

Mezei Kitti

Az elektronikus bizonyítékokkal kapcsolatos kihívások és szabályozási újdonságok

The challenges and legislative novelties related to electronic evidence

Absztrakt

A tanulmány célja, hogy bemutassa az elektronikus bizonyítékokkal kapcsolatos kihívásokat és szabályozási újdonságokat. Először érintve a 2017. évi büntetőeljárásról szóló XC. törvény rendelkezéseit az elektronikus adat lefoglalásával kapcsolatban. Ezt követően az új uniós elektronikus bizonyítékok határon átnyúló megszerzésére vonatkozó rendelet javaslatával foglalkozik. Végül a titkosítással összefüggő aktuális kérdések vizsgálata következik, különös tekintettel az önvádra kötelezés tilalmára a büntetőeljárás során.

Kulcsszavak: elektronikus bizonyíték, elektronikus adat lefoglalása, kriptovaluták, titkosítás, önvádra kötelezés tilalma

Abstract

The aim of the publication is to introduce the challenges and legislative novelties related to electronic evidence. Firstly, it focuses on the current Hungarian Criminal Procedure Law's provisions on seizure of electronic data. Then it continues with the new proposal for regulation on cross-border access to e-evidence at EU level. Finally, it deals with the encryption related issues in the criminal proceedings with special regard to prohibition of self-incrimination.

Keywords: electronic evidence, seizure of electronic data, cryptocurrencies, encryption, prohibition of self-incrimination

Az elektronikus bizonyíték fogalma

A technológiai fejlődés egyre inkább lehetővé teszi a személyazonosság hatékony elrejtését és ez sok esetben megnehezíti a nyomozást, ugyanakkor az elkövetők gyakran digitális nyomot hagynak maguk után, éppen ezért, az elektronikus bizonyítékok egyre fontosabbá válnak a büntetőeljárások során. Az új technológiai vívmányok az elkövetés eszközeként jelennek meg és mindez nem korlátozódik kizárólag az informatikai bűncselekményekre, hanem szinte bármely más deliktum is elkövethető ezek segítségével. A felvázolt esetekben a nyomozó hatóságoknak az elektronikus adatokat kell felkutatniuk, ezért a büntetőeljárásban egyre nagyobb szerepet kap a digitális felderítés. (Lásd ehhez Fenyvesi, 2019, 64-82.) Ez a hazai nyomozások során is tetten érhető, ugyanis már az emberölés miatt induló bűnügyek gyanúsítottjainak is rutinszerűen vizsgálják át a számítógépeit és telefonjait közvetett bizonyítékok után kutatva. (Elek, 2014, 158.)

Először a fogalmi áttekintéssel foglalkozom részletesen. A szakirodalomban a digitális vagy elektronikus bizonyíték elnevezés jelenik meg, amelyek már a második generációs bizonyítékok körébe tartoznak. (Fenyvesi, 2014, 438-440.) Az elektronikus bizonyíték (electronic evidence) fogalma alatt legáltalánosabb értelemben értendő minden olyan bizonyító erejű információ és adat, amelyeket bináris formában tároltak vagy továbbítottak (pl. IP-címek, e-mailek, kép- és videófelvevételek stb.). (Scientific Working Groups on Digital Evidence and Imaging Technology, 2016, 7.) Casey Eoghan szerint a digitális bizonyíték, minden olyan adat, amely alátámaszthatja, hogy bűncselekmény valósult meg, vagy amely összekapcsolja a bűncselekményt annak elkövetőjével. (Casey, 2012, 7.) Marie-Helen Keles szerint az elektronikus bizonyíték magában foglal bármely olyan információt, amely kinyerhető számítástechnikai rendszerekből vagy más digitális eszközökből, amennyiben ez a bűncselekménnyel összefüggésbe hozható, akkor bizonyítékként felhasználható az eljárás során. (Keles, 2015, 76-77.) Peszleg Tibor szerint a digitális bizonyíték: „*olyan számítástechnikai eszközről beszerzett adat, amelyet a bűncselekménynél valamilyen formában számítástechnikai eszközök tároltak, vagy amelyek feldolgoztak információkat a bűncselekményekkel kapcsolatban.*” (Peszleg, 2005, 25.) A fogalom-meghatározásokban közös, hogy büntetőjogilag releváns információkra vonatkoznak, és amelyeket információs rendszeren tárolnak, vagy továbbítanak.

Továbbá az elektronikus bizonyítékokkal kapcsolatban felmerül a kérdés, hogy mit tekintünk a bizonyíték forrásának. Erre vonatkozóan két elmélet létezik: az egyik szerint a forrás minden esetben a tárgy, például adathordozó, amely a bizonyítékot tartalmazó adatot tárolja, míg a másik elmélet alapján – amely főleg az angolszász jogterületen terjedt el – a forrás maga az adat. (Sorbán, 2016, 82-83.)

A hatályos büntető eljárásjogi szabályozás Magyarországon

A Be. hatályba lépése számos változást eredményezett a kényszerintézkedések rendszerében, amely alkalmasabbá tette a digitális kihívásoknak való megfelelésre. Az egyik legfontosabb szabályozási lépés volt, hogy a bizonyítási eszközök közé a 165. § f) pontba bekerült az elektronikus adat is. A törvény 205. § (1) bekezdése a fogalmat is meghatározza, amelynek értelmében: „*elektronikus adat a tények, információk vagy fogalmak minden olyan formában való megjelenése, amely információs rendszer általi feldolgozásra alkalmas, ideértve azon programot is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja.*”. A bizonyítási eszköz a bizonyíték hordozója, a bizonyíték pedig az információ, a büntetőjogilag releváns tény, amelyhez az eszközből jutunk.

Peszleg hangsúlyozza, hogy akár más bizonyítási eszközöknél, így az elektronikus adatok esetében is fontos a törvényesség, szakszerűség és a zárt bizonyítási lánc megléte. (Peszleg, 2005, 24.) Három alapvető kritériumnak kell megfelelni a nyomozás során: a bizonyíték beszerzésénél ne sérüljön vagy módosuljon az eredeti adat, bizonyítható legyen az egyezés az eredetivel, valamint a bizonyíték elemzése ne változtassa azt meg. (Wang, 2007, 218.)

