DR. DORNFELD LÁSZLÓ

AZ ELEKTRONIKUS BIZONYÍTÉKSZERZÉS AKTUÁLIS KÉRDÉSEI[1,2*]

Bevezetés

Napjainkra nyilvánvalóvá vált, hogy a digitális forradalom következtében számos merőben új kihívásra kell választ adni. Különösen igaz ez állami szinten, hiszen mind a nemzeti, mind a nemzetközi jogban felmerült az igény az új élethelyzetekre alkalmazható szabályok megalkotására. A felgyorsult világban ennek kimunkálását azonban nem lehetett az organikus fejlődésre bízni; a jogalkotói megoldások sokszor erőltetettek vagy egyenesen ellentétesek a megalkotásuk céljával. Ez hangsúlyosan igaz a kiberbiztonság területén, hiszen ennek biztosítása ma már az államok működésének alapfeltétele.[3]

A kiberfenyegetések kapcsán a nagy államok jelentős többsége elsődlegesen a kibervédelemre fókuszál, míg a kiberbűnözés elleni küzdelmet csupán pár állam tekinti prioritásnak.[4] A kritikus infrastruktúra védelme valóban kiemelkedő fontosságúnak tűnik, azonban még a legmagasabb szintű védelemben is lehet hibát találni. Ez látható abból is, ahogy 2010-ben a Stuxnet névre keresztelt kártevő súlyos károkat volt képes okozni az iráni urándúsító centrifugákban. Bár nagy a valószínűsége, hogy ez egy amerikai–izraeli titkosszolgálati akció volt, a szervezett bűnözői csoportok támadókapacitása is folyamatosan erősödik, így az államoknak eszközre van szükségük ahhoz, hogy aktívan felléphessenek saját vagy állampolgáraik védelmében.[5]

---

[1] Az előadás elhangzott a Magyar Kriminológiai Társaság Kriminológia és Bűnügyi Tudományok PhD Szekciója által szervezett „Új kutatási területek a kriminológiában" című konferencián, 2016. október 14-én.

[2*] Szeretnék köszönetet mondani témavezetőmnek, Prof. Dr. Róth Erika egyetemi tanárnak a lektorálásért

[3] Jól mutatja ezt, ahogy Észtország működése gyakorlatilag megbénult a 2007-ben oroszpárti hackertámadások következtében. Eric Talbot Jensen: *Cyber Sovereignty: The Way Ahead*. The Texas International Law Journal, 50/2. sz., 276. o.

[4] Avner Levin – Daria Ilkina: *International Comparison of Cyber Crime*. Ryerson University, 2013. Online: http://www.ryerson.ca/tedrogersschool/privacy/documents/Ryerson_International_Comparison_ofCyber_Crime_-March2013.pdf (Letöltés ideje: 2016. 11. 12.) 35. o.

[5] Bővebben a Stuxnet kapcsán lásd: Dornfeld László: *A kibertér főbb nemzetközi és nemzeti szabályozásai*. In: Pintér István (szerk.): A virtuális tér geopolitikája. Geopolitikai Tanács Műhelytanulmányok, 2016/1. Budapest: Geopolitikai Tanács. 58–59. o.

Az elektronikus bizonyítékgyűjtés kiemelkedő jelentőségű eszköz a fenti cél elérésében, hiszen a kibertérben elkövetett bűncselekmények esetén az ott tárolt adatok segítségével lehet megtalálni az elkövetőt, és később a bíróság előtt bűnösségét bizonyítani. Tanulmányomban az ezzel kapcsolatos legfontosabb kérdésekkel fogok foglalkozni a hazai, uniós és bizonyos más országokban létező szabályozásuk tükrében.

Elektronikus adat, mint bizonyíték

A kibertér megjelenésével számos új bűncselekmény is elterjedt, amely kizárólag az új vívmányok sajátosságait használja ki (pl. hackelés, botnetek). Bizonyos területeken – így például a gazdasági bűncselekményeknél – a korábban is létező bűncselekmények informatikai eszközök segítségével történő elkövetése egyre elterjedtebbé válik. Ebben nagy szerepet játszik az, hogy a gazdasági életben központi szerepet tölt be az információs technológia, valamint az is, hogy az elkövetők számára ezen vívmányok igénybevétele egyszerűsíti az elkövetést, és csökkenti a lebukás veszélyét.[6] Végül pedig olyan bűncselekmények esetén is létezhetnek elektronikus bizonyítékok, amelyek elkövetésére a fizikai térben kerül sor (pl. emberrablás részleteit taglaló e-mail). Az első két körbe tartozó bűncselekmények esetén kiemelkedően nagy szerepük van az elektronikus adatoknak, amelyek bizonyítékokként használhatók.

Az elektronikus bizonyíték leggyakoribb meghatározása szerint minden olyan bizonyító erővel bíró adat, amelyet digitális formában tárolnak, feldolgoznak vagy továbbítanak.[7] A definíció legnagyobb problémája, hogy nem tesz eleget a technológiasemlegesség követelményének: bár napjainkban a digitális számítógépek elterjedtek, elképzelhető, hogy a jövőben nem digitális megfelelőiket is szélesebb körben használni kezdik. Egy másik, általánosabb definíció szerint ide sorolható minden olyan bizonyító erővel bíró adat vagy információ, amelyet számítógép segítségével tárolnak vagy továbbítanak.[8] Itt viszont azt lehet kifogásolni, hogy a definíció nem tartalmazza a mobil kommunikációs eszközöket.

A meghatározásokban szereplő adatok fizikailag nem léteznek, ezért valamilyen módon megjeleníthetővé kell tenni őket, és a nyomozás során a rögzítésükhöz és felhasználásukhoz külön eszközök szükségesek. Tulajdonságaiból kifolyólag az adat nagyon sérülékeny, könnyen manipulálható, elrejthető vagy megsemmisíthető, így a nyomozóhatóságnak nagy körültekin-

---

[6] Silvia Signorato: *ICT, Data Retention, and Criminal Investigations of Economic Crimes*. Journal of Eastern European Criminal Law, 2015/2. sz. 204–205. o.

[7] Antonela Gropeneanu – Adrian Iacob: Investigative issues regarding cybercrime. European Journal of Public Order and National Security 10. o.

