NAGY ZOLTÁN ANDRÁS*

A joghatóság problémája a kiberbűncselekmények nyomozásában

E rövid, néhány, – az írója szerint remélhetőleg hasznos, hasznosítható – gondolatot, jogi problémát felvillantó, azokra reflektáló tanulmány a büntető eljárásjogot és a nemzetközi büntetőjogot érintő újabb kihívásokról szól, ám a tanulmányban több gondolat rejlik, mint csupán a joghatósági vitákról egy adott bűncselekménytípus esetében.

I.

A számítástechnika, különösen az Internet közvetítésével megjelent és egyre szaporodó, egyre veszélyesebb bűncselekmények valamennyi bűnügyi tudomány számára jelentenek kihívást. A számítógépes környezetben elkövetett bűncselekmények, nemcsak az anyagi büntetőjog számára jelentettek új kihívást, hanem a büntető eljárásjog és a kriminalisztika számára is.

Az elektronikus impulzusok, adatok „testetlensége," „láthatatlansága," – mint e bűncselekmények egyik kriminalisztikai jellemzője – az anyagi büntetőjogot új tényállások megalkotására ösztönözték. Komoly kihívás a dogmatika felé, hogy egyfelől értsük meg a jogsértés lényegét (és persze veszélyességét). Alapvető *Nagy Ferenc* ama megállapítása, miszerint az állami kényszerrel csak azon érdekek, értékek védendők, amelyek a közösségi együttélés számára nélkülözhetetlenek.[1] Nem kívánatos, ha bár létező, érzékelhető társadalmi anomáliát észlelünk, ám ez hatásában nem éri el a közösségi együttélés veszélyeztetését, és arra büntetőjogi reagálás történik. Ez devalválja a büntetőjog szerepét, tekintélyét.

A számítógépes környezetben elkövetett bűncselekményekkel kapcsolatos másik törvényhozási megfontolás az, hogy ne kerüljön sor a tényállások duplikálására, különös tekintettel arra a tényre, hogy egyre szűkül azon bűncselekmények köre, amelyeket számítógéppel nem lehet elkövetni.[2] Magunk a valós térbeli bűncselekményeket tekintjük alapvető igazodási pontnak és ehhez képest gondolkodhatnánk újabb tényállásokon.

---

* habilitált egyetemi docens, Pécsi Tudományegyetem

1 NAGY FERENC: *Régi és új tendenciák a büntetőjogban és a büntető jogtudományban*. Budapest, 2013. 34. p.

2 Közlekedés biztonsága elleni bűncselekményt a közlekedési lámpákat vezérlő számítástechnikai rendszerbe történő illetéktelen beavatkozással, vagy – extrém példát említve, – emberölést az intenzív osztály számítógépeinek manipulálásával is el lehet követni.

A bűncselekményeket számítógépekkel, számítógépekhez kötötten vagy számítógépes hálózatokon, így az Interneten[3] keresztül követik el. Az Internet határok nélküli, a tényállási elemek különböző földrajzilag lokalizálható vagy éppen nem lokalizálható helyen valósulnak meg. A nemzetközi büntetőjog nem képes minden kérdésre – remélhetőleg csupán időlegesen – adekvát választ adni.

A számítógépes hálózatokon elkövethető bűncselekmények jellemzően nemzetközi jellegűek, ugyanakkor a bűnüldözés nemzeti keretek közé szorított. Kívánatos volna egységes büntetőjogi fellépés e körben (is). A büntetőjogi jogharmonizáció vagy akár europaizálódásának[4] elmaradása a joghatóság (a legtágabban értelmezhető hatáskör) problematikusságát kiemelik. A belső határok eltörlése óta növekvő számú problémával szembesülünk.[5] Az államok hatékony együttműködését számtalan körülmény gátolja, a sokszor túl formalizált eljárási szabályok, a saját állampolgár kiadatásának tilalma, a ne bis in idem nemzetközi hatályának elutasítása és más körülmények.

Kiáltunk, kiáltanánk egy közös – legalább – az Európai Unió területén hatályos büntető törvénykönyvért, hiszen értékeink, érdekeink inkább az azonosság irányába mutatnak, sem mint a különbségekébe. Ennek a büntető törvénykönyvnek nem kellene teljes körűen meghatározni az elkövethető valamennyi bűncselekményt, hanem – és ebben hamar konszenzus születne – a relatív állandósággal jelen levő bűncselekményeket. Biztos van 60-80 olyan tilalmazott tevékenység, amelyet az európai országok büntetni rendelnek. Ez képezhetné az alapját *egy közös Európai Uniós büntető törvénykönyvnek*. E mellett az egyes *nemzeti büntető törvénykönyvek*, mintegy *szubszidárius* megoldásként további bűncselekményeket állapíthatnának meg. Ezzel a jogtechnikai megoldással az állami szuverenitás, önállóság a bűncselekmények meghatározásában kisebb mértékben sérülne, a tradíciók, egyes magatartások eltérő erkölcsi megítélése továbbra is figyelembe veendő tényezők lennének a nemzeti törvényhozásban. A jogalkalmazónak egyszerre két büntető törvénykönyvet kellene a kezében és az eszében tartani.