A Be. egyúttal az elektronikus adatra épülő kényszerintézkedések rendszerét vezette be, így a lefoglalását (Be. 315. §), és ezen belül a megőrzésre kötelezettségét (Be. 316. §), valamint az ideiglenes hozzáférhetetlenné tételét (Be. 335. §) (Lásd ezekhez részletesen Herke, 2019, 107-110.). Érdemi változást a lefoglalás szabályozása hozott, így részletesen csak ezzel foglalkozom.

Az elektronikus adat lefoglalása

A Be. 151. § (1) bekezdése alapján a lefoglalás célja a bizonyítási eszköz, illetve az elkobozható dolog vagy a vagyonek Kobzás alá eső vagyron biztosítása a büntetőeljárás eredményes lefolytatása érdekében. Jelen kényszerintézkedés az elektronikus adat feletti tulajdonjogot korlátozza, amelyet a bíróság, az ügyészség és a nyomozó hatóság is elrendelhet. E jogintézmény kulcsfontosságú szerepet játszik az informatikai bűncselekmények felderítésében, az elektronikus bizonyítékok megszerzésének és megőrzésének eszközeként.

Régóta viták folynak arról, hogy pontosan mit is kellene az eljárás során lefoglalni, így a meghatározott adatok körét, vagy az adathordozót, vagy a teljes információs rendszert. Érdemes megemlíteni, hogy az adat lefoglalását először a 2013. évi CLXXXVI. törvény 21. §-a illesztette be a régi 1998. évi büntetőeljárásról

szóló XIX. törvénybe. Ezt megelőzően bevett gyakorlatként volt érvényben a számítógép egészének a lefoglalása (pl. sokszor a büntetőeljárás szempontjából lényegtelen hardvereszközökkel együtt, mint a monitor és a billentyűzet), később a merevlemez vagy még azt sem, és csak másolatot készítettek róla, majd a módosítást követően csak az adatokat foglalták le. (Vadász, 2010, 20.)

Az elektronikus adat lefoglalásának módjait a Be. 315. § (1) bekezdésében felsorolással rögzíti, ami egyben a fokozatosság szabályait figyelembe véve sorrendet állít fel. (Czine, 2018.) A lefoglalása történhet:

- az elektronikus adatról való másolat készítésével,
- az elektronikus adat áthelyezésével,
- az azt tartalmazó információs rendszer vagy adathordozó teljes tartalmáról történő másolat készítésével,
- az azt tartalmazó információs rendszer vagy adathordozó lefoglalásával, vagy a jogszabályban meghatározott más módon lehet végrehajtani.

Az első két esetben magát az adathordozó tartalmát, vagyis az adatokat foglalják le másolat készítésével vagy áthelyezéssel. A lefoglalás módszertani kérdéseivel nem foglalkozik a törvény, annak ellenére, hogy ennek komoly jelentősége van. A másolás történhet egyszer úgy, hogy a hatóság a rendszert a helyszínen átvizsgálja, és a relevánsnak ítélt adatokat hagyományos módon másolja át az információs rendszerről közvetlenül egy adathordozóra. Ennek alkalmazása azonban kihívás elé állítja mind a hitelesség, mind a teljesség kriminalisztikai elvének érvényesülését. A digitális bizonyíték akkor hiteles, ha a későbbiekben is pontosan meghatározható, hogy az adat mely rendszerről származik, illetve, hogy az elektronikus adat pontos és teljes mása került lefoglalásra, továbbá, hogy az adat a lefoglalása óta változatlan maradt. A hiteles adatokon végzett vizsgálatok bármikor megismételhetők, a vizsgálat eredménye reprodukálható. (Matus, 2004, 292.) Ezen alapelvek érvényesülését hivatott biztosítani a 11/2003. (V. 8.) IM-BM-PM együttes rendelet 67. § (2) bekezdése, amely arról rendelkezik, hogy a lefoglalás kizárólag utólag meg nem változtatható adathordozóra történhet, amely a lefoglalás időpontjában adatokat nem tartalmazhat. A hatóság köteles a jegyzőkönyvben feltüntetni az átmásoláshoz használt adathordozó típusát, gyártási számát, illetve a rajta tárolt adat jellegét és tartalmát. Továbbá a rendelet rendelkezik arról, hogy az átmásolás során biztosítani kell, 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. Amennyiben a lefoglalást végző személy nem rendelkezik kellő szakértelemmel, akkor fontos bizonyítékok veszhetnek el (pl. a metaadat, a cache tartalma stb.), ezért indokolt esetben szaktanácsadót kell igénybe venni.

Az adatok lefoglalására nyitva áll egy másik lehetőség is, mégpedig amikor a hatóság szakértő vagy szaktanácsadó bevonásával bitazonos, hash kulccsal ellátott tükörmásolatot készít a teljes adathordozóról, de ez hatékonyan csak kisebb mennyiségű adatállomány esetén alkalmazható. (Sorbán, 2016, 89.)

A teljes rendszer lefoglalásának a hátránya, hogy annak egyes hardver részei (pl. videokártya, alaplap, tápegység stb.) gyorsan amortizálódnak és az elhúzódó büntetőeljárás következtében a lefoglalás elszenvedőjét akár komoly anyagi kár is érheti ezáltal, vagy ennek következményeként akár egy vállalkozás működését is veszélyeztetheti. A lefoglalásnál a szükségtelen károkozás tilalmát, az arányosság és a fokozatosság elvét is figyelembe kell venni. Ennek megfelelően a Be. 271. § egyes bekezdéseiben rögzíti a következőket: kerüljék – különösen a vagyont érintő – kényszerintézkedés megvalósítása során, hogy az érintettek vagy másnak indokolatlanul kárt okozzanak. Továbbá csak a legszükségesebb mértékben és ideig valósuljon meg a kényszerítő eszköz alkalmazása, vagyis arányosságot követel meg, valamint súlyosabb kényszerintézkedés csak akkor rendelhető el, ha enyhébb eszközzel a cél nem érhető el. A kényszerintézkedést az érintett kíméletével kell végrehajtani.

Parti Katalin véleménye szerint a teljes adathordozó lefoglalásának alapját nem képezheti csak az a tény, hogy a bűncselekmény elkövetésére utaló releváns adatokat tartalmaz. Ehhez szükséges a szerver üzemeltetője, tulajdonosa és a bűncselekmény közötti kapcsolat fennállása (pl. megállapítható a gyanúja annak, hogy bűncselekmény elkövetésére használták fel). Hiszen a szerver-gazda számára aránytalan veszteséggel is járhat, ha a teljes adatparkot lefoglalják, mert például nem végezheti tovább az üzleti tevékenységét. (Parti, 2004, 97-101.)

Mindemellett adatvédelmi problémák is felmerülhetnek, mert a lefoglalt számítógép olyan személyes adatokat is érinthet, amelyek nincsenek összefüggésben a büntetőeljárással, vagy több személy adatait is tartalmazhatja (pl. egy vállalati hálózat több számítógépének vagy szerverének lefoglalásakor). (Sorbán, 2016, 89.) A Be. a hatóságok számára kötelezettségként állapítja meg az érintett azon – a magánéletével összefüggő – személyes adatai védelmét, amely adatok a büntetőeljáráshoz nem kapcsolódnak, a bűncselekmények feltárása szempontjából irrelevánsak. A Be. 271. § (5) bekezdésében kimondja, hogy a hatóságok kötelezettsége arra is kiterjed, hogy az érintett magánéletéhez kapcsolódó, de személyes adatnak nem minősülő egyéb körülményei se kerüljenek a nyilvánosság elé. Ennél fogva, amennyiben lehetőség van a szelektálásra, akkor az ilyen jellegű adatokat már eleve ki kell vonni a lefoglalás köréből, ha pedig azok a rögzítést követően, vagyis utólag jutnak a hatóság tudomására, úgy a szükséges biztonsági intézkedések megtétele mellett, a törlésükről kell gondoskodni. Ugyanez a kitétel vonatkozik a gazdálkodó szervek, intézmények

és más szervezetek üzleti, bank vagy ezekkel egy tekintet alá eső titkot képező egyéb adataira is. (Laczi, 2011, 726-728.)

A rendőrségről szóló 1994. évi XXXIV. törvény 90. § is rögzíti, hogy csak bűnüldözési célra lehet felhasználni az összegyűjtött és tárolt személyes adatokat, és e céllal csak azokat kezelhetik, amelyek tényleges veszély elhárításához, illetve meghatározott bűncselekmény megelőzéséhez, felderítéséhez, bizonyításához szükségesek.

Az adatvédelmi biztos állásfoglalásában felhívta a figyelmet arra, hogy az eljáráshoz nem szükséges személyes adatokhoz való hozzáférés csak észszerű időtartamra korlátozható, és egy félévig elhúzódó lefoglalás már ezen túl mutat. (URL1)

Az adatvédelmi biztos beszámolója alapján ismertté vált rendőrségi gyakorlat szerint a személyes adatokhoz csak az igazságügyi informatikai szakértő, az ügy előadója és előjárói férhetnek hozzá és olyan vizsgálati környezetben dolgoznak, ahonnan kizárják az illetékteleneket. A kialakított gyakorlat szerint ugyanakkor a személyes jellegű információkhoz csak az igazságügyi informatikai szakértő férhet hozzá. A rendőrség az igazságügyi informatikai szakértő szakvéleménye alapján határozza meg a bűnyüyleg releváns információkat. (Trócsányi, 2009, 1.) A Nemzeti Nyomozó Iroda gyakorlata alapján a lefoglalt rendszerről teljes másolatot készítenek, és ezt vizsgálják át az eljárás során, ami egyúttal korlátozza az adatokhoz hozzáférők körét. (Dornfeld, 2018, 123.)

Az adathordozók lefoglalásakor a kiszerezéshez mindig hozzáférő személy szükséges, mert előfordulhatnak inkompatibilitási problémák. A merevlemeznek az eredeti hardver környezetből való eltávolítása esetén felmerül az a veszély, hogy a számítógépen futó programok egy része nem lesz elindítható és ezáltal az értékes információkat nem lehet utólag kinyerni. (Vadász, 2010, 19.)

A törvényben a szükségesség-arányosság követelménye a 315. § (4) bekezdésében kiemelten jelenik meg, mert a jogalkotó rögzíti, hogy a büntetőeljárás szempontjából szükségtelen adathordozóra ne terjedjen ki a lefoglalás, amennyiben az mégis kiterjed, akkor a legrövidebb ideig érintse az ilyen adatot. Abban az esetben, ha a másolatkészítés nem veszélyezteti az eljárás érdekét, akkor másolatot kell készíteni az erre jogosult kérésére. Továbbá kimondja, hogy az elektronikus adatot tartalmazó információs rendszer vagy adathordozó akkor foglalható le, ha az elkobozható, illetve vagyonkibozás alá esik, az tárgyi bizonyítási eszközként bír jelentőséggel, vagy a bizonyítás érdekében az abban tárolt, előre meg nem határozható vagy jelentős mennyiségű elektronikus adat átvizsgálására van szükség.

Összességében előrelépés a jelenlegi szabályozás, azonban hiányzik az elektronikus bizonyítékok lefoglalására vonatkozó átfogó és szakszerű útmutatás

hazai viszonylatban, míg példaként említhető az Egyesült Államok, ahol az Igazságügyi Minisztérium részéről, valamint Európában az Európai Tanács és az ENISA által már vannak erre irányuló törekvések. (Lásd U.S. Department of Justice, 2009.; Council of Europe, 2013.; ENISA, 2014.)

Előremutató a törvény a tekintetben is, hogy a jövőben a decentralizált virtuális fizetőeszközök (pl. kriptovaluták) a lefoglalás tárgyát képezhetik. A 315. § (2) bekezdésének értelmében a fizetésre használt elektronikus adat lefoglalását úgy is végre lehet hajtani, ha olyan műveletet végeznek, amely végül is a vagyoni érték feletti rendelkezési lehetőségét akadályozza meg. Ezzel kialakítva az ún. virtuális vagyontárgyak biztosításának a keretszabályát. (Czine, 2018.)