[8] Eoghan Casey: *Foundations of Digital Forensics*. In: Eoghan Casey (ed.) Digital Evidence and Computer Crime. USA: Academic Press. 7. o.

téssel kell eljárnia, hogy a bizonyítás során is használható módon szerezze meg.[9] Fontos tényező még – ahogy a Tanács 14369/15. sz. feljegyzése rámutat –, hogy az elektronikus bizonyíték természeténél fogva rövid életű, és számos olyan eszköz létezik, amely nehezíti a beszerzését.

Felmerül azonban a kérdés, hogy a megszerzett elektronikus adat milyen módon értékelhető a bizonyítás során. Hatályos büntetőeljárási törvényünk (1998. évi XIX. törvény, a továbbiakban Be.) ugyanis nem tartalmazza azt a bizonyítási eszközök között. A szakirodalom eltérő álláspontokat alakított ezzel kapcsolatban, így például Laczi álláspontja alapján az adathordozó tárgyi bizonyítási eszköznek minősülhet, illetve bizonyos esetekben az adat okiratként is értékelhető.[10] Az új Be. társadalmi vitára bocsátott tervezete (a továbbiakban: Tervezet)[11] már különálló bizonyítási eszközként tartalmazza az elektronikus adatot. A 200. szakasz határozza meg a fogalmát, eszerint ide értendő az információs rendszerben tárolt, kezelt, feldolgozott vagy továbbított 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.

Joghatóság és bűnügyi együttműködés

A joghatóság megállapítását segítő tényezők

A büntetőeljárás megindításának és lefolytatásának egyik feltétele, hogy az adott ügy az állam joghatósága alá tartozzon. A Be. 6. § (3a) kimondja, hogy joghatóság hiányában eljárás nem indítható, vagy pedig meg kell szüntetni. A kibertér sajátosságai miatt sokszor nehéz lehet eldönteni, hogy a joghatóság fennáll-e az adott bűncselekmény vonatkozásában. Könnyedén elképzelhető ugyanis olyan helyzet, hogy amellett, hogy a terhelt és a sértett más-más országban él, a bűncselekmény által érintett információs eszköz (pl. e-mailszerver) harmadik országban található. Tovább bonyolítja a helyzetet, amennyiben az elkövető valamilyen harmadik ország közbeiktatásával követi el a bűncselekményt. Ez joghatósági összeütközésekhez és párhuzamos eljárások megindításához vezethet a gyakorlatban.

---

[9] Antonela Gropeneanu – Adrian Iacob: i. m. 10. o., Shiuh-Jeng Wang: *Measures of retaining digital evidence to prosecute computer-based cyber-crimes*. Computer Standards & Interfaces, 2007/2. sz. 216. o.

[10] Laczi Beáta: *A számítógépes környezetben elkövetett bűncselekmények nyomozásának és a nyomozás felügyeletének speciális kérdései*. Magyar Jog, 20011/12. sz. 728–729. o.

[11] http://www.kormany.hu/download/e/ba/b0000/20160603%20El%C5%91terjeszt%C3%A9s%20a%20b%C3%BCntet%C5%91elj%C3%A1r%C3%A1sr%C3%B3l%20sz%C3%B3l%C3%B3%20t%C3%B6rv%C3%A9nyr%C5%91l.zip#!DocumentBrowse (Letöltés ideje: 2016. 11. 20.)

Az Európai Unió ide vonatkozó másodlagos jogforrásai tartalmaznak a joghatóság meghatározását elősegítő rendelkezéseket. Az információs rendszerek elleni támadásokról szóló 2005/222/IB kerethatározat[12] 10. cikke az általa szabályozott bűncselekmények körében állapítja meg a joghatóság fennállásának eseteit. Így eljárás indítható, ha a bűncselekményt egészben vagy részben a tagállam területén követték el, az elkövető az adott állam állampolgára vagy olyan jogi személy javára követték el, amelynek tevékenysége végzésének központja a tagállam területén található. A (4) bekezdés alapján ez egyúttal sorrendiséget is jelent annak eldöntése során, hogy több joghatósággal rendelkező állam között melyiknek kell lefolytatnia a büntetőeljárást. A kerethatározatot felváltó 2013/40/EU irányelv[13] 12. cikke már csak az elkövetés helyét, illetve az állampolgárságot tartalmazza, de lehetőséget ad a tagállamoknak, hogy megállapítsák joghatóságukat, ha a területükön található jogi személy javára történt az elkövetés, vagy pedig az elkövető szokásos tartózkodási helye a területükön van. Az irányelv már nem állapít meg sorrendiséget ezen joghatósági okok között.

Fontos azonban hangsúlyozni, hogy a két másodlagos uniós jogforrás csak az általuk szabályozott bűncselekmények esetére tartalmaz szabályokat. De még az ide tartozó esetekben is gondot jelenthet szövetségi államokon – pl. Németországon – belül annak eldöntése, hogy a büntetőeljárás szövetségi vagy tagállami szinten induljon-e meg. További súlyos problémákat okozhat, ha nem csak uniós, hanem harmadik államok valamelyike is érintett egy ügyben.

Bűnügyi együttműködés

Ha sikerült eldönteni a joghatóság kérdését és megindult az eljárás, máris újabb problémaként jelentkezik, hogy a bizonyítékok több különböző állam területén találhatók. Az eljárás jelentősen elhúzódhat ilyen esetekben, különösen, mert a hagyományos eszközök ilyenkor elégtelennek bizonyulhatnak.[14] A jogsegélykérelmek hosszadalmas teljesítése önmagában veszélyezteti a sikeres bizonyítást.[15] Mivel az államok a büntetőjogra a szuverenitásuk utolsó védőbástyájaként tekintenek, igen vonakodva közelítik csak vonatkozó szabályozásaikat, így a bizonyítékszerzésre vonatkozó eltérő sztenderdek és garanciák miatt korántsem biztos, hogy a más államban beszerzett adatok bizonyítékként felhasználhatók lesznek. Az Európai Unió két új

[12] A Tanács 2005/222/IB kerethatározata (2005. február 24.) az információs rendszerek elleni támadásokról. HL 2005 L 69, 2005.3.16. Átültetési határidő: 2007. március 16.