Persze, vannak elsőre megoldhatatlannak látszó kérdések, a szankciórendszer, az életkor vagy a halmazat megítélése abban az esetben, ha az egyik cselekményt az Uniós büntető törvénykönyv, a másik cselekményt a nemzeti törvénykönyv nyilvánítja bűncselekménynek. Biztos vagyok benne, hogy ez lehetne egy *Európai Unió büntetőkódexéhez vezető út*. In practice, az államok nem vennék magukra azt a terhet, hogy náluk „érdemes" bűncselekményt elkövetni, mivel ott ez nem bűncselekmény, szemben más országokkal, ahol ez a cselekmény büntetni rendelt.

Visszatérve a távoli jövőből a jelenbe vagy inkább a nem túl távoli jövőbe. Sajnos, el kell ismerni, hogy van az Internetnek olyan része, amelyhez szinte lehetetlenség hozzáférni, ahol a szolgáltatás - ellenszolgáltatás legfeljebb akkor bizonyítható, ha az ügylet

---

[3] Internetworking System rövidítése a ma használatos Internet elnevezés. Története a szovjet szputnyik 1957-es fellövésével kezdődött. Az USA szembesült azzal, hogy a szovjetek a nagyhatóságú rakétáikkal nemcsak űreszközöket, hanem pusztító eszközöket is képesek eljuttatni, és ezzel a vezetési pontok váltak veszélyeztetté. Majd a sok évtizedes katonai felhasználást követően az 1990-es évektől – az üzleti érdek nyomására – kereskedelmi célú felhasználásra kapott „engedélyt."

[4] NAGY FERENC: *Az európai büntetőjog fejlődési irányairól és jogállami alapjáról.* Acta Juridica Et Politica. Tomus Lxi. Szeged, 2002. 308. p.

[5] Vö. LIGETI KATALIN: *Büntetőjog és bűnügyi együttműködés az Európai Unióban.* Budapest, 2004. 41. p.

valamely eleme, az ebben részt vevő valamelyik személy a valós térben felbukkan.[6] Mindehhez tegyük hozzá, hogy a technika rendkívüli gyors fejlődése miatt újabb és újabb kérdésekre kell választ keresnünk, választ adnunk, szinte folyamatosan. Ez a kutatónak öröm, ám a számítástechnikai szakma számára kevésbé.[7]

II.

A büntetőeljárás sikerét a bűncselekmény teljeskörű felderítése, bizonyítása jelenti. Ez alapozhatja meg az aggálymentes bírói döntést az elkövető eljárásjogi bűnösségében. Az elektronikus adatok, mint elektronikus impulzusok, mint bizonyítékok beszerzéséhez, vizsgálatához nem minden esetben nyújtanak kielégítő megoldást a tradicionális eljárásjogi szabályok. Az elektronikus bizonyítékok megszerzésének, felhasználásának dilemmáját *Ulrich Sieber* az alábbiakban összegezte:

- a büntetőeljárás során passzív tűrési kötelezettség (számítógép átvizsgálása, adatok lefoglalása, a számítógépek közötti kommunikáció rögzítése stb.) szabályozása mellett
- aktív közreműködési kötelezettségek (a terhelt, a sértett, a tanúk, a sértett-tanú részéről), valamint
- a nyomozás során feltárt adatok védelme.[8]

A számítógépes környezetben fellelhető bizonyítékok egyrészről a számítógépen, számítógépes hálózatokon megvalósuló bűncselekmények által keletkeznek, másrészt a valós térben megvalósuló bűncselekmények bizonyítékai lelhetők fel számítógépes környezetben. E bizonyítékok megjelenítéséhez jellemzően további technikai eszközökre van szükség láthatóságukhoz, értékelésükhöz.

Kérdés, hogy az elektronikus adatok lehetnek-e eredeti bizonyítékok. *Herke Csongor* szerint az eredeti („ősforrás") bizonyítékok lényege az, hogy a bizonyítékok az ügydöntő hatóság előtt vannak, a hatóság azt közvetlenül – érzékszerveivel – érzékeli.[9]

---

[6] Az Internet két, illetőleg három részre osztható:
- a Surface web, a „jéghegy csúcsa" az Internetnek az a része, amely szabadon elérhető, szabadon keresheto, amelyre a keresőszolgáltatók linket adva mutatnak,
- a Deep weben található adatállományokhoz jelszóval, más azonosítóval lehet csak hozzáférni, akadémiai hálózatok, belső (cégek, egyetemek stb.) hálózatai (intranetek), FTP-szerverek stb.,
- a Dark web, amely tulajdonképpen az előző része a bűnözők találka- és üzletkötő helye, speciális (kliens-) programokkal érhető el, fegyver-, kábítószer-, hamis okiratok vásárlása, bérgyilkos igénybe vétele, pornográf-, pedofil-, szerző jogi tartalmak elérése és más tiltott tevékenységek találhatók ehelyütt. A virtuális valutával történő fizetés még inkább jól leplezheti ezt a világot. Általában a Cr2Cr-rel (criminals to criminals – a bűnöző a bűnözővel kerül kapcsolatba) jelölik a Dark webes üzleteléseket.