A kriptovaluták esetében azonban problémát jelent az, hogy a jogosult soha nincs fizikai birtokában a kriptovaluta-egységeinek. Mindenképpen a pénztárca fájlra és a privát kulcsra van szükség ahhoz, hogy azokkal rendelkezni lehessen. Éppen ezért az áthelyezés, másolat készítés és az információs rendszerek vagy adathordozók lefoglalása sem vezethet feltétlenül eredményre, mert ugyan a pénztárca fájl át másolható vagy a lefoglalt eszközt (pl. hardver pénztárca) elvonhatják, fennállhat azonban annak a veszélye, hogy a jogosult előzőleg biztonsági másolatot készített róla, és akkor továbbra is rendelkezhet a kriptovaluta egyenlege felett. A megoldást azokban az esetekben, ha a hatóság hozzáfér a privát kulcshoz, az jelentené, hogy rendelkezzenek egy hatósági címmel, amelyre átkellene utalni a virtuális fizetőeszközöket a lefoglalás során, ún. „kikényszerített tranzakcióval”. (Szathmáry, 2015, 646.) Ezen kívül a hatósági felügyelet alatt álló kriptovalutáknak a biztosítása is fontos, különösen a hatósági visszavételek elkerülése érdekében. Például a Silk Road-ügy során nyomozók lopták el a lefoglalt bitcoin-egységeket a hatósági pénztárcából. (URL2) Éppen ezért a hatósági tárcának a legalkalmasabb az ún. multisig vagy multisignature tárca típus, amely csak akkor engedélyezi a kriptovaluták küldését, ha a meghatározott számú privát kulccsal igazolást kap, az előre megadott kulcsok közül. Ezt a rendszert bármilyen kombinációban ki lehet alakítani a felek megegyezése szerint. (Furieux, 2018, 71.)

Az elektronikus bizonyítékok határon átnyúló megszerzése

Napjainkban a nyomozások több mint felében végeznek határokon átnyúló megkeresést egy másik tagállamban vagy az EU-n kívül székhellyel rendelkező szolgáltatók birtokában lévő elektronikus bizonyítékok beszerzése céljából.

Jelenleg az ilyen adatok beszerzéséhez igazságügyi együttműködésre és kölcsönös jogsegélyre van szükség, azonban az eljárás lassú és nehézkes. Ma az olyan bűncselekmények csaknem kétharmada esetén nem lehet megfelelően lefolytatni a nyomozást és a büntetőeljárást, ahol más országban tárolnak elektronikus bizonyítékokat. Ennek az a fő oka, hogy rendkívül időigényes az ilyen bizonyítékok begyűjtése, illetve széttagolt a jelenlegi jogi szabályozás kerete. E kérdéskörben már jelentős bírósági döntések is születtek, amelyek szintén rámutattak arra, hogy ez mennyi problémát hordoz magában (Lásd *Microsoft Corp v. United States-ügy* vagy *Yahoo és Skype v. Belgium-ügy*). (Daskal, 2018.) (Franssen, 2017, 534-538.) Az Egyesült Államokban önkéntes együttműködés alapján működik a bűnüldöző hatóságok és a szolgáltatók közötti adat átadás, ami alternatív módszerként szolgál az elektronikus bizonyítékok beszerzéséhez. Ez a fajta kooperáció ugyan általában gyorsabb, mint az igazságügyi, azonban a szolgáltatók eltérő módon kezelik a megkereséseket és szabadon dönthetnek a kért adatok kiadásáról, ezért megállapíthatjuk, hogy az eljárásból hiányzik az átláthatóság, ami végül jogi bizonytalansághoz vezet. A felhasználók nagy mennyiségű adatot generálnak, amelyek általában a szolgáltatók birtokában vannak, ezért különösen fontos a megfelelő együttműködés alapjainak a megteremtése velük szemben.

Az elektronikus bizonyítékok megszerzésének a gyorsítása és hatékonyabbá tételének érdekében az Európai Tanács elfogadta az álláspontját a büntetőügybeli elektronikus bizonyítékokra vonatkozó, közlésre és megőrzésre kötelező európai határozatokról szóló rendeletről, amit következő lépésként az Európai Parlament előtt tárgyalnak meg.

A rendeletben foglalt legfontosabb újítás, hogy létrehozzák a közlésre kötelező európai határozatot (European Production Order), amely lehetővé teszi, hogy valamely tagállam igazságügyi hatósága – az adatok helyétől függetlenül – közvetlenül igényeljen elektronikus bizonyítékot bármely, az Unióban szolgáltatásokat kínáló és más tagállamban letelepedett vagy képvisellel rendelkező szolgáltatótól. Aki köteles erre 10 napon belül, hitelesen megállapított veszélyhelyzet esetén pedig 6 órán belül válaszolni, így különösen az emberi életet vagy testi épséget vagy kritikus infrastruktúra épségét veszélyeztető helyzet esetén. Ehhez képest a meglévő európai nyomozási határozat esetében 120 nap, míg a kölcsönös jogsegély eljárás esetén pedig 10 hónap a válaszadási határidő.

A rendelet meghatározza az elektronikus bizonyíték fogalmát. Ennek értelmében olyan bizonyítékról van szó, amely elektronikus formában van tárolva a szolgáltatónál vagy a szolgáltató nevében, és fontos követelmény, hogy a határozatok kibocsátásakor a szolgáltatónál rendelkezni kell vele, vagyis nem vonatkozhat a jövőben megszerzendő adatokra. (Tosza, 2018, 214.) A szabályozás

négy adatkategóriát határoz meg. Ezeknek a megkülönböztetésére azért van szükség, mert eltérő szenzitivitásúak, ekként a büntetőeljárás, a bizonyítás, a felderítés során a magánszférát érintő hatósági beavatkozások lehetőségét is differenciálni kell aszerint, hogy melyik adat megismerésére és meddig jogosult az eljáró hatóság. (Szabó, 2011, 16.)

Az előfizetői adat (subscriber data), amely az előfizető vagy ügyfél azonosítását szolgálja, mint például ilyen a megadott név, születési idő, postacím, számlázási és fizetési adat, telefonszám vagy e-mail cím, valamint a szolgáltatás típusa és tartama, az általa használt vagy részére biztosított interfészeket azonosító adatok, a szolgáltatás igénybevételének érvényesítésére vonatkozó adatok, de ez alól kivételt képeznek a felhasználó által megadott vagy a kérésére létrehozott jelszavak, vagy egyéb hitelesítési eszközök.

A hozzáférési adat (access data), amely nem alkalmas a felhasználó azonosítására, azonban az első fontos lépést jelenti ehhez. Ez magában foglalja a felhasználói hozzáférési adatokat egy szolgáltatáshoz például a ki- és bejelentkezések dátumát és idejét, vagy a szolgáltató által kiosztott IP-címet. Az IP-címekre érdemes részletesen kitérni, mert lehetnek statikusak vagy dinamikusak. A statikus cím meghatározott felhasználó számára kerül kiosztásra, míg a dinamikus esetén fontos, hogy pontosan meg kell határozni, hogy milyen időintervallumra nézve szeretné leválogatni az adott IP-címhez tartozó felhasználói kört az arra jogosult szerv, mert lehetséges, hogy egyetlen címet két nap alatt harminc felhasználó használ. A szolgáltatónak ezért több felhasználóra nézve kell vizsgálnia a forgalmi adatot. Éppen ezért a dinamikus IP-cím és az előfizetői adat megismerése gyakran eltérő megítélés alá esik országonként. (Cybercrime Convention Committee, 2018. 4.)

Mind az előfizetői, mind a hozzáférési adat esetében az egyik uniós országból az ügyész vagy bíró közvetlenül, míg a nyomozó hatóság csak valamelyik hozzájárulásával kérheti a másik országban található szolgáltatót vagy annak jogi képviselőjét, hogy biztosítsa a kért elektronikus bizonyítékot a részére.

A tranzakciós adat (transactional data), amely a szolgáltatással kapcsolatba hozható adatok csoportját tartalmazza, így az üzenet forrását vagy célállomását, adat az eszköz helymeghatározására, dátumra, időre, időtartamra, méretre, adattúra, formátumra, a protokoll használatára és a tömörítés típusára vonatkozóan.

A tartalmi adat (content data), amely bármely digitális formában tárolt adat, így például szövegek, hang-, kép- és videófelvevételek stb.

Az előfizetői, hozzáférési és tranzakciós adatok egyben az ún. nem-tartalmi adatok (non-content data). Az előfizetői és hozzáférési adatok elsősorban a felhasználó azonosítását célozzák, míg a tranzakciók és tartalmi adatok már részletesebb képet adhatnak az adott személy tevékenységéről, ezért nagyobb

védelem illeti ezeket. (Tosza, 2018, 214.) Erre tekintettel az utóbbi két adatkategória esetében az egyik uniós országból kizárólag a bíróság közvetlenül, míg az ügyészség és nyomozó hatóság csak a bírói hozzájárulással – aki ellenőrzi a határozatot az ezzel kapcsolatos törvényességi, szükségességi és arányossági követelménynek való megfelelést – kérheti a szolgáltatót vagy annak jogi képviselőjét, hogy biztosítsa a kért elektronikus bizonyítékot a részére. (URL3) A tranzakciós vagy tartalmi adatok egyedi küszöbérték alkalmazása mellett, kizárólag olyan bűncselekményekkel összefüggésben kérhetők, amelyek büntetési tételének felső határa a kibocsátó államban legalább három év szabadságvesztés, illetve kiberbűnözéssel vagy terrorizmussal kapcsolatos bűncselekmények esetében.

Mindezekre tekintettel a megkeresett szolgáltató országának a hatósága csak akkor válik érintetté az ügyben, ha konkrét jogi probléma merül fel, vagy a határozatot végre kell hajtani, mert azt nem teljesíti a szolgáltató.

Az eljárás menete ugyanúgy alakul és ez a szabályozás alkalmazandó, ha az elektronikus bizonyíték nem uniós országban található. Amennyiben a szolgáltató az európai felhasználókra vonatkozó adatokat az EU-n kívül például az Egyesült Államokban tárolja, akkor ugyanúgy köteles az adatokat a határozat értelmében az európai hatóság számára szolgáltatni.

Az elektronikus bizonyítékok egy hozzáértő személy keze által könnyedén megváltoztathatók vagy törölhetőek, ezért sor kerül egy másik fontos jogintézmény bevezetésére, hogy megakadályozzák ezt. Ez az ún. megőrzésre kötelező európai határozat (European Preservation Order). Ez az új eszköz lehetővé teszi, hogy valamely tagállam igazságügyi hatósága konkrét adatok megőrzésére kötelezzon bármely, az Unión belül szolgáltatásokat kínáló és egy másik tagállamban letelepedett vagy képvisellel rendelkező szolgáltatót, annak érdekében, hogy a hatóság ezt az információt később a rendelkezésre álló jogintézmények útján kikérhesse. (URL4)

Az új határozatokat közvetlenül az EU területén működő szolgáltatóknak lehet címezni. Fontos további követelmény ehhez, hogy másik tagállamban kell letelepedniük vagy másik tagállamban rendelkezniük kell képvisellel. Önmagában az EU-n belüli szolgáltatás nyújtás nem elégséges, mert minden szolgáltató ennek következtében a rendelet hatálya alá tartozna.

A szolgáltató fogalmát is meghatározza a rendelet, amelynek értelmében lehet természetes vagy jogi személy és az általa nyújtott szolgáltatás a meghatározó, amik a következők lehetnek: elektronikus hírközlési szolgáltatás, az információs társadalommal összefüggő szolgáltatás, amelynek az adattárolás meghatározó eleme a felhasználó részére nyújtott szolgáltatásoknak, beleértve a közösségi oldalakat is (Twitter és Facebook), valamint az internet domain névvel

és IP-címmel összefüggő szolgáltatás (mint például az IP-cím szolgáltatók, domain név nyilvántartások és nyilvántartók, valamint a kapcsolódó titkosítási és proxy szolgáltatók). Az első két kategória magában foglalja például a következőket: Skype, WhatsApp, Amazon, Dropbox, eBay és az e-mail szolgáltatókat, míg utóbbi kettő az internet infrastruktúrával foglalkozó szolgáltatókat fedti le, akik olyan adatokkal rendelkeznek, amelyek hozzájárulhatnak az elkövetők azonosításához. (Franssen, 2018.)

A javaslat emellett erős biztosítékokat és jogorvoslatokat nyújt. Mindkét határozat kizárólag büntetőeljárás keretében bocsátható ki, és azokra valamilyen büntetőjogi eljárási biztosíték alkalmazandó (pl. védelemhez való jog és ügyirathoz való hozzáférés). Emellett az új szabályok garantálják az alapvető jogok védelmét, valamint a személyes adatok védelméhez való jogot (pl. tájékoztatást kapnak arról, hogy a személyes adatukat kikérték). A kért adatokat nem lehet a megszerzésük céljától eltérő célra felhasználni, kivéve a következő esetekben: a kibocsátó állam közbiztonságát vagy alapvető érdekeit érintő azonnali és súlyos fenyegetés megelőzése érdekében, vagy olyan eljárások céljára, amikor közlésre kötelező európai határozatot lehetett volna kibocsátani. Különböző biztosítékok és jogorvoslatok állnak a szolgáltatók, és azon személyek rendelkezésére, akiknek az adatait kikérik, így az a lehetőség, hogy a szolgáltató felülvizsgálatot kérhet, ha például a határozat nyilvánvalóan sérti az Európai Unió Alapjogi Chartáját. (URL5)

2018 áprilisában, az Európai Tanács javaslat csomagjának a részeként egy irányelv tervezet elfogadására is sor került, annak érdekében, hogy a rendelet hatékonyságát biztosítani tudják. Ennek az irányelvnek a célja, hogy meghatározza a jogi képviselőknek a bizonyítékok összegyűjtése céljából történő kinevezéséről szóló harmonizált szabályozását a büntetőeljárásban. E szerint kötelezik a szolgáltatókat, hogy jelöljenek ki jogi képviselőt az Unión belül annak biztosítása céljából, hogy azonos kötelezettségek vonatkozzanak minden szolgáltatóra, amely szolgáltatásokat nyújt az Európai Unión belül, még akkor is, ha a székhelyük harmadik országban található. Kötelesek jogi képviselőt kijelölni az Unióban a tagállamok illetékes hatóságai által a büntetőeljárás során a bizonyítékok összegyűjtése céljából kibocsátott határozatok és végzések átvétele, az azoknak való megfelelés, és azok végrehajtása érdekében. A jogi képviselőnek azon tagállamok egyikében kell tartózkodnia, ahol a szolgáltató letelepedett vagy szolgáltatásokat nyújt. (URL6)

A határozatok kötelező erejűek lesznek a szolgáltatókra nézve, ami előrelépést jelent, mert jelenleg gyakran a szolgáltatók jóindulatától függ, hogy átadják-e a bűnüldöző hatóságoknak a szükséges bizonyítékokat vagy sem. Továbbá javítja a jogbiztonságot is a vállalkozások és szolgáltatók számára, mivel a jövőben az

elektronikus bizonyítékok közlésének elrendelésére vonatkozó azonos szabályokat kell majd alkalmazni valamennyi szolgáltatóra nézve. (Buono, 2018, 1-6.)

Az új határozatok mellett továbbra is nyitva állnak a hagyományos jogintézmények, így az igazságügyi együttműködés és a kölcsönös jogsegély. A rendelet a szankciókra vonatkozóan nem határoz meg konkrétumot, amennyiben a szolgáltatók nem teljesítik a határozatokat, tehát ennek részletes kidolgozását a tagállamokra bizza.

További kérdést vet fel, hogy az Egyesült Államokban elfogadták a Clarifying Lawful Overseas Use of Data (CLOUD) törvényt, amely kimondja, hogy „*az Egyesült Államokban székhellyel rendelkező szolgáltatónak meg kell őriznie és rendelkezésre kell bocsátania minden vezetékes és elektronikus tartalmat, amely egy ügyféllel vagy előfizetővel kapcsolatban keletkezett, amennyiben ezzel a szolgáltató rendelkezik, függetlenül attól, hogy az adott adatokat, információkat a szolgáltató az Egyesült Államok területén belül vagy azon kívül tárolja.*” (Daskal, 2018, 227-250.)

Végül a felhő alapú technológiai megoldásokra (cloud computing) szeretném felhívni a figyelmet, amelyek különösen nagy kihívást jelentenek a nyomozó hatóságok számára. Ennek a leggyakoribb formája a nyilvános felhőszolgáltatás, amely igénybevételenek az esetén a szolgáltatók a felhasználóknak csak az erőforráshoz, infrastruktúrához (pl. hálózatokat, szervereket) biztosítanak távoli hozzáférést az interneten keresztül. Ez általában egy decentralizált rendszer és világszerte elhelyezkedő több szerverre másolják a tartalmat, így ez lehet a felhasználóhoz a legközelebbi, vagy amely kevésbé leterhelt hálózatra tudja irányítani. Ennek az előnye, hogy a felhasználóknak nem kell a saját gépükön tárolniuk az adataikat, hanem egy megosztott, távoli tárhelyre tölthetik fel, amelyhez bárhonnán hozzáférhetnek, azonban az adatok pontos helye nem határozható meg ebben az esetben, ami elvezet a loss of (knowledge of) location problémaköréhez. Ugyanis kérdésként felmerül, hogy a szerver melyik országban található, illetve az adott pillanatban melyik szerveren érhető el az adat. Ez pedig azt jelenti a jelenlegi szabályozásra tekintettel, hogy nem tudják megállapítani, hogy melyik állam jogosult eljárni, azonban az új rendelet immár ezt a problémát orvosolná.

Ezentúl a felhőszolgáltatások különböző szolgáltatási modellt is magukban foglalhatnak (pl. szoftver, platform, infrastruktúra), így az adott szolgáltató esetén nehéz megállapítani, hogy a hatóságnak milyen típusú adatra kell a közlésre kötelező határozatot kiállítania (előfizetői, hozzáférési, tranzakciós vagy tartalmi). (Kleijssen - Perri, 2016, 158-159.)

A titkosítással kapcsolatos aktuális kérdések a büntetőeljárás során

A titkosításnak (encryption) – például jelszavas, kriptográfiai vagy egyéb titkosítást nyújtó szoftveres védelem – mindennapi használata elterjedt, ezért ezt már a bűnelkövetők is kihasználják. A különböző titkosítási megoldások a már bevett bűnüldöző technikák, módszerek alkalmazását is ellehetetlenítik. A privátszférát erősítő technológiákat (Kiss, 2013, 113.) gyakran rendelkezésüktől ellentétesen alkalmazzák. (Miskolczi – Szathmáry, 2019, 177-178.)

A titkosított eszközökkel és az azokon tárolt adatokkal pedig sok esetben a probléma az, hogy a tartalmuk nem ismerhető meg a nyomozó hatóságok számára, így a bizonyítás során sem tudják felhasználni ezeket. Mindez következik abból, hogy a legtöbb ország büntető eljárásjogában – így hazánkban is – a terhelt együttműködésén, illetve a helyszínen fellelhető és beszerzett bizonyítási eszközökön múlik sokszor a nyomozás sikere, mivel az önvádra kötelezés tilalma érvényesül a büntetőeljárás során. Ez azt jelenti a Be. 7. § (3) bekezdése szerint, senki sem kötelezhető arra, hogy önmagára nézve terhelő vallomást tegyen vagy önmaga ellen bizonyítékot szolgáltatson.

Azonban erre már van ellenpélda is, mert pár ország engedi a titkosítás feloldására való kötelezést, így a francia büntető törvénykönyv három, illetve minősített esetként öt évig terjedő szabadságvesztéssel fenyegeti azt, aki megtagadja a titkosítás feloldáshoz szükséges jelszó, kód átadását a hatóságnak, míg az Egyesült Királyságban két évig (Koops – Kosta, 2018, 894.). Belgiumban egy évig terjedő szabadságvesztéssel rendelik büntetni ezt. (Dornfeld, 2017, 248.) Felmerül a kérdés, hogy a terhelt esetében ez nem jelenti-e az önvádra kötelezés tilalmának a megsértését. A francia Legfelsőbb Bíróság döntése értelmében ez a rendelkezés alkotmányosnak tekinthető, mert a gyanúsítottat nem kötelezik ezzel magára nézve terhelő vallomásnak a megtételére, valamint az adat már tárolva van valahol, ami a gyanúsított akaratától függetlenül létezik. Belgiumban a bíróságok ítéletei között eltérések mutatkoznak, vannak olyan esetek, amikor a tilalom megsértéseként értékelték, míg mások összeegyeztethetőnek tartották a tisztességes eljárással. Ez a kérdés rendkívül aktuális és vitatott mind a szakirodalomban, mind a gyakorlatban is, vélhetően idő kérdése, hogy valamelyik ügy eljut egészen Strasbourgig, az Emberi Jogok Európai Bíróságához.

Ezzel szoros összefüggésben érdemes említést tenni azokról az esetekről is, amikor a felhasználó olyan titkosítást használ, ami nem egy jelszó vagy kód, hanem biometrikus adat (pl. ujjlenyomat, arcfelismerés, írisz), amely különösen megnehezítheti a nyomozó hatóságok helyzetét és az eljárás lefolytatását, mert egyre több eszköznél jelenik meg a digitális azonosításnak ezen formája,

például okostelefonoknál és laptopoknál már általánossá vált a használatuk és ezek köre folyamatosan bővül.

Az itt felvázolt problémát megoldva, példaként említendő Norvégia, mint első állam, amely a büntető eljárásjogában engedi a biometrikus titkosítás feloldását, vagyis a nyomozó hatóság jogosult elrendelni azt, hogy a terhelt a biometrikus azonosítással hozzáférést biztosítson az eszközökhöz vagy adatokhoz. Abban az esetben, ha ezt megtagadja, akkor – arányos mértékben – kényszert alkalmazhatnak vele szemben a védelem feloldásához (pl. az ujjnak a lenyomatolvasóhoz való helyezését). (Koops – Kosta, 2018, 894-895.) A kényszer alkalmazásához azonban az ügyészség engedélyére van szükség, amennyiben a késelem a nyomozást veszélyezteti, akkor a rendőrség mérlegelheti a helyszínen és dönthet erre vonatkozóan, amit később az ügyészségnek kell átadni.

Az Európai Emberi Jogok Bíróságának *Saunders v. United Kingdom* döntésében a gyanúsított önvádolás alóli mentességének és a hallgatás jogának a kérdéseit vizsgálta részletesen. A Bíróság kimondta, hogy ezen jogokat azonban nem lehet kiterjesztően értelmezni: a nyomozó hatóság megszerezhet a terhelttől – a kényszerítő erő elfogadható használatával – olyan tárgyakat és anyagokat, amelyek a terhelt akaratától függetlenül léteznek, ilyen például egy dokumentum, a lehelet, a vér és vizelet minta, valamint a testi szövetminta (pl. DNS teszt céljából). Mindezekre tekintettel a norvég jogalkotók azon az állásponton vannak, hogy a kikényszerített biometrikus hitelesítés az önvádra kötelezés tilalmát nem sérti, mert a terhelttel szemben valamely testi jellemzőjét használják fel, ami a gyanúsított akaratától független, és nem kell önmagát terhelő bizonyítékot szolgáltatnia. Ez azt a célt szolgálja, hogy a nyomozó hatóság olyan információkhoz férjen hozzá – a fizikai-technikai akadályt leküzdve –, amelyre már törvényes alapjuk van a lefoglalás körében. Ezzel szemben a terheltet nem kényszeríthetik a jelszó vagy kód megadására. Valószínű, hogy ez esetben a bűnelkövetők a jelszavas védelmet fogják előnyben részesíteni az ujjlenyomattal szemben, mert utóbbit kikényszerítheti a nyomozó hatóság, míg előbbit nem. (Bruce, 2017, 26-30.)

Felhasznált irodalom

- Bruce, I. (2017): *Forced biometric authentication – on a recent amendment in the Norwegian Code of Criminal Procedure*. Digital Evidence and Electronic Sigranute Law Review, 14, 26-30.
- Buono, L. (2018): *The genesis of the European Union's new proposed legal instrument(s) on e-evidence – Towards the EU Production and Preservation Orders*. Era Forum, 2018 September 9. 1-6.
- Casey, E. (2012): *Digital Evidence and Computer Crime*. Amsterdam: Elsevier, 840.

- Council of Europe (2013): *Electronic evidence guide – A basic guide for police officers, prosecutors and judges*.
- Cybercrime Convention Committee (2018): *Conditions for obtaining subscriber information in relation to dynamic versus static IP addresses: overview of relevant court decisions and developments*. 1-25.
- Czine Á. (2018): *L. fejezet – A lefoglalás*. In: Belegi J. (szerk.): *Büntetőeljárás jog I-II. – új Be. – Kommentár a gyakorlat számára*. Budapest: HVG-ORAC Lap- és Könyvkiadó Kft. HVG-ORAC Jogkódex
- Daskal, J. (2018): *Microsoft Ireland, The CLOUD Act, and International Lawmaking 2.0*. Stanford Law Review Online, 9. <https://www.stanfordlawreview.org/online/microsoft-ireland-cloud-act-international-lawmaking-2-0/>
- Daskal, J. (2018): *Unpacking the CLOUD Act*. *Eucrim*, 4, 220-224.
- Dornfeld L. (2017): *Az elektronikus bizonyítékszerzés egyes kérdései*. *Kriminológiai Közlemények*, 77, 241-256.
- Dornfeld L. (2018): *A kibertérben elkövetett bűncselekményekkel összefüggésben alkalmazható kényszerintézkedések*. *Belügyi Szemle*, 2, 115-135.
- Elek B. (2014): *Informatikus szakértés a büntetőeljárásban*. *Belügyi Szemle*, 7–8, 158-180.
- ENISA (2014): *Electronic evidence – a basic guide for first responders*.
- Fenyvesi Cs. (2014): *Az új generációs bizonyítékok a kriminalisztika történeti mérföldköveinek tükrében*. *Magyar Jog*, 7-8, 433-443.
- Fenyvesi Cs. (2019): *Kriminalisztikai világtendenciák – Különös tekintettel a digitális felderítésre*. In: Mezei K. (szerk.): *A bűnügyi tudományok és az informatika*. Budapest-Pécs: MTA Társadalomtudományi Kutatóközpont PTE ÁJK, 64-82.
- Franssen, V. (2017): *The Belgian Internet Investigatory Powers Act – A Model to Pursue at European Level?* *European Data Protection Law Review*, 3, 534-542.
- Franssen, V. (2018): *The European Commission's E-Evidence Proposal: Toward an EU-Wide Obligation for Service Providers to Cooperate with Law Enforcement?* *European Law Blog*, 10. <https://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/>
- Furneaux, N. (2018): *Investigating cryptocurrencies – Understanding, extracting and analyzing blockchain evidence*. Wiley, 320.
- Herke Cs. (2019): *A digitalizáció szerepe a büntetőeljárásban*. In: Mezei K. (szerk.): *A bűnügyi tudományok és az informatika*. Budapest-Pécs: MTA Társadalomtudományi Kutatóközpont - PTE ÁJK, 104-124.
- Keles, M.-. H. (2015): *Computer Forensics: Cybercriminals, Laws and Evidence*. Second Edition, Jones & Bartlett Learning, 408.
- Kiss A. (2013): *A privátszférát erősítő technológiák*. *Infokommunikáció és Jog*, 3, 113-120.
- Kleijssen, J. – Perri, P. (2016): *Cybercrime, Evidence and Territoriality: Issues and Options*. In: Kuijter M. – Werned, W. (eds.): *Netherlands Yearbook of International Law*, 147-173.

- Koops, B.-J. – Kosta, E. (2018): *Looking for some light through the lens of “cryptowar” history: Policy options for law enforcement authorities against “going dark”*. Computer Law & Security Review, 4, 890-900.
- Laczi B. (2011): *A számítógépes környezetben elkövetett bűncselekmények nyomozásának és a nyomozás felügyeletének speciális kérdései*. Magyar Jog, 12, 726-738.
- Matus M. (2004): *Kutatás, lefoglalás, bűnjelkezelés számítástechnikai környezetben*. In: Bócz E. (szerk.): *Kriminálisztika*. Budapest: BM Duna Palota és Kiadó, 1160.
- Miskolczi B. – Szathmáry Z. (2019): *Büntetőjogi kérdések az információk korában*. Budapest: HVG-ORAC Lap- és Könyvkiadó Kft, 224.
- Parti K. (2004): *Gondolatok a szerver-lefoglalásokról*. Infokommunikáció és Jog, 3, 97-101.
- Peszleg T. (2005): *Interneten, számítógépen történő nyomrögzítés*. Ügyészek Lapja, 1, 25-40.
- Scientific Working Groups on Digital Evidence and Imaging Technology (2016): *Digital & Multimedia Evidence Glossary*, 7.
- Sorbán K. (2016): *A digitális bizonyítékok a büntetőeljáráásban*. Belügyi Szemle, 11, 81-96.
- Szabó I. (2011): *A számítástechnikai adat, mint elektronikus bizonyíték – A magyar szabályozás elemzése az Európa Tanács számítástechnikai bűnözésről szóló egyezménye alapján*. Kriminológiai Tanulmányok, 48, 13-28.
- Szathmáry Z. (2015): *Az elektronikus pénz és a bitcoin biztosítása a büntetőeljáráásban*. Magyar Jog, 11, 639-648.
- Tosza, S. (2018): *The European Commission’s Proposal on Cross-Border Access to E-evidence*. Eucriam, 4, 212-219.
- Trócsányi S. (2009): *Első oldal*. Infokommunikáció és jog, 6, 1.
- U.S. Department of Justice (2009): *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Law*.
- Vadász V. (2010): *A számítógép demisztifikálása*. Ügyészek Lapja, 2, 3-21.
- Wang, S.-J. (2007): *Measures of retaining digital evidence to prosecute computer-based cyber-crimes*. Computer Standards & Interfaces, 29, 216-223.

A cikkben szereplő online hivatkozások

- URL1: Az adatvédelmi biztos beszámolója, 2009. www.naih.hu/files/Adatvedelmi-biztos-beszamolaja-2009.pdf
- URL2: <https://www.ethnews.com/two-more-years-in-prison-for-ex-secret-service-agent-who-stole-government-seized-bitcoin>
- URL3: http://europa.eu/rapid/press-release_MEMO-18-3345_en.htm
- URL4: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN>
- URL5: http://europa.eu/rapid/press-release_IP-18-3343_hu.htm
- URL6: <https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52018PC0226>