[13] Az Európai Parlament és a Tanács 2013/40/EU irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról. HL 2013 L 218., 2013.8.14. Átültetési határidő: 2015. szeptember 4.

[14] Parti Katalin: *Nyomozás az interneten: együttműködés – korlátokkal*. Belügyi Szemle, 2004/11–12. sz. 205. o.

[15] Laczi: i. m. 726. o.

eszközzel is igyekszik a bűnügyi együttműködés hatékonyságát növelni: egyrészt a közös minimumszabályok meghatározásával, másrészt a kölcsönös bizalom elvének az alkalmazásával.[16]

Az utóbbi körbe tartozó instrumentumok közül az első a 2003/577/IB kerethatározat[17] a bizonyítékok biztosítását teszi lehetővé, de hatálya csakis erre korlátozódik, a bizonyíték beszerzéséhez már a bűnügyi együttműködés más formáit kell igénybe venni. Így egy kétlépéses eljárási rend alakult ki, ami nemcsak az együttműködés hatékonyságát rontja, de a gyakorlati alkalmazására való hajlandóságot is. Az európai bizonyításfelvételi parancsról szóló 2008/978/IB kerethatározat[18] azzal a céllal született, hogy felváltsa az addig meglévő, kölcsönös jogsegélyen alapuló eszközök helyét, de erre annak hiányosságai miatt – például, hogy nem terjed ki hatálya minden bizonyítékra, és csak a már meglévő bizonyítékok beszerzésére használható – mégsem került sor.[19]

Az Unió ismételten hasonló reményeket fűz az európai nyomozási határozathoz, amelynek szabályait a büntetőügyekben kibocsátott európai nyomozási határozatról szóló 2014/41/EU irányelv[20] tartalmazza. Ez felváltja a bűnügyi együttműködést szabályozó korábbi uniós instrumentumokat, kibocsátására a bíróság, ügyészség és nyomozóhatóság jogosult, de a terhelt védője is indítványozhatja azt. A hozzá tartozó formanyomtatvány egyszerűsíti, a megszabott határidők pedig gyorsítják a határokon átnyúló bizonyítékgyűjtést. Előnyének tekinthető az is, hogy bizonyos bűncselekményi kör esetén – melybe a számítástechnikai bűnözés is beletartozik – nem szükséges a kettős büntethetőség fennállását vizsgálni.[21] A Tanács 14369/15. sz. feljegyzése rámutat, hogy a kiberbűncselekmények nyomozása során az elektronikus bizonyítékok beszerzését nagyban könnyíteni fogja az instrumentum. A sikerével kapcsolatos kilátások azonban nem ilyen egyértelműek, számos kritika hozható fel a megoldásai kapcsán. Így például az, hogy a kölcsönös elismerés elvét a versenyjogra találták ki, és a büntetőügyekben történő alkalmazása olyan szintű bizalmat igényel a tagállamok között, amely jelenleg nincs

[16] Láris Liliána: *Az Európai Nyomozási Határozat*. Ügyészek lapja, 2015/1. sz. 87–88. o.

[17] A Tanács 2003/577/IB kerethatározata (2003. július 22.) a vagyonnal vagy bizonyítékkal kapcsolatos biztosítási intézkedést elrendelő határozatoknak az Európai Unióban történő végrehajtásáról. HL 2003 L 196, 2003.8.2. Átültetési határidő: 2005. augusztus 2.

[18] A Tanács 2008/978/IB kerethatározata (2008. december 18.) a büntetőeljárások során felhasználandó tárgyak, dokumentumok és adatok megszerzéséhez szükséges európai bizonyításfelvételi parancsról. HL 2008 L 350, 2008.12.30. Átültetési határidő: 2011. január 19.

[19] Jánosi Andrea: *Az európai nyomozási határozat előzményei és vívmányai*. In: Hallók Tamás (szerk.) Publicationes Universitatis Miskolcinensis Sectio Juridica et Politica Tomus XXXIII. Miskolc: Miskolc University Press, 213–215. o.

[20] Az Európai Parlament és a Tanács 2014/41/EU irányelve (2014. április 3.) a büntetőügyekben kibocsátott európai nyomozási határozatról. HL 2014 L 130, 2014.5.1. Átültetési határidő: 2017. május 22.

[21] Jánosi: i. m. 216–217. o., Láris: i. m. 89–93. o.

meg.[22] Láris pedig egyek mellett rámutat arra is, hogy míg nem születik több uniós közös minimumszabály, addig nem lehet garantálni, hogy az európai nyomozási határozat eléri célját.[23] Ráadásul sok esetben az sem világos, egy adott adatot tartalmazó szerver pontosan melyik ország joga alá is tartozik, különösen, ha azt felhőszolgáltatás segítségével tárolják a világhálón.[24]

Az anonimizáció és az azonosítás nehézsége

Az internetszolgáltatók a hálózatra felcsatlakozó felhasználók számára IP címet osztanak ki, amely alapján azonosítani lehet őket. A jelenleg használt 4. verzióban (IPv4) a kiosztható címek száma 4,3 milliárdra korlátozódik, ami a használatban lévő eszközök számát tekintve nem elegendő, ezért a szolgáltatók dinamikusan osztják ki az IP címeket. Ez a gyakorlatban azt jelenti, hogy az IP-k eltérő időpontban eltérő felhasználókat jelölnek. A nyomozóhatóságnak ezért úgy kell kikérnie az adatokat az internetszolgáltatótól, hogy az a bűncselekmény elkövetésének időpontjára vonatkozzon. A problémára technikai megoldást kínál az IPv6-ra történő átállás, hiszen itt már 50 billiárd IP cím válik kioszthatóvá. Ez a folyamat azonban a tervezettnél máris hosszabb időt vesz igénybe, és egyelőre bizonytalan az időpontja. Ráadásul az átmeneti időszakban a két verzió párhuzamosan működik, ami további komplikációkat jelenthet egy büntetőeljárás során.[25]

Problémát jelent még a szolgáltató-szintű hálózati címfordítás (*Carrier-grade network address translation*, CGN) is. Ekkor az internetszolgáltató előfizetői egyetlen IP cím alatt jelennek meg, és annak 65535 portjának valamelyikén keresztül kommunikálnak. A nyomozóhatóságnak ilyenkor már nem csak az IP címet, és az elkövetés idejét, de a kiinduló- és célportokat is ismernie kell. Mivel a szolgáltatók gyakran nem őrzik meg az ezzel kapcsolatos naplókat, sokszor lehetetlenné válik a felhasználó azonosítása.[26]

Azonban súlyosabb gondot jelent az, hogy a felhasználók bárhol hozzáférhető és használható eszközökkel, illetve bizonyos módszerekkel könnyen képesek elfedni a saját nyomaikat. Az

---

[22] Alföldi Ágnes Dóra: *A bűnügyi együttműködés általános kérdései az Európai Unióban*. Európai Jog, 2011/2. sz. 15. o.

[23] Láris: i. m. 93–94. o.

[24] Erről bővebben lásd: TCY(2016)5 *Criminal justice access to data in the cloud challenges.* Council of Europe, 2015. május 25. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e (Letöltés ideje: 2016. november 16.), 22. o.

[25] TCY (2016)5 22. o.

[26] TCY(2016)5 22. o.; Philippe van Linthout: *Significant legal and technical challenges in combating cybercrime for legal practitioners* című előadása a 2016. május 10-11-én Dublinban megtartott Fighting Cybercrime: Between Legal Challenges and Practical Difficulties című konferencián Online: https://files.era.int/f/e66ddf8d8b/ (Letöltés ideje: 2016. 11. 20.)

anonimitás igénye a kibertér jellegéből fakad, ahol a kommunikáció főszabályként ilyen módon folyik (az IP címek és a felhasználók összekapcsolására csak az internetszolgáltatók képesek). Az anonimitásnak ugyanakkor társadalmi gyökerei is vannak, és összességében egy igen komplex problémát jelent, amelynek részletes tárgyalása túlmutat jelen tanulmány keretein.[27]

Az eszközök terén ide sorolhatók a proxy szerverek, illetve a virtuális magánhálózatok (VPN), amelyek segítségével a felhasználó könnyedén kaphat a világ bármely más országába mutató IP címet. Ilyen eszköz még az Amerikai Egyesült Államok által katonai célokra kifejlesztett TOR (The Onion Router), amely igen nehezen feltörhető titkosítási módszerrel védi a kommunikáció tartalmát. 2013-ban a Snowden-ügy kapcsán kiderült, hogy az amerikai Nemzetbiztonsági Ügynökség (National Security Agency, NSA) 2013-ban sikerrel azonosított több TOR segítségével kommunikáló felhasználót is különféle hibák kiaknázásával.[28] Ennek bűnüldözési célú felhasználása azonban egyelőre elég kétséges, főleg, mivel a sikerhez vagy felhasználói hibára vagy sok száz órányi befektetett munkára volt szükség. Szervezettebb támadásokra kínálnak lehetőséget az ún. botnetek, vagyis vírussal fertőzött számítógépek hálózatai, amelyeket egyszerre irányítanak a távolból. Az ilyen számítógépek a külső szemlélődő számára nem tűnnek fertőzöttnek, és továbbra is betöltik eredeti funkciójukat.[29] A 2013/40/EU irányelv 7. cikke a botnetek előállítását, árusítását, használtra beszerzését is büntetni rendeli.

A különböző eszközökön túl bizonyos módszerek is megnehezíthetik a nyomozóhatóság dolgát. Így például az, ha az elkövető egy nyilvános hotspoton át kapcsolódik a világhálóra, vagy pedig egy nem kódolt wifi segítségével. Utóbbi esetén a gyanú szinte azonnal a router rendes használójára terelődik, és ezután már az is kétségessé válhat, hogy kizárható-e egyáltalán végleg a gyanúsításból az illető.[30] Az anonimizáció kapcsán felmerülő problémákra még nem született megfelelő számítástechnikai vagy jogi megoldás.

---

[27] Bővebben lásd: Vincenzo Zeno-Zencovich: *Anonim véleménynyilvánítás az interneten*. In Medias Red 2014/2. sz. 290–303. o.

[28] Bruce Schneier: *Attacking Tor: how the NSA targets users' online anonymity*. The Guardian, 2013. október 4. Online: http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity (Letöltés ideje: 2013. 10. 09.)

[29] Wystke van der Wagen – Wolter Pieters: *From Cybercrime to Cyborg Crime: Botnets as Hybrid Criminal Actor-networks*. The British Journal of Criminology 2015/3. sz., 578–581. o.

[30] Laczi: i. m. 726. o.

Titkosítás és önvádra kötelezés tilalma

A titkosítás a mindennapi internethasználat része, azonban mint más tényezőket, ezt is felhasználhatják az elkövetők saját nyomaik leplezésére. Philippe van Linthout belga vizsgálóbíró dublini előadásában érintette ezt a kérdést is. A titkosított adatok nem megismerhetők a nyomozóhatóság számára, így a bizonyításban sem használhatók fel. A modern titkosítások többsége „*brute force*" technikával (a lehetséges kombinációk végigpróbálgatása) nem törhető fel, mivel igen hatalmas számú variáció képzelhető el.[31] Éppen ezért több országban is születtek olyan törvények, amelyek kötelezik a tikosítót arra, hogy szüntesse meg az adatai titkosítását. A belga büntetőtörvénykönyv egy, míg a francia kódex 434-15-2. szakasza három, illetve minősített esetben öt évig terjedő szabadságvesztéssel rendeli büntetni azt, aki megtagadja a feloldáshoz szükséges jelszó átadását a hatóságoknak. Ezek a rendelkezések a terheltre is vonatkoznak, ami felveti az önvádra kötelezés tilalmának megsértését is.

Linthout szerint a rendelkezés támogatói az ittas vezetéshez hasonlítják a fennálló helyzetet: az intézkedés alá vont sofőr sem tagadhatja meg, hogy alávesse magát a hatósági intézkedésnek. Ez a kötelezés sem jelent azonban egyértelmű megoldást: bizonyos programok, így például a VeraCrypt nevű program már képes úgy titkosítani adatokat, hogy maga a felhasználó sem ismeri az azt feloldó jelszót. Rainer Franosch hesseni „rangidős" ügyész (Oberstaatsanwalt) előadta,[32] hogy a tartományban éppen ezért kialakult az a gyakorlat, hogy amennyiben félő, hogy a gyanúsított titkosítja a számítógépe tartalmát, kommandósok váratlan rajtaütéssel biztosítják a bizonyítékok hozzáférhetőségét.

A kérdés az Amerikai Egyesült Államokban is felmerült, itt az Alkotmány ötödik kiegészítésébe ütközését illetően folynak a viták. 2007-ben Sebastian Boucher gyermekpornográfia birtoklásával kapcsolatos ügyében (In re Boucher, No. 2:06-mJ-91, 2009 WL 424718) a szövetségi kerületi bíróság úgy ítélte meg, hogy az ötödik kiegészítésbe ütközne, amennyiben a vádlottat kötelezik a kód megadására, ugyanis azzal beismerné, hogy rendelkezik a gépen tárolt fájlok felett. Brenner szerint ugyanakkor más lenne a helyzet megítélése, amennyiben a kódot a terhelt egy naplófájlba mentette volna le. Ennek felhasználása ugyanis nem tekinthető vallomásnak, így nem esik az ötödik kiegészítés védelme alá.[33] 2009-ben Sessions bíró megváltoztatta a magisztrátusi bíró döntését, és kötelezte Bouchert a jelszó átadására, arra hivatkozva, hogy az eljárás elején már megmutatta gépe tartalmának egy részét a hatóságoknak, így ez nem tekinthető önvádra

[31] 256 bites kódolásnál ez 2^{256} lehetséges kombinációt jelent

[32] Rainer Franosh: *Investing and prosecuting cybercrimes in the framework of European (and international) legal instruments: challanges faced by prosecutors*. Online: https://files.era.int/f/e66ddf8d8b/ (Letöltés ideje: 2016. 11. 20.)

[33] Susan W. Brenner: *Cybercrime Law – A United States Perspective*. In: Eoghan Casey. Digital Evidence and Computer Crime. USA: Academic Press. 115–118. o.

kötelezésnek.[34] 2012-ben a United States v. Fricosu ügyben a kerületi bíróság arra kötelezte a terheltet, hogy a titkosítással védett számítógépen található fájlok másolatát adja át a hatóságoknak.[35] Széles körben ismertté vált az az eset, amikor az FBI felszólította az Apple-t arra, hogy egy terrorista iPhone-jának titkosítását oldja fel, hogy azon keresztül hozzáférhessenek a felhőben tárolt fájljaihoz, az Apple azonban ezt megtagadta. Ian Walden professzor előadása[36] szerint a helyzet elkerülhető lett volna, ha a hatóságok rögtön a felhőhöz kérnek hozzáférést a cégtől.

2016-ban hazánkban a terrorellenes intézkedések között felmerült a titkosított kommunikáció teljes tilalma, amely azonban alapjában lehetetlenítené el az internet gazdasági célú felhasználását is (elég csak a netbanki szolgáltatások használatára gondolni). Az eredeti jogalkotói szándék lényeges változásának eredményeként megszületett a titkosított kommunikációt biztosító alkalmazásszolgáltatók és a titkos információgyűjtésre feljogosított szervezetek együttműködésének rendjéről szóló 185/2016. (VII. 13.) Kormányrendelet, amely előírta, hogy alkalmazásszolgáltatóknak, hogy nem hajthatnak végre olyan fejlesztéseket, amelyek a titkos információgyűjtést kizárják vagy ellehetetlenítik. Ennek hatásai ugyanakkor kétségek, hiszen az elkövetők számos külföldi fejlesztésű eszközt beszerezhetnek, amelyek fejlesztőire ezek a rendelkezések nem vonatkoznak.

Adatmegőrzés

Az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezménye[37] meghatározása alapján a forgalmi adat minden olyan, a számítástechnikai rendszeren átmenő és a számítástechnikai rendszer, mint a kommunikációs lánc egyik eleme által létrehozott kommunikációra vonatkozó adat, mely jelzi a kommunikáció eredetét, rendeltetési helyét, útvonalát, idejét, napját, terjedelmét és időtartamát vagy a szolgáltatás típusát. Az ilyen információknak különösen fontos szerepe lehet a büntetőeljárás során, hiszen fizikai nyomok – mint például az ujjlenyomat – híján ez vezethet el a bűncselekmény elkövetőjéhez. Az eljárás sikere szempontjából tehát alapvető fontosságú, hogy ezek az adatok elérhetők legyenek, különös tekintettel arra, hogy akár hónapok is eltelhetnek egy kiberbűncselekmény elkövetése és annak észlelése között (pl. adatlopás esetén).

---

[34] William K. Sessions: Memorandum of Decision. Online: http://volokh.com/files/BoucherDCT.1.pdf (Letöltés ideje: 2016. 11. 19.)

[35] Nicholas Soares: *The Right to Remain Encrypted: The Self-Incrimination Doctrine in the Digital Age*. American Criminal Law Review, 2012/4. sz., 2002. o.

[36] Ian Walden: *International Cybercrimes and Investigations.* Online: https://files.era.int/f/e66ddf8d8b/ (Letöltés ideje: 2016. 11. 20.)

[37] Kihirdette a 2004. évi LXXIX. törvény

A forgalmi adatok megőrzésére kötelezés minden személy kommunikációját érinti, bármiféle egyéb követelmény nélkül. Kötelezettjei az internetszolgáltatók, akik piaci szereplők, nem pedig állami szervek, és ezért egy rosszul kidolgozott szabályozás súlyos anyagi következményekkel járhat számukra. Visszautalva a joghatósággal foglalkozó fejezetre, az adatmegőrzés egyik problémáját is az jelenti, hogy még az egy államon belüli kommunikáció esetén sem biztos, hogy az annak adatait tároló internetszolgáltató székhelye az adott államban található.[38] A forgalmi adatoknak alapvetően három formáját különböztethetjük meg: a kommunikáció tartalmára, jellemzőire és az előfizetőre vonatkozó adatokat.[39]

Az Európai Unió is igyekezett válaszolni a kihívásra, és elfogadta a 2006/24/EK irányelvet,[40] amely előírta a hírközlési szolgáltatásnyújtók számára, hogy mely adatokat kötelesek megőrizni. Deklarált cél volt, hogy ezek súlyos bűncselekmények kivizsgálása, felderítése és üldözése céljából elérhetők legyenek. Az ötödik cikk alapján a kötelezettség a kommunikációs jellemzőkkel kapcsolatos, valamint az előfizetői adatokra vonatkozik, míg a tartalmi adatokra nem. Azt az időtartamot, amíg az adatok megőrzésére kötelezhető a szolgáltató, a közléstől számított 6–24 hónapos időszakban határozta meg, valamint előírta, hogy kérelemre az adatokat az illetékes hatóságok számára haladéktalanul továbbítani kell.

Az irányelv elfogadását jelentős jogi manőverezések előzték meg. Így 2005-ben az Európai Parlament jelentésében kritizálta a Tanács tervezetét, és amellett érvelt, hogy azt nem a harmadik pillért képező bel- és igazságügyi együttműködés, hanem a belső piacot szabályozó első pillér részeként kellene elfogadni. Ez egyúttal azt is jelentette, hogy a végső szabályozás kialakításába nem csak a Tanácsnak volt beleszólása, és a harmadik pillérrel kapcsolatos más intézményi korlátozásokkal sem kellett számolni.[41] A Tanács 2005-ös brit elnöksége idején meghozott döntésben szerepet játszott az a tény is, hogy így már nem egyhangú, hanem minősített többségi döntést kellett hozni, így elkerülhették a várható német vétót.[42] Ezek a politikai manőverek végül célt értek, és az instrumentumot az első pillér részeként fogadták el. Mindezek után nem meglepő, hogy Írország hibás jogalapra hivatkozással támadta meg az irányelvet az Európai Unió Bírósága előtt (C-301/06). Az ügyben 2009-ben született ítéletben a Bíróság elutasította a megsemmisítés iránti kérelmet.

---

[38] Signorato: i. m. 206–207. o.

[39] Ezek részletesebb meghatározását lásd: Szabó Imre: *A számítástechnikai adat mint elektronikus bizonyíték*. In: Virág György (szerk.) Kriminológiai tanulmányok. 48. kötet, 2011. 14–16. o.

[40] Az Európai Parlament és a Tanács 2006/24/EK irányelve (2006. március 15.) a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről s a 2002/58/EK irányelv módosításáról. HL 2006 L 105, 2006.4.13. Átültetési határidő: 2007. szeptember 15.

[41] A harmadik pillér működésével kapcsolatban lásd: Damian Chalmers – Gareth Davies – Giorgio Motti: *EU Criminal Law*. New York: Cambridge University Press, 2014. 583. o.

[42] Christian DeSimone: *Pitting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive*. German Law Journal, 2010/3. sz. 299–301. o.

Az irányelv átültetése azonban számos országban igen nehéznek bizonyult az alapjogokkal kapcsolatos kérdések miatt. Így például Németországban, Csehországban és Romániában az alkotmánybíróság megsemmisítette az instrumentumot implementáló rendelkezéseket (a Tanács egyik dokumentuma szerint összesen 9 tagállamban történt meg 2015-ig).[43] A döntésekben közös volt, hogy kiemelték az arányosság hiányát, annak pontos meghatározását, hogy mely szervek kérhetik a megőrzött adatok átadását, valamint a „súlyos bűncselekmények" részletesebb meghatározását.[44] Ezt követően két előzetes döntéshozatal iránti kérelem is érkezett a Bíróság elé, a Digital Rights Ireland és Seitlinger beadványával kapcsolatban, amiket egyesítve tárgyaltak (C-293/12. és C-594/12). 2014. április 8-i ítéletében a nagytanács érvénytelennek mondta ki az irányelvet, mivel az megsértette az Európai Unió alapjogi chartájának 7. (magánélethez való jog) és 8. (személyes adatok védelméhez való jog) cikkét, és az arányosság követelményét.[45]

A döntés következményei nem érintették közvetlenül az átültető jogszabályokat, amennyiben azt nemzeti bíróság vagy törvényhozás nem helyezte hatályon kívül, ugyanakkor konkrét kötelezettség már nincs ezek megtartására. A Tanács 2015. novemberi információi szerint tizenhat tagállamban – köztük hazánkban is –[46] hatályban maradtak az implementáló jogszabályok, míg az hatályon kívül helyezésre 10 országban került sor. Legalább hét törvényhozás új jogszabályokat alkotott az adatmegőrzés szabályozására. Az Eurojust jelentése szerint a tagállami szabályozások széttöredezettsége súlyos következményekkel járhat az elektronikus bizonyítékok gyűjtése, és a bűnügyi együttműködése terén.[47] A svéd és brit adatmegőrzési szabályozás kapcsán 2015-ben előzetes döntéshozatali eljárás indult a Bíróság előtt, az egyesített ügyben a Charta rendelkezéseinek fényében a szabályozás uniós jognak való megfelelése a kérdés (Tele2 Sverige AB és Watson és társai, C-203/15 és C-698/15).

Mindezek alapján mihamarabb szükséges egy új, a Bíróság megállapításainak, és különösen az arányosság elvének megfelelő szabályozás kidolgozása. Ebben különös tekintettel kell lenni a megfelelő garanciák beépítésére, amelyek garantálják, hogy nem történik visszaélés a személyes adatokkal. Egyúttal szükséges annak meghatározása is, hogy mely hatóságok férhetnek hozzá ezekhez az adatokhoz, és milyen esetekben.

---

[43] A Tanács 14677/15. sz. feljegyzése, 3. o.

[44] Signorato: i. m. 208. o.

[45] Chronowski Nóra: *Szabadság kontra biztonság – az Alapjogi Chartába ütközik az adatmegőrzési irányelv*. Magyar Tudományos Akadémia, http://hpops.tk.mta.hu/blog/2014/05/az-alapjogi-chartaba-utkozik-az-adatmegorzesi-iranyelv. (Letöltés ideje: 2016. november 14.)

[46] Az irányelv rendelkezéseit az elektronikus hírközlésről szóló 2003. évi C. törvénybe a 2007. évi CLXXIV. törvénnyel ültette át a magyar jogalkotó

[47] A Tanács 14677/15. sz. feljegyzése, 2–3. o.

Lefoglalás

Az elektronikus adatok sérülékenysége miatt a nyomozóhatóságnak különös gonddal kell eljárnia annak beszerzése során. Wang szerint három alapvető kritériumot kell a nyomozás során betartani: a bizonyíték beszerzésénél ne sérüljön vagy módosuljon az eredeti adat, bizonyítható legyen az egyezés az eredetivel, és a bizonyíték elemzése ne változtassa meg azt.[48] A lefoglalás a bizonyítékok biztosításának elsődleges módja, ennek megfelelően az elektronikus bizonyítékok esetén is fontos annak megfelelő alkalmazása.

A gyakorlatban azonban régóta felmerült több kérdés is, elsősorban azzal kapcsolatban, hogy mire is kell foganatosítani a kényszerintézkedést: magára az adatra vagy pedig az azt tartalmazó adathordozóra.[49] Régebben a nyomozóhatóság a számítógép egészét foglalta le, utóbb azonban már csak a merevlemezt, vagy pedig csak másolatot készített róla, miután a Be. lehetővé tette adatok lefoglalását is. Vadász Viktor ugyanakkor nem ért egyet az utóbbival, mivel egyrészt az elkövetés eszköze elkobzás alá esik, másrészt magából a merevlemezből nem nyerhető ki minden információ, amely fontos lehet az eljárás és a bizonyítás során.[50]

Ugyanakkor könnyedén belátható, hogy egy többek által használt számítógép hónapokra történő lefoglalása súlyos jogsértésekkel járhat. Mivel a Rendőrségről szóló 1994. évi XXXIV. törvény 90. szakasza előírja, hogy személyes adatok kezelését bűnüldözési célra azokra az adatokra kell korlátozni, amelyek tényleges veszély elhárításához, illetőleg meghatározott bűncselekmény megelőzéséhez, felderítéséhez, bizonyításához szükségesek, így felmerül a kérdés, hogy a rendőrség ezt hogy képes biztosítani. Az adatvédelmi biztos 2009-es állásfoglalásában úgy találta, hogy az eljáráshoz nem szükséges adatokhoz való hozzáférés csak ésszerű időtartamra korlátozható, és az ügyben felmerült fél éves lefoglalás már túlmutat ezen.[51]

A jogalkotó is felismerte, hogy nem minden esetben szükséges azonnal lefoglalni az adatokat tartalmazó információs rendszereket, mivel a bizonyítékok biztosítása más módon is megoldható. A Be. 158/A. szakasza szerinti információs rendszerben tárolt adatok megőrzésére kötelezés kényszerintézkedése pontosan ilyen alternatívát jelent. Ennek alkalmazásakor az adat birtokosát, feldolgozóját vagy kezelőjét kötelezik a büntetőeljáráshoz szükséges adatok megőrzésére, aki köteles együttműködni a nyomozóhatósággal a kényszerintézkedés időtartama alatt. Az elrendelését követően haladéktalanul meg kell kezdeni az adatok átvizsgálását, amire három hónap áll rendelkezésre. Ezt követően dönteni kell az adatok más adathordozóra átmásolásával történő lefoglalásáról vagy pedig a megőrzés megszüntetéséről.

---

[48] Wang: i. m. 218. o.

[49] Laczi: i. m. 730. o.

[50] Vadász Viktor: *A számítógép demisztifikálása*. Ügyészek Lapja, 2010/2. sz. 20. o.

[51] Trócsányi Sára: *Első oldal*. Infokommunikáció és Jog, 2009/6. sz., 1. o.

A Tervezet 306. szakasza, amely az adat lefoglalásának szabályait tartalmazza is elsősorban magának az adatnak a megszerzését preferálja. Az (1) bekezdés szerint ez történhet másolat készítésével, áthelyezéssel, az információs rendszer vagy adathordozó egészéről másolat készítésével, illetve ezek lefoglalásával. Ez utóbbira a (4) bekezdés alapján csak akkor kerülhet sor, ha az adott rendszer elkobozható, illetve vagyonelkobzás alá esik; tárgyi bizonyítási eszközként bír jelentőséggel; valamint a bizonyítás érdekében az abban tárolt, előre nem meghatározható vagy jelentős mennyiségű elektronikus adat átvizsgálására van szükség. A (3) bekezdés külön előírja, hogy a lefoglalás a büntetőeljárás célja szempontjából szükségtelen elektronikus adatra lehetőleg ne terjedjen ki, illetve az ilyen elektronikus adatot a lefoglalás a legrövidebb ideig érintse.

A Nemzeti Nyomozóirodánál töltött tudományos gyakornoki időm során elmondták, hogy a számítógépek lefoglalása esetén különleges elektrosztatikus csomagolásra lenne szükség, amely biztosítja az adathordozók fizikai védelmét. Ennek hiányában ugyanis előfordulhat, hogy a házkutatás során lefoglalt eszközökön található adatok véletlenül vagy szándékos behatásra (pl. a gyanúsítottak mágnesek segítségével) még az átvizsgálás előtt sérülnek. Az autentikusság biztosítása érdekében pedig ajánlott a csomagoláson nyommentesen nem felnyitható biztonsági jelzések használata. A számítógépek tartalmáról a lefoglalást követően hiteles másolatot készítenek, és minden szükséges hatósági és szakértői átvizsgálást ezen a változaton végeznek el. Mivel a klón kijelzi, ha az adatok az elkészítést követően módosításra kerültek, hitelességéhez nem férhet kétség. Ugyanakkor a lefoglalás gazdaságossági okokból nem mindig felel meg az itt leírtaknak, hiszen az említett speciális csomagolás túlságosan is drága lenne. Sokszor azonban a nyomozóhatóság az, amely nem kellő körültekintéssel végzi el a lefoglalást, így előfordul, hogy bármiféle csomagolás nélkül adják át a számítógépeket az NNI munkatársainak. Elméletben ez akár komoly kétségeket is felvethet az adatok hitelességét illetően, a gyakorlatban azonban a fájlok felkerülésének dátuma jól naplózott, így megállapítható, mely adatok voltak rajta eredetileg is a számítógépen.

Záró gondolatok

Az elektronikus bizonyítás nagyon fiatal területe a büntető eljárásjognak, ezért számos nyitott kérdést tartalmaz. Nagy szakértelmet igényel annak biztosítása, hogy a beszerzett adatok később bizonyítékként felhasználhatók legyenek, és számos olyan tényező létezik, amely ezt tovább nehezíti. Az anonimizáció és a titkosítás két ilyen probléma, és a rá adott válaszok mutatják, hogy igen nehéz feladat a megfelelő szabályozás kialakítása. Akárcsak előbbiek, a lefoglalás és az adatmegőrzés kapcsán is hasonlóan komoly alapjogi aggályok merülnek fel, főleg mivel az elektronikus adat nem semleges adat, képet adhat egy személy teljes magán-

életéről, beleértve számos érzékeny kérdést (egészségügyi állapot, vallás, szexuális irányultság stb.).[52] Nem megfelelő kezelése esetén súlyosan sértheti a magánélethez való jogot.

A valamennyi érdeket szem előtt tartó szabályozás szükségességét mind az európai, mind a magyar jogalkotó kezdi megérteni. Az adatmegőrzési irányelv megsemmisítése komoly figyelmeztetés volt erre, de az új Be. tervezete is számos kérdésben – például a lefoglalandó adatokat illetően – igen előremutató és átgondolt. Bizonyos szabályozások azonban még mindig nem veszik figyelembe a kibertér és az elektronikus bizonyítás sajátosságait, például a titkosított kommunikációval kapcsolatos magyar kormányrendelet, vagy az adatmegőrzési irányelv után született brit adatmegőrzési törvény (*Data Retention and Investigatory Powers Act 2014*).

A jogalkotáson túl fontos a jogalkalmazók, különösen az ügyész és a nyomozóhatóság szakmai felkészültsége is. Az elektronikus adatok sérülékenysége miatt ugyanis apró hibák is azt eredményezhetik, hogy a megszerzett adatok bizonyítékként nem lesznek figyelembe vehetők. A lefoglalás kapcsán számos olyan hanyagságból fakadó probléma ütközik ki, amelyek már némi odafigyeléssel is kiküszöbölhetők lehetnének. Az ezzel kapcsolatos tudatosságot erősítő képzésekre igen nagy szükség van.

Irodalom

Alföldi Ágnes Dóra: *A bűnügyi együttműködés általános kérdései az Európai Unióban*. Európai Jog, 2011/2. sz. 15. o.

Brenner, Susan W.: *Cybercrime Law – A United States Perspective*. In: Casey, Eoghan. Digital Evidence and Computer Crime. USA: Academic Press. 85–122. o.

Casey, Eoghan: *Foundations of Digital Forensics*. In: Casey, Eoghan (ed.) Digital Evidence and Computer Crime. USA: Academic Press. 7–34. o.

Chalmers, Damian – Davies, Gareth– Motti, Giorgio: *EU Criminal Law*. New York: Cambridge University Press, 2014

Christian DeSimone: *Pitting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive*. German Law Journal, 2010/3. sz. 291–317. o.

Chronowski Nóra: *Szabadság kontra biztonság – az Alapjogi Chartába ütközik az adatmegőrzési irányelv*. Magyar Tudományos Akadémia, http://hpops.tk.mta.hu/blog/2014/05/az-alapjogi-chartaba-utkozik-az-adatmegorzesi-iranyelv. (Letöltés ideje: 2016. november 14.)

[52] Signorato: i. m. 207. o.

Dornfeld László: *A kibertér főbb nemzetközi és nemzeti szabályozásai*. In: Pintér István (szerk.): A virtuális tér geopolitikája. Geopolitikai Tanács Műhelytanulmányok, 2016/1. Budapest: Geopolitikai Tanács. 43–88. o.

Jánosi Andrea: *Az európai nyomozási határozat előzményei és vívmányai*. In: Hallók Tamás (szerk.) Publicationes Universitatis Miskolcinensis Sectio Juridica et Politica Tomus XXXIII. Miskolc: Miskolc University Press, 213–223. o.

Jensen, Eric Talbot: *Cyber Sovereignty: The Way Ahead*. The Texas International Law Journal, 50/2. sz. 275–304. o.

Laczi Beáta: *A számítógépes környezetben elkövetett bűncselekmények nyomozásának és a nyomozás felügyeletének speciális kérdései*. Magyar Jog, 20011/12. sz. 726–738. o.

Láris Liliána: *Az Európai Nyomozási Határozat*. Ügyészek lapja, 2015/1. sz. 87–93. o.

Levin, Avner – Ilkina, Daria: International Comparison of Cyber Crime. Ryerson University, 2013. Online:http://www.ryerson.ca/tedrogersschool/privacy/documents/Ryerson_International_Comparison_ofCyber_Crime_-March2013.pdf (Letöltés ideje: 2016. 11. 12.)

Parti Katalin: Nyomozás az interneten: együttműködés – korlátokkal. Belügyi Szemle, 2004/11–12. sz. 204–220. o.

Signorato, Silvia: *ICT, Data Retention, and Criminal Investigations of Economic Crimes*. Journal Of Eastern European Criminal Law, 2015/2. sz.

Soares, Nicholas: *The Right to Remain Encrypted: The Self-Incrimination Doctrine in the Digital Age*. American Criminal Law Review, 2012/4. sz., 2001–2019. o.

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

Trócsányi Sára: *Első oldal*. Infokommunikáció és Jog, 2009/6. sz., 1. o.

Vadász Viktor: *A számítógép demisztifikálása*. Ügyészek Lapja, 2010/2. sz. 13–21. o.

van der Wagen, Wystke– Pieters, Wolter: *From Cybercrime to Cyborg Crime: Botnets as Hybrid Criminal Actor-networks*. The British Journal of Criminology, 2015/3. sz. 578–595. o.

Wang, Shiuh-Jeng: *Measures of retaining digital evidence to prosecute computer-based cyber-crimes*. Computer Standards & Interfaces, 2007/2. sz. 216–223. o.

Zeno-Zencovich, Vincenzo: *Anonim véleménynyilvánítás az interneten*. In Medias Red 2014/2. sz. 290–303. o.