerű kiszereléséhez minden esetben hozzáértő személy szükséges. Hátrány lehet továbbá, ha az is előfordulhat, hogy a lefoglalt adathordozó inkompatibilis a vizsgálatot végző szervezet rendszerével (például az adathordozó beszerelése egy másik rendszerbe *incompatible BIOS translation detected* hibaüzenetet idézhet elő), vagy ahogy Peszleg Tibor is rávilágít, vannak olyan eszközök, amelyek *„olyan egységet képezhetnek, hogy ha megbontják őket, már nem lehetséges az eredeti adattartalom visszaállítása (pl. RAID tömbök esetében)”*[12].

Harmadik opcióként lehetőség van arra, hogy a hatóság csak az adathordozó tartalmát, vagyis az adatokat foglalja le. A lefoglalás és a büntetőeljárás során lefoglalt dolgok kezelésének, nyilvántartásának, előzetes értékesítésének és megsemmisítésének szabályairól, valamint az elkobzás végrehajtásáról szóló 11/2003. (V. 8.) IM–BM–PM együttes rendelet megerősíti azt a nézetet, hogy az adat önmagában is lefoglalható. A rendelet 67. §-a kimondja, hogy *„Az elektronikus úton rögzített adatot a hatóság adathordozóra történő rögzítés (átmásolás) útján foglalja le, vagy a helyszínen lefoglalt adathordozóról az adatokat szakértő vagy szaktanácsadó bevonásával menti le”*. A magyar nyomozó hatóságok gyakorlatában azonban egyáltalán nem jellemző az adat helyszíni lefoglalása, a hatóság rendszerint a teljes gépet lefoglalja, majd később szakértő bevonásával végzi el a szükséges műveleteket. Az adat lefoglalásának módszertani kérdéseiről sem a törvény, sem a rendelet nem szól részletesen, pedig a másolás módszerének fontos jelentősége van. Az adat átmásolására ugyanis kétféle lehetőség is kínálkozik.

Az egyik, amikor a hatóság a rendszert a helyszínen átvizsgálja és a relevánsnak ítélt adatokat hagyományos módon másolja ki az információs rend-

12 Peszleg Tibor: A digitális bizonyítási eszközök megszerzésének elvei és gyakorlati érvényesülésük. Ügyészek Lapja, 2010/2., 23–31. o.

szerből közvetlenül egy adathordozóra (esetleg egy másik információs rendszerre). E módszer előnye, hogy nem kell hozzá különös szakértelem, illetve, ha a lefoglalás elszenvedője együttműködő, a rendszer adminisztrátora, tulajdonosa maga is feltárhatja a hatóság előtt az egyes bizonyítékokat. Emellett viszont számos szempontból aggályos, az alkalmazása próba elé állítja ugyanis mind a hitelesség, mind a teljesség kriminalisztikai elvének érvényesülését. A digitális bizonyíték akkor hiteles, ha a későbbiekben is pontosan meghatározható, hogy az adat egy bizonyos számítógépről/helyszínről származik, illetve hogy a digitális bizonyítékot tartalmazó adat pontos és teljes másának lefoglalására került sor, továbbá hogy az adat a lefoglalása óta változatlan maradt. Ezen alapelvek érvényesülését hivatott biztosítani a 11/2003. (V. 8.) IM–BM–PM együttes rendelet 67. §-ának (2) bekezdése, amely arról rendelkezik, hogy a lefoglalás kizárólag utólag meg nem változtatható adathordozóra történhet, amely a lefoglalás időpontjában adatokat nem tartalmazhat. Ezen felül rendelkezik arról, hogy az átmásolás során gondoskodni kell arról, hogy az eredeti adatok ne változzanak meg, ami általában csak speciális írásvédő eszköz vagy szoftver segítségével valósítható meg. A teljesség elve azt jelenti, hogy minden bizonyítékot le kell foglalni, azonban ha a lefoglalást végzőnek nincs kellő szakértelme, fontos bizonyítékok veszhetnek el. A számítógép ugyanis sokszor az átlagfelhasználó számára láthatatlan helyeken is tárol információkat, valamint olyan adatokat kezel, amelyeket a gép működés közben nem ment a merevlemezre. Előbbire példák lehetnek a metaadatok, a cache tartalma, illetve a RAM által ideiglenesen tárolt információk, utóbbira pedig a sandboxban futó alkalmazások adatai (például a chatablakban folytatott beszélgetés).

Az adatok lefoglalására nyitva áll egy másik lehetőség is, mégpedig amikor a hatóság bitazonos, hash kulccsal ellátott tükörmásolatot készít a teljes adathordozóról. A hitelesség szavatolására ebben az esetben egy hash kulcsnak nevezett ellenőrző kód szolgál, amely egy egyedi adatállományhoz rendelt karaktersorozat. Abban az esetben, ha az eredeti és a tükörmásolat bitről bitre ugyanazokat az adatokat tartalmazza, a hash kulcs azonos, azonban ha bármelyik adathordozón utólag változtatnak, az ellenőrzés során eltérő értékeket kapunk. A tükörmásolat-készítés hátránya, hogy nem praktikus, ha nagy mennyiségű információ lefoglalása szükséges, ugyanis rendkívül idő- és erőforrásigényes. A tükörmásolat készítésére vonatkozó előírások azonban korántsem ismeretlenek a magyar jogban. Az 1996. évi LVII. számú, a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról szóló törvény (a továbbiakban: versenytörvény) *A tényállás tisztázása* alcím alatt rendelkezik arról, hogy *„hi-*

vatalból folytatott eljárásban a vizsgáló jogosult az adathordozóról fizikai tükörmásolatot készíteni, és a tükörmásolat felhasználásával az adathordozón lévő adatokat átvizsgálni, ha valószínűsíthető, hogy az adathordozón a vizsgált magatartáshoz kapcsolódó, a felhasználó által a számítógép rendeltetésszerű használata során már nem megjeleníthető adatok találhatók"[13].

Információs rendszerben tárolt adatok megőrzésére kötelezés

Az elektronikusan tárolt adat külön jelenik meg az információs rendszerben tárolt adatok megőrzésére kötelezésének szabályai között is. A Be. 158/A §-ának (2) bekezdése úgy szól, hogy *„A bíróság, az ügyész, illetőleg a nyomozó hatóság elrendeli* annak az információs rendszerben tárolt adatnak a megőrzését, amely bizonyítási eszköz, *vagy bizonyítási eszköz felderítéséhez, a gyanúsított kilétének, tartózkodási helyének a megállapításához szükséges"*. A törvény indokolása szerint ennek a kényszerintézkedésnek a bevezetésére azért volt szükség, mert a számítógépes hálózatokon tárolt adatok mennyisége az utóbbi években ugrásszerűen növekedett, és a jogalkotó felismerte, hogy adott esetben egy teljes szerver lefoglalása a vétlen hálózatüzemeltetőnek méltánytalanul nagy hátrányt okozhat. A kényszerintézkedés elrendelése után azonnal meg kell kezdeni az érintett adatok átvizsgálását, amely két eredményre vezethet: a megőrzésre kötelezést meg kell szüntetni, vagy az adat lefoglalását kell elrendelni. A nyomozó hatóságok nagyon ritkán alkalmazzák ezt a kényszerintézkedést, ugyanis a legtöbb esetben az adatok lementésére, a bizonyítékok biztosítására törekednek, így nem hagyják az adatokat olyan személyek megőrzésében, akik valamilyen módon az elkövetéshez köthetők. Az elkövetéshez nem köthető esetekben (például sértett vagy harmadik személy) a kényszerintézkedés elszenvedője pedig szinte mindig együttműködő, ezért szintén végrehajtható a lefoglalás, kimentés.

Az elektronikusan tárolt információ az amerikai büntetőeljárásban

Az amerikai büntetőeljárásban sokkal átláthatóbb szabályok vonatkoznak erre a területre, a digitális bizonyíték forrása kapcsán több precedensértékű

13 A tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról szóló 1996. évi LVII. törvény, 65. § (2) bekezdés.

döntés is született. Az Egyesült Államokban kialakult rendszer szerint a digitális bizonyíték forrása az elektronikusan tárolt információ *(electronically stored information),* a hardver és az adat nem interdependens, hanem egymástól függetlenül is kezelhető.

Ha az amerikai büntetőeljárás bizonyításról szóló törvényi rendelkezéseit vizsgáljuk, azt találjuk, hogy a bizonyítási eszközöket sem a szövetségi büntetőeljárásról szóló törvény *(Federal Rules of Criminal Procedure*[14]*),* sem a bizonyítékok szövetségi szabályairól szóló törvény *(Federal Rules of Evidence*[15]*)* nem sorolja fel tételesen. Ennek oka a kontinentális és az angolszász büntetőeljárás-jogi rendszerek közötti eltérésben keresendő. A kontinentális jogrendszerekben ugyanis a bizonyítékok összegyűjtésére és értékelésére már az ügy bíróság elé kerülése előtt, az eljárás nyomozati szakaszában sor kerül, és ez az eljárás törvényi szinten szabályozott, szigorú formaságokhoz kötött. Ezzel szemben, ahogy azt Tremmel Flórián is kifejtette[16], az amerikai bizonyítási rendszer negatív kötött, hiszen fő szabályként bármi lehet bizonyíték, kivéve, amelyet jogszabály vagy a bíróság kizár. A bizonyítékok felhasználhatóságáról való döntés *(admissibility)* a bíróság egyedi mérlegelésére van bízva, a részletes eljárási szabályokkal szemben a hangsúly sokkal inkább az eljárási garanciákon van. Törvényi szinten csak annyi szerepel a bizonyítási eszközökről, hogy *„minden releváns bizonyíték felhasználható, kivéve amennyiben az alkotmány, szövetségi törvény, a bizonyítékokról szóló szövetségi törvény vagy a legfelsőbb bíróság által előírt egyéb szabályok így rendelkeznek”*[17]. Ennek megfelelően bizonyítási eszköz lehet minden, amit az alkotmány vagy jogszabály nem tilt, ha az ügyben eljáró bíró azt az adott ügy viszonylatában relevánsnak ítéli. A bizonyíték akkor releváns, *„ha alkalmas arra, hogy egy tényt valószínűbbé vagy kevésbé valószínűvé tegyen, mint az a bizonyítási eszköz hiányában lenne, és a tény következményekkel bír a cselekmény meghatározásánál”*[18]. A relevancia kritériumának teljesülése azonban önmagában nem elégséges ahhoz, hogy egy bizonyíték az eljárásban felhasználható legyen. *Gordon Mahler* szerint a bizonyítékok mérlegelése egy számos technikai szabállyal megtűzdelt rendszer, amely az amerikai jogi egyetemeken külön tantárgy.[19] Ennek megfe-

14 Federal Rules of Criminal Procedure. https://www.law.cornell.edu/rules/frcrmp

15 Federal Rules of Evidence. https://www.law.cornell.edu/rules/fre

16 Tremmel Flórián: i. m. 63. o.

17 Federal Rules of Evidence Rule 402. General Admissibility of Relevant Evidence

18 Fantoly Zsanett: A büntető tárgyalási rendszerek sajátosságai és a büntetőeljárás hatékonysága. HVG-ORAC Lap- és Könyvkiadó Kft., Budapest, 2012, 135. o.

19 Gordon Mahler: Az amerikai büntetőeljárás vázlata. In: Tóth Mihály (szerk.): Büntető eljárásjogi olvasókönyv. Osiris Kiadó, Budapest, 2003, 77. o.

lelően az elektronikusan tárolt információknak is számos követelménynek kell megfelelniük ahhoz, hogy bizonyítékként felhasználhatók legyenek. Az elektronikusan tárolt információk bizonyítékként való felhasználhatóságáról először 2007-ben egy polgári ügyben, a *Lorraine v. Markel-ügy*ben született döntés. A döntéshez fűzött indokolás[20] egy ötlépcsős tesztet ír elő, amelyen az elektronikusan tárolt információknak át kell menniük ahhoz, hogy az eljárás során bizonyítékként értékelhetők legyenek. Ha az elektronikusan tárolt információ az említett teszten sikeresen átmegy, akkor a büntetőeljárásban bizonyítékként felhasználható. Az, hogy a *Lorraine v. Markel-döntés* polgári eljárásban született, nem jelenti azt, hogy büntetőügyben nem alkalmazható. A *United States v. O'Keefe-ügy*ben a bíróság kimondta, hogy *„botorság lenne figyelmen kívül hagyni a polgári eljárásban alkalmazott szabályokat csak azért, mert büntetőügyről van szó, különösen akkor, ha jobbnak tűnik ezen szabályokat alkalmazni, amikor a dokumentumok előállítása mind polgári mind büntető ügyekben ugyanazokat a problémákat vetik fel, mint újra feltalálni a kereket"*[21].

Az egyes kényszerintézkedések, főleg a lefoglalás tekintetében igen részletes szabályok vonatkoznak arra, hogy mikor van szükség az elektronikusan tárolt információ mellett az azt hordozó hardverre is. Az Egyesült Államok igazságügyi minisztériuma *(United States Department of Justice)* 1994-ben ajánlást adott ki a számítógépek átvizsgálásáról és lefoglalásáról, valamint az elektronikus bizonyítékok összegyűjtéséről. Az ajánlás az első kiadás óta folyamatosan frissül, hogy lépést tarthasson a legújabb technológiai fejlesztésekkel, a legfrissebb eljárási szabályokkal és az esetjoggal. Az ajánlás elválasztja egymástól azokat az eseteket, amelyekben a hardver, és amelyekben a tárolt információ lefoglalása szükséges. A dokumentum szerint: *„a legfontosabb döntés, amelyet a nyomozóknak meg kell hozniuk, amikor összeállítják a lefoglalandó dolgok listáját az, hogy a lefoglalandó dolog a számítógép fizikai komponense (hardver) vagy csupán az információ, amelyet a hardver tartalmaz"*[22]. Bizonyos esetekben ugyanis a hardver csupán az elektronikusan tárolt információk tárhelyéül *(container)* szolgál, így önmagában csekély relevanciával bír. Minden ügyben egyedi mérlegelést kíván annak eldöntése, hogy a sikeres bizonyításhoz szükség van-e a hardverre, vagy ele-

20 Lorraine v. Markel Am. Ins. Co., 2007. https://www.lexisnexis.com/applieddiscovery/LawLibrary/LorraineVMarkel_ESI_Opinion.pdf

21 United States v. O'Keefe, 2008. p. 7. http://www.craigball.com/okeefe.pdf

22 H. Marshall Jarrett – Michael W. Bailie – Ed Hagen – Nathan Judish: Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. Washington, 2009, p. 70. http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf

gendő a tárolt adat. A döntés meghozatalához elsősorban azzal kell tisztában lennünk, hogy a számítógépek milyen lehetséges szerepeket tölthetnek be egy bűncselekményben. Az amerikai *Donn Parker*[23] a bűncselekményekben megjelenő számítógépek (információs rendszerek) lehetséges szerepeit tanulmányozta, és listát készített azokról a szerepekről, amelyekben a számítógép egyes alkotóelemei előfordulhatnak:

– A számítógép lehet fizikai valójában (hardver) az elkövetés tárgya (például amikor a számítógépet, vagy infokommunikációs eszközt ellopják vagy megrongálják).
– A számítógépes környezet lehet az elkövetés tárgya. Ez az eset akkor következhet be, ha a sérelem nem a hardverben következik be, hanem valamely számítógépes adatban, amely lehet valamely futtatott program, vagy a számítógépen tárolt információ. Tipikus példa, amikor a számítógépet vírussal vagy más malware-rel fertőzik meg, amely akadályozza annak helyes működését.
– A számítógép fizikai valójában (hardver) lehet az elkövetés eszköze: ritkán ugyan, de előfordul, hogy a számítógép valamilyen fizikai komponensével követnek el bűncselekményt. Ilyen például az a 2010-es emberölési eset, amelyben három fiatal számítógép-vezetékkel fojtott meg egy férfit.[24]
– A számítógépes környezet mint az elkövetés eszköze (a számítógép az elkövetés eszköze azokban az esetekben, amikor az elkövető a számítógépet arra használja, hogy azzal valamilyen bűncselekményt kövessen el). Tipikus példák a zaklatás, gyermekpornográf tartalmak letöltése, online aukciós csalás.

Az amerikai igazságügyi minisztérium útmutatója szerint a hardverre akkor van szükség, ha az tiltott eszköz, a bűncselekmény „gyümölcse", azaz eredménye vagy eszköze. Eoghan Casey szerint tiltott eszköz a hardver, amennyiben az *„olyan eszköz, amelynek a birtoklása tilos az állampolgárok számára. Az Egyesült Államokban, bizonyos esetekben tilos az egyéneknek olyan hardvert birtokolniuk, amely az elektronikus kommunikáció lehallgatására szolgál."*[25] A bűncselekmény eredménye az információs rendszer, ha azt az elkövetés során szerezték, vagy az elkövetés során jött létre, ilyenek tipikusan a lopott alkatrészek, amelyek vonatkozásában kétségen felül áll, hogy az elkövető birtokából el kell vonni. A hardver akkor lehet a bűncselekmény eszkö-

23 Eoghan Casey: i. m. 40. o.
24 Számítógép-vezetékkel fojthatták meg a jászberényi pedofilt. Origo.hu, 2010. február 12. http://www.origo.hu/itthon/20100212-szamitogepvezetekkel-fojthattak-meg-a-jaszberenyi-pedofilt.html
25 Eoghan Casey: i. m. 44. o.

ze, ha a fizikai sérülés okozására használják, ám Eoghan Casey szerint van ennél jóval szemléletesebb példa is: az olyan speciálisan elkészített, felszerelt, konfigurált hardver is lehet a bűncselekmény elkövetésének eszköze, amelyet bizonyos bűncselekmények elkövetésére hoztak létre. Példának hozza az úgynevezett *sniffer*eket, amelyek a hálózati forgalom lehallgatására alkalmas eszközök. Minden más esetben elegendő pusztán az elektronikusan tárolt információt beszerezni, amely a hardver analógiájára lehet tiltott információ, a bűncselekmény gyümölcse, illetve eszköze, valamint maga a bizonyíték is. Tiltott információ például a gyermekpornográfia. Az információ a bűncselekmény eszköze akkor lehet, ha a bűncselekmény megvalósítására használták, például a vírusok és egyéb kártékony kódok. Egyéb esetekben, ha az információ birtoklása nem tiltott és nem is használták a bűncselekmény eszközéül, az információ a bűncselekmény bizonyítéka. Az Egyesült Államok igazságügyi minisztériumának ajánlása utóbbira egy vállalkozás elektronikusan tárolt meghamisított üzleti könyveit, valamint a drogkereskedők tranzakcióinak listáját hozza példaként.

Konklúzió

A magyar büntetőeljárási rendszer rendkívül elnagyolt képet fest a digitális bizonyítékok forrását illetően. A rendelkezéseket vizsgálva látszik, hogy a magyar jogalkotó lehetőséget kívánt nyújtani mind az adathordozó tárgyi bizonyítékként való kezelésére, mind az adathordozón lévő adatnak mint önálló bizonyítási eszköznek a kezelésére, a szabályok azonban nem kellőképpen kidolgozottak, ami a gyakorlatban értelmezési nehézségekhez vezethet. Az amerikai büntetőeljárási rendszert vizsgálva megállapítható, hogy az elektronikus információ beemelése a bizonyítási eszközök közé korántsem elvetendő gondolat, hiszen a hardver és az információ elválasztása változatosabb jogszabályi lehetőségek kialakítását teszi lehetővé, ez által a büntetőeljárási rendszer jobban alkalmazkodhat az egyes ügyek sajátosságaihoz. Annak érdekében, hogy a csak az adathordozót, valamint a csak az adatot érintő kényszerintézkedések elhatárolása teljesen egyértelmű legyen, ajánlott lenne kiterjeszteni a bizonyítási eszközök körét az elektronikusan tárolt adatra is. Ez a szemlélet egyébként sem áll távol a Be. rendelkezéseitől, hiszen több kényszerintézkedés leírásánál említést tesz olyan adatokról, amelyek bizonyítási eszközök. Ahogy Tremmel Flórián is megjegyzi: *„a kriminalisztika folytonosan kutatja, bővíti és gazdagítja azoknak az információhordozóknak a körét, fajtáit, ame-*

lyek felhasználásával a bűncselekmények nem csak felderíthetők, hanem bizonyíthatók is lesznek. E két tendencia együttes megléte a bűnügyek gyakorlatában bizonyos feszültséggel is járhat: egyfelől elavulttá válhatnak eljárásjogi rendelkezések (pl. eskü), másfelől pedig még törvényes szabályozást, elismerést nem nyert potenciális bizonyítási eszközök és bizonyítási módok kerülhetnek előtérbe."[26] A hardver és az információ elválasztása során kiemelendő, hogy a megfelelő kényszerintézkedés megválasztása, illetve a végrehajtásának módszere az adott ügy körülményeit, illetve az információs rendszer tulajdonságait figyelembe véve esetenként mérlegelendő. A jogrendszer feladata megteremteni azt az egyértelmű és világos keretrendszert, amely meghatározza, milyen lehetőségek állnak a nyomozó hatóságok rendelkezésére. Az általam javasolt megoldás a lefoglalás esetében egy többoldalú rendszer megalkotása lenne, amely lehetőséget nyújtana annak mérlegelésére, hogy a hardver (teljes információs/csak az egyes adathordozók) vagy csupán a tárolt adat (egyes adatok/az összes adat) lefoglalására kerüljön sor. Ennek érekében mindenképpen indokoltnak tartom a lefoglalás jelenlegi szabályainak átstrukturálását és részletezését. Az adathordozó tartalmának lefoglalásával kapcsolatos szabályok kialakításához jó példa lehet a versenytörvény, amely részletesen, garanciális szabályok beépítésével rendelkezik mind az egyes adatok, mind az adathordozó teljes tartalmának az átmásolásáról. Az előbbieken túl szükségesnek látom egy olyan ajánlás elkészítését, amely útmutatásul szolgál az informatikai elemet tartalmazó bűncselekmények nyomozásában részt vevő személyeknek. Mivel az információs rendszerek vizsgálata és szakszerű lefoglalása nagyon sok esetben hozzáértő személyt igényel, indokoltnak tartom a nyomozó hatóság tagjainak továbbképzését. A szakmai tudás átadását Peszleg Tibor is kiemelten fontos feladatként tartja számon, tanulmányában azt írja, hogy *„igazságügyi szakértőt csak akkor célszerű kirendelni, ha ténylegesen szakkérdés megállapítása szükséges, nem pedig a digitális írástudás pótlására"*[27].

IRODALOM

Bartley, Nancy: A trial of tangled webs. *The Seattle Times,* May 8, 2000

Casey, Eoghan: Digital Evidence and Computer Crime. 3rd edition. Academic Press, 2011

Fantoly Zsanett: A büntető tárgyalási rendszerek sajátosságai és a büntetőeljárás hatékonysága. HVG-ORAC Lap- és Könyvkiadó Kft., Budapest, 2012

26 Tremmel Flórián – Fenyvesi Csaba – Herke Csongor: Kriminalisztika. Dialóg Campus Kiadó, Budapest–Pécs, 2009, 40. o.

27 Peszleg Tibor (2010): i. m. 32. o.

Jarrett, H. Marshall – Bailie, Michael W. – Hagen, Ed – Judish, Nathan: Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. Washington, 2009

Mahler, Gordon: Az amerikai büntetőeljárás vázlata. In: **Tóth Mihály (szerk.):** Büntető eljárásjogi olvasókönyv. Osiris Kiadó, Budapest, 2003

Máté István Zsolt: Digitális bizonyíték. In: **Törő Csaba – Cservák Csaba – Rixer Ádám – Fábián Ferenc – Miskolczi Bodnár Péter – Deres Petronella – Trencsényiné Domokos Andrea (szerk.):** IX. Jogász Doktoranduszok Országos Szakmai Találkozója 2013. Károli Gáspár Református Egyetem, 2014, 86–94. o.

Peszleg Tibor: Interneten, számítógépen történő nyomrögzítés. *Ügyészek Lapja,* 2005/1.

Peszleg Tibor: A digitális bizonyítási eszközök megszerzésének elvei és gyakorlati érvényesülésük. *Ügyészek Lapja,* 2010/2.

Szabó Imre: A számítástechnikai adat, mint elektronikus bizonyíték. In: **Virág György (szerk):** Kriminológiai Tanulmányok 48. Országos Kriminológiai Intézet, Budapest, 2011, 13–28. o.

Tremmel Flórián – Fenyvesi Csaba – Herke Csongor: Kriminalisztika. Dialóg Campus Kiadó, Budapest–Pécs, 2009

Tremmel Flórián: Bizonyítékok a büntetőeljárásban. Dialóg Campus Kiadó, Budapest–Pécs, 2006