Vizsgálódásunk főleg a Surface webre koncentrál, bár esetlegesen a Deep webre kitekintünk.

[7] 2016. április 1-jén nagy erejű, összevont támadás érte a magyar kormányzati szervereket: 16-18 óra és 22-24 óra között le kellett kapcsolni a kormányzati és az MTA szervereit. Majd másnap 11-13 óra között le kellett kapcsolni a kormányzati és az MTA szervereit. Magyarország állam- és közigazgatását gyakorlatilag 6 órára lekapcsolták a világhálóról 86400 másodperc alatt 64000 „betörési kísérlet" terhelte a kormányzati és az MTA szervereit.

[8] SIEBER, ULRICH: *Computerkriminalität und Informationsstrafrecht*. Computer und Rechts 1995/11, 109–110. pp.

[9] HERKE CSONGOR: *Büntető eljárásjogi alapismeretek*. Pécs, 1998. 16. p.

Az elektronikus adatok – ontológiai szempontból – másodlagosak, hiszen kinyomtatva, fényképen láttatva, szakértői jegyzőkönyv segítségével stb. jut el az ügydöntő hatósághoz. *Wolfgang Bar* azt a véleményt képviseli, hogy „a nyomozás szempontjából meghatározó információk ... csak a tárgyiasult adathordozóval együtt, mint a legkisebb önállósítható egységgel együtt foglalhatók le."[10]

Az angol *J. C. Smith* közlése szerint a számítógéppel kinyomtatott dokumentumok általában „hallomásnak" tekintendők.[11] Kivétel ez alól, ha a dokumentum létrejötte ténykérdéshez kötött (az elkövető billentyűzte-e be a tiltott tartalmat, ő általa történt-e a hamis utalás stb.), akkor ennek a ténynek a bizonyítása szükséges. További kivétel a hersay alól, ha a számítógép figyelte meg, rögzítette a jogellenes cselekményt, így például naplózta a történéseket, az írásos,- vagy videó-kommunikációt, programok telepítését, vagy a tevékenység, így a szövegírás stb. nyomai a „szemétfájlokban" fellelhetők és más módok.

Az elektronikus adatok között megkülönböztethetők:

- tartalmakat hordozó elektronikus adatok, szövegek, képek, a HTML oldalakhoz csatolt (feltöltött) audió- vagy videófolyamok, e-mailek és más adatok;
- forgalmi adatok: internetes munkamenetet (számítógépek kapcsolódásait) jelölő napló (log-)fájlok, előfizetők adatai, TCP/IP – számok (számítógépek egyedi azonosítója, „személyi igazolványa") és más adatok;
- egyéb elektronikus adatok, nyomok: törölt adatok (temp-fájlok), programok telepítésének/törlésének nyomát rögzítő napló (log)-fájlok, a registry-ben rögzített információk, a gyanúsított jelszavai, azonosítói és más adatok.

Keletkezhetnek más bizonyítékok is a valós térben, pl. a nyomtatófesték fogyása, a nyomtatóban levő papír fajtája, minősége, a próbanyomat.

Bizonyítékhordozók lehetnek a legkülönfélébb technikai eszközök:

- asztali számítógépek, laptop, tablet, mobiltelefon stb.;
- hálózati kapcsoló eszközök;
- a számtalan féle-fajta adattároló: winchester, külső merevlemez, pen-drivek stb.[12]

A bizonyítékok fajtái lehetnek:

- statikus bizonyíték: egy eszközökön levő, fizikai hozzáféréssel elérhető elektronikus impulzusok (adatok), mint bizonyítékok,
- dinamikus bizonyíték: ezen elektronikus adatok a hálózaton belül vagy szerverek között „keringenek."

[10] BAR, WOLFGANG: *Beschlagnahme von Computerdaten.* Computer und Recht 1996/12. 752. p.

[11] SMITH, JOHN: *Criminal Evidence.* London, 1995. 91–93. pp. Innen a Hersay-törvény elnevezése.

[12] Hol vannak már a lyukkártyák, lyukszalagok, hajlékony lemezek, kazettás floppy-lemezek. Ez utóbbi feltalálója Jánosi Marcell (1931-2011), sajnos a szabadalmi idő lejártát követően nem hosszabbította meg találmányának védettségét, így a kiváló ötlete „szabad rablás tárgya" lett. A mágnesszalagok, mint adathordozó ma még használatosak. A mai DVD-k is hamarosan átadják helyüket a Blue Ray lemezeknek. [Az adathordozókon szerzői műveket gyártó cégeknek óriási üzlet, hogy 6-10 évenként más-más adathordozón adhatják ki az egyszer megszerzett (és kifizetett) szerzői műveket: gramofon(sellak)lemezeken, SP- és LP bakelit (vinyl) lemezeken, hangkazettákon, CD-ken, DVD-ken stb.].

A tipizálás jelentősége gyakorlati elérésükben, a lefoglalásuk módszerében, a bűnügyi jogsegélyt érintő kérdésekben kerül elő.

III.

A számítógépeken és számítástechnikai hálózaton elkövethető bűncselekmények nyomozását már ma több körülmény nehezíti:

- A nyomozók felkészültsége az inkriminált adatok (pl. tartalomközlések), a hálózati történések (számítástechnikai rendszerbe történő illegális belépés, mint hacking, web-oldal felülírása, mint defacing, a számítástechnikai rendszert érő terheléses támadás, mint botnet-támadás, a felhasználót fenyegető zsarolóvírus, mint ransomware és más rosszindulatú szoftverek, mint malicous software-ek, röviden malware-ek stb.) megértése, ismerete.
- Ha a számítógépek, hálózatok fizikailag elérhetők, Magyarországon vagy a zászló-elv miatt magyar felségterületen található, akkor a bizonyítékok megszerzésére irányuló és sajátos megoldásokat kívánó kényszerintézkedések végrehajtása.
- Ha a számítógépes hálózat vagy annak részét képező számítógép – az előző eseten kívül - fizikailag nem érhető el, különösen, ha nem is lokalizálható a bizonyítékok megszerzésének a helye, akkor nemzetközi büntetőjogi intézmények formalizmusa.

A bizonyítékok az alábbi földrajzi helyeken érhetők el:

1. Magyarországon, magyar felségterületen levő számítástechnikai rendszerben tárolt bizonyíték elérése

A számítógépes bűncselekményekkel összefüggő nemzeti és nemzetközi jogi kötelezettségek, nemzeti és nemzetközi jogban büntetni ajánlott cselekmények meghatározásainak mind mai napig alapvető gyűjtőhelye a 2001-es ún. budapesti egyezmény, amelyből néhány rendelkezés utal a nemzeti hatóságok kötelezettségére. Alkossanak olyan jogszabályokat, amelyek lehetővé teszik a

- számítástechnikai rendszer vagy annak egy része és az abban tárolt számítástechnikai adatok, és
- a számítástechnikai adatok tárolását lehetővé tevő számítástechnikai adattároló-egység átvizsgálását vagy ahhoz más módon történő hozzáférést.

Az előzőekhez kapcsolódó kényszerintézkedések sajátosságaira is felhívta a figyelmet az Egyezmény:

a) a számítástechnikai rendszer vagy annak része, illetőleg számítástechnikai adattároló-egység lefoglalása vagy más hasonló módon történő biztosítása;
b) számítástechnikai adatról másolat készítése és annak megőrzése;
c) a szükséges tárolt számítástechnikai adatok épségének megóvása; és
d) az átvizsgált számítástechnikai rendszer fenti számítástechnikai adatainak hozzáférhetetlenné tétele vagy eltávolítása.

E szabályok természetesen a nemzetközi relációban szerzett bizonyítékok kezelésére is alkalmazandók. Néhány különös szabály született a dinamikus bizonyítékok beszerzésére vonatkozóan, a szolgáltatók együttműködési kötelezettségét nevesítve.

A nemzeti jogalkalmazáson túl igazán izgalmas kérdés és megoldásra váró jogi probléma a bűncselekmény jellegéből következően a külföldről beszerzendő bizonyítékok elérése. Rövid tanulmányunk ez utóbbi kérdéskörre fókuszál, ismeretet adva, écát nyújtva az Olvasónak (is).

2. Külföldön, meghatározott földrajzi helyen levő számítástechnikai rendszerben tárolt bizonyíték elérése

Az elérés lehetséges bűnügyi jogsegély keretében, ez esetben a bűnügyi jogsegélyre, irányára, kérésére és nyújtására vonatkozó jogi feltételek teljesülése az alap. A bűnügyi jogsegély fejlődésére vonatkozó a jogtörténetből már ismert lépések:

- H. Grotius: aut punire, aut dedere (1625) principiumát fogalmazta meg.[13] Ma helyesebb az aut punire, aut judicare elvéről beszélni. Ennek indokoltságára terjedelmi korlátok miatt nem térhetünk ki.
- 1927. Lotus-ügy: az állam büntetőhatalmát akkor érvényesítheti, ha erre lehetősége van.[14] Ez ma a terrorizmussal szembemenő ellenség-büntetőjog eszmeiségében és gyakorlatában érvényesül.[15] Ma az irreguláris migrációval szemben hazai jogi szabályozás az absztrakt társdalomra veszélyesség kiemelésével[16] ezen úton indult el és halad. Törekedni kellene arra, hogy az idegenrendészeti eszközök kapjanak elsőbbséget.[17] A reális helyzetértékeléshez figyelembe kell vennünk, hogy az irreguláris migrációnak, ahogy a jogszerű vagy jogellenes határátlépéseknek is „csatornája" lehet tárgyak, más személyek engedély nélküli mozgásának, továbbá célja és iránya lehet bűncselekmények elkövetése.[18]

További veszélye az, hogy az irreguláris migrációval azonosítatlan személyek százai léphetnek be a schengeni határok közé.[19]

Félretéve ezt a nagyon komoly, évtizedekre kiható és valószínűleg évtizedekig tartó szociológiai, jogi, politikai problémát, az azt övező polémiát, folytassuk a joghatóság fejlődésének vázlatos áttekintését:

1965. Európa Tanácsi egyezménytervezet[20] született a joghatósági összeütközésekről.

---

[13] Vö. LIGETI 2004, 49. p.
[14] Vö. LIGETI 2004, 43. p.
[15] Vö. NAGY 2013, 165. p.
[16] AMBERG ERZSÉBET: *Migráció, büntetőjog, ultima ratio*. In: Hautzinger Zoltán (szerk.): A migráció bűnügyi hatásai. Budapest, MRTT.2016. 206. p.
[17] HAUTZINGER ZOLTÁN: *Az irreguláris migráció büntetőjogi aspektusai*. In: Hautzinger Zoltán (szerk.): Migráció és rendészet. Budapest, Magyar Rendészettudományi Társaság Migrációs Tagozat. 2015. 50. p.
[18] HAUTZINGER ZOLTÁN: Büntetőjogi tényállások a külföldiség és a migráció vonzásában. In: Hautzinger Zoltán (szerk.): A migráció bűnügyi hatásai. Budapest, MRTT.2016. 181. p.
[19] ANGYAL MIKLÓS – MÉSZÁROS BENCE: *Egyek vagyunk, de nem ugyanazok – személyazonosítás és európai bevándorlás.* In: HAUTZINGER ZOLTÁN (szerk.): A migráció bűnügyi hatásai. 108. p.
[20] http://coe.archivalware.co.uk/awweb/pdfopener?smd=1&md=1&did=936207 [Láttam: 2017. 04. 07.]

E tervezet szerint az elkövetés helye szerinti államnak van elsődleges joga büntető igényét érvényesíteni (lex loci elve - Tervezet 2. cikk). Ezt az elvet az ún. védelmi elv törhette meg, ebben az esetben a fenyegetett országé az elsődleges büntető igény (7. cikk).

A tervezet további sorrendet határozott meg az eljárás lefolytatásához:

– az az ország, ahol a tettes vagy a bűnrészes a cselekményt elkövette,
– az az ország, ahol a cselekményt elősegítő magatartás megvalósult,
– az az ország, ahol a cselekmény eredménye bekövetkezett (3. cikk 3. pontja).

Ennek supplementuma az Európai Tanács 2009/948/IB Kerethatározata. A kerethatározathoz fűzött jogértelmezést az Eurojust 2003-as Éves Jelentése.[21] Ennek témánk szempontjából azért van jelentősége, ugyanis a számítógépes környezetben nem ritkán a bűncselekmények megvalósulásának egyetlen eleme detektálható, értelmezhető a nemzeti hatóságok számára.

A joghatóság megállapításához figyelembe kell venniük például

– azt a helyet, ahol a bűncselekmény legnagyobb részét elkövették,
– azt a helyet, ahol a kár vagy veszteség jelentős része keletkezett,
– a gyanúsított vagy vádlott tartózkodási helyét, valamint
– más joghatóságok számára történő átadásának vagy kiadatásának lehetőségeit,
– a gyanúsított vagy vádlott állampolgárságát vagy lakóhelyét,
– a gyanúsított vagy vádlott jelentős érdekeit,
– a sértettek és tanúk jelentős érdekeit,
– a bizonyítékok elfogadhatóságát vagy
– az esetlegesen előforduló késedelmeket.

A felsoroltak egyben sorrendet teremtettek. Az európai ügyészek szervezetének iránymutatásában megfogalmazottak beépülése az államok joggyakorlatába kétségeket ébreszt, bármennyire is tartalmaz ésszerű elemeket.

A bizonyítékok összegyűjtése történhet azok közvetlen elérésével, ez esetben a megközelítés összetettebb, több szegmenst érint, így

– a területi elv realitását,
– a nemzeti szuverenitás érzékenységét,
– a felhasználók személyes jogainak védelmét.[22]

Az 1989-ben született a „Számítógépes környezetben elkövetett bűncselekményekről" szóló Európai Tanácsi ajánlásában[23] az ET még nem vetette fel ez a problémát. Ez még az Internet kommercializálódása előtti idő. Az Európa Tanácsnak a pénzmosásról, a bűncselekményből származó jövedelmek felkutatásáról, lefoglalásáról és elkobzásáról szóló 1990-es 141. egyezménye szintén nem szólt a számítógépes környezetben elköve-

[21] http://eurojust.europa.eu/doclibrary/corporate/eurojust%20Annual%20Reports/Annual%20Report%202003/Annual-Report-2003-EN.pdf p(s) 62-64. [Láttam: 2017. 04. 07.]

[22] Vö. LIGETI 2004, 42. p.

[23] Recommendation No. R (89) 9 Of The Committee Of Ministers To Member States On Computer-Related Crime. https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=610660&SecMode=1&DocId=702280&Usage=2

tett bűncselekmények bizonyítékainak külföldről történő lefoglalásáról és más kényszerintézkedésekről rendelkezni.[24]

Az Internet térhódításával, továbbá egyes bűncselekmények elterjedésével összefüggésben[25] az 1995-ös „Büntetőeljárási kérdések az informatikai bűncselekményekben,"[26] amely – az országok szuverenitása tiszteletben tartásának követelményével – nemzetközi megállapodást sürgetett a határokon átívelő hálózatokban fellelhető bizonyítékok felkutatása, lefoglalása alkalmazásának lehetőségére (17. pont).

A számítástechnika fejlődésével és a növekvő büntetőjogi kihívások elemzésére és a megoldási lehetőségek keresésére az Európa Tanács 1997-ben létrehozta a bűnözés kérdéseivel foglalkozó bizottságot [teljes nevén: European Committee on Crime Problems of the Council of Europe (CDPC)] és ezen belül létrejött a számítógépes bűnözés szakértőinek bizottsága [teljes nevén: Committee of Experts on Crime in Cyber-Space (PC-CY)].

A későbbi budapesti egyezmény szövegezését segítette a G8-as miniszterek által 1999-ben kiadott nyilatkozat *„A tárolt számítógépes adatok határokon átnyúló hozzáférésének alapelveiről."* Az ott közzétett normaszöveget átvette a 2001-es budapesti egyezmény. Ugyanakkor a nyilatkozatban szerepel egy – általunk fontosnak tartott és a jogsegély ügyében a megoldást segítő, ám a budapesti egyezményből kihagyott – mondat, jelesül, „a kereső államnak fontolóra kell vennie a keresett állam bejelentését, ha az ilyen bejelentést a nemzeti jogszabályok megengedik, és az adatok a büntetőjog megsértését tárják fel, vagy a keresett államra nézve más szempontból tűnik fontosnak."

A 2001-ben kihirdetett Európa Tanács Budapesten, 2001. november 23-án kelt *Számítástechnikai Bűnözésről szóló Egyezménye* bűnügyi jogsegély hiányában is megnyitotta az utat az egyezményben részes országok számára az együttműködésre a tárolt elektronikus adatok megszerzésére. „A Szerződő Fél megkeresheti a másik Felet, hogy a területén található számítástechnikai rendszer útján tárolt adatokat átvizsgálja vagy azokhoz más hasonló módon férjen hozzá, foglalja le vagy más hasonló módon szerezze meg, illetőleg adja át."[27] (31. pont)

Ennél is izgalmasabb kérdés egy másik állam számítástechnikai hálózatából történő bizonyítékszerzés lehetősége. A statikus elektronikus adatok esetében bármely ország bármely más szerződő állam beleegyezése nélkül

- a nyilvánosság számára elérhető (open source, azaz nyílt forrású) módon tárolt számítástechnikai adathoz hozzáférhet, függetlenül az adat földrajzi elhelyezkedésétől; vagy
- a másik Szerződő Fél területén tárolt számítástechnikai adathoz hozzáférhet, vagy a területén levő számítástechnikai rendszer útján azt megszerezheti, amennyiben a

[24] EC Convention On Laundering, Search, Seizure And Confiscation Of The Proceeds From Crime (1990.) https://www.imolin.org/doc/amlid/Belgium_Convention_8_November_1990_English.pdf [Láttam: 2017. 04. 07.]

[25] PUSZTAI LÁSZLÓ: *Komputerbűnözés és a büntetőjogi reform az NSZK-ban*. MJ. 1987/11, 958. p. – Szeretett és Tisztelt Kollégánk az akkoriban elterjedőben levő manipulált banki átutalásokról írt.

[26] Recommendation No. R (95) 13 Of The Committee Of Ministers To Member States Concerning Problems Of Criminal Procedural Law Connected With Information Technology https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=1900870&SecMode=1&DocId=528034&Usage=2

[27] http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0400079.TV 31. pont [Láttam: 2017.04.15.]

> Fél beszerzi az adat számítástechnikai rendszer útján történő átadására jogszabályban feljogosított személy önkéntes és jogszerű hozzájárulását.[28] (31. pont)

Az első esetben a bármely ország bármely felhasználója által szabadon elérhető adatállomány elérése megengedett, a másik esetben az adatállományhoz a feljogosított, illetékes személy önkéntes és legális hozzájárulásával szerezhet meg adatokat.

A dinamikus elektronikus adatok esetében az egyezményben részes országok kölcsönös jogsegély keretében közreműködnek a forgalmi adatok összegyűjtésében[29] (33–34. pontok).

A számítógépes bűnözéssel foglalkozó különböző munkacsoportok több javaslatot dolgoztak, dolgoznak ki napjainkban is:

- Nemzetközi protokollok, az előfizetők adatai iránt kölcsönös jogsegélykérelmek egyszerűsítése iránt. (Rec 20 T-CY).
- Közvetlen együttműködés az igazságügyi hatóságok közötti kölcsönös jogsegély iránti kérelmek (Rec 21 T-CY).
- Közös vizsgálatok és közös nyomozócsoportok (Rec 23 T-CY).
- Tanúk, sértettek audió/videó meghallgatása.
- Sürgősségi eljárások (Rec 8 T-CY).

3. Külföldön, meg nem határozható földrajzi helyen levő számítástechnikai rendszerben tárolt bizonyíték elérése

A felhőszolgáltatás (cloud computing) napjaink olyan új technikai megoldása, amely tehermentesíti a felhasználókat attól, hogy nagytömegű adatot tároljanak, illetve különböző programokat telepítsenek számítógépükre.

A felhő-alapú szolgáltatások népszerűsége, száma növekszik (kereskedelmi szolgáltatások, pl. Amazon, Ebay). A szerverek személyes adatokat is tárolhatnak (pl. bankkártyaszámokat, Gmail és más e-mail kliens címeket, nagy kártyatársaságok adatait stb.). A felhasználó által előállított információk, (szövegek, képek) kerülhetnek ilyen tárhelyekre (pl. Dropbox, Evernote). E technikai megoldásnak következménye, hogy a bűnözés is átterjed a felhőre (2012. Operation High Roller csalás olyan malware segítségével, amely kiiktatta a PIN-es és chipes azonosításokat[30]).

A felhőszolgáltatások típusai:

- szoftver-szolgáltatás: a web-böngészőn keresztül érhetők el különböző szoftverek,
- platform-szolgáltatás: alkalmazás üzemeltetéséhez szükséges környezetet biztosítja, terheléselosztással, frissítéssel,
- infrastruktúra-szolgáltatás: virtuális hardver szolgáltatása, tárhely, számítási stb. kapacitás szolgáltatása.

---

[28] http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0400079.TV 31. pont [Láttam: 2017.04.15.]

[29] http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0400079.TV 33-34 pontok [Láttam: 2017.04.15.]

[30] http://www.networkworld.com/article/2189619/malware-cybercrime/bank-hack---operation-high-roller--has-netted--78m---so-far.html [Láttam: 2017.04.15.]

A technikai részleteknél talán érdekesebbnek tűnhet a hozzáférés lehetőségei szerinti csoportosítás:

- privát felhő: csak a dedikált felhasználó veheti igénybe, és akár egy felhasználó is létrehozhatja saját magának,
- publikus felhő: mások számára is nyitva áll a szolgáltatások igénybevétele,
- hibrid felhő: az előzőek kombinációja.

A szolgáltatás számtalan előnnyel kecsegtet, lehetővé teszi azt, hogy a felhasználók az adataikhoz, programokhoz, egyéb feladatok végrehajtására a világ bármely pontjáról hozzáférhessenek. A felhasználó adatai nem vesznek el, nem kell aggódnia, hogy számítógépe, adathordozói tönkremennek, adatait letörli véletlenül, villámcsapás az elektromos hálózatot, így a számítógépet éri stb. Jogtiszta programok legfrissebb verziói találhatók meg, amelyek garantáltan vírusmentesek, a szolgáltatás gyors és biztonságos. A felhasználó több platformot tud egyesíteni munkája végzéséhez (pl. munkahelyén, utazása során és másutt a saját számítógépén, laptopján, mobiltelefonján keletkező, előállított adatokat együtt tárolja, dolgozik azokkal).

A technikai részletek kíméletes említése nélkül nem érthetjük meg a jogi problémákat.

A szolgáltatók több szerveren (nagy kapacitású számítógépeken), más eszközön tárolják az adatokat, programokat. A szerverek lehetnek ugyanazon vagy különböző országokban, távoli szigeteken. Ez utóbbi a jellemző. Közöttük az adatkapcsolat élő, hiszen az adatok folyamatos biztonsági mentése a felhőszolgáltató feladata, kötelessége. Az adatokat a felhőszolgáltató titkosítja, a felhasználókon kívül, más nem ismerheti meg.

A számítástechnika folyamatos fejlődése újabb és újabb válaszokat kíván a büntetőjogtól. A felhőszolgáltatásokban megjelenő digitális bizonyítékok jellemzően dinamikus digitális tartalmak (események, folyamatok, adatok változása), a hálózati és mobilforgalom bizonyítékaihoz állnak közel. A felhőszolgáltatás esetében a kihívás a következő. A felhőben (egy ismeretlen helyen levő szerveren) levő inkriminált adatállomány (pl. egy tiltott tartalom) és annak előállítója, közösségi oldalon közlője, blog-oldalra feltöltője stb.) hogyan válhatnak egy büntető- vagy más eljárásban bizonyítékká.

A bűnügyi jogsegély nehézsége felhőszolgáltatás esetében:

- általában a kettős inkrimináció feltétele (tartalomközlés esetében ez kétséges),
- nem lokalizálható, hogy mely országban vannak a szerverek,
- nem lokalizálható, hogy mely ország mely szerverén található meg adott pillanatban az inkriminált tartalom.

A gyakorlatban a felhasználó valamelyik országban csatlakozik az Internethez (ha profi elkövető, akkor a TCP/IP címe nem létező cím vagy proxy server mögé rejtve használja az Internetet). Majd csatlakozik a felhőszolgáltatóhoz (ha profi az elkövető, akkor hamis e-mail címmel), annak valamely országban levő szerveréhez, majd feltölt egy tiltott tartalmat, amely valamely ország szerverére kerül, majd kikerül az Internetre egy tükrözött web-oldalra egy soha el nem érhető karibi ország domain-nevén. A klaszszikus bűnügyi jogsegély intézményei fiókban maradnak. Persze, a felhő-szervert sem lehet feltörni (meghackelni), mert az már bűncselekmény. (Legfeljebb titokban, de ehelyütt ezt említeni méltatlan.)

Nem marad más megoldás, mint a felhőszolgáltató megkeresése az inkriminált elektronikus adatok, mint az eljárásban felhasználni kívánt bizonyítékok kiadása iránt. A felhőszolgáltatók válasza vagy a kérés teljesítése vagy annak elutasítása. A válasz függ a felhőszolgáltatást alapító cég bejegyzése helyének jogszabályi feltételeitől, azaz jellemzően az Egyesült Államok jogszabályai kívánalmaitól (pl. a véleménynyilvánítási szabadság megítélésétől). Ugyanakkor, ha a szolgáltató nem adja át a kért információkat, mert például az adott tartalomközlés a szolgáltatóra vonatkozó (hazai) jogszabályok szerint a véleményszabadságba belefér, akkor gyakorlatilag a koronabizonyítékokat, vagy azok előállítóinak, feltöltőinek személye megismerését rendkívül megnehezíti az információkat kérő ország hatóságai számára. Persze, mondhatnók más bizonyítékokat keressen az eljáró hatóság a cselekmény bizonyításához, csak hát egy tartalomközlést a tartalommal és a készítő személyének a feltárásával lehet bizonyítani.

Durva és provokatív közelítéssel konstatálhatjuk, hogy egy külföldi ország jogi szabályait a hazai (magyar) jogszabályok felé helyezik, vagy másképpen fogalmazva a külföldi jogszabály értelmezője szerint a cselekmény elkövetője a szolgáltató szemében (döntésében) nem bűnös. Hiszen, ha legalább feltételezi a bűnösséget, akkor átadja a felhasználóra vonatkozó adatokat, aztán majd az átadást kérő nemzeti jogalkalmazó hatóságok ennek ismeretében (is) döntenek a felhasználó bűnösségéről.

De ne feledkezzünk meg a felhasználó személyes adatainak védelme fontosságáról, továbbá arról, hogy az információk átadását követően üldöztetésnek lesz kitéve a felhasználó saját hazájában. Manapság a terrorizmussal összefüggésben említett tevékenységek gyanúja adhatja, adja azt a lehetőséget, amely a szolgáltatókat a kért információk átadására ösztönzi. A polgárjogi felelősség kérdése is valós, például az elvesztett adatállományért vagy szolgáltatás igénybe vételének elmaradásáért való civiljogi felelősség.

A leadben felvetett gondolatra visszautalva, büntetőjogunk tovább erodálódik, amennyiben nemzetközi (akár EU-s) jogi aktus (szerződés, egyezmény, EU-s jogforrások stb.) hiányában a magyar Büntető Törvénykönyv területi és személyi hatálya szerinti felelősségre vonás érvényesülésének feltétele (akadálya) keletkezett a technika fejlődése folytán.

Ez az *anomália* – pesszimista realizmus meglátással – *örök lesz*, hiszen világunkban még az azonos erkölcsi-, vallási felfogások esetében is a hagyományok, az értékek differenciált elismertsége, a demokrácia-felfogása, annak fejlettsége, tradíciója, ezzel összefüggésben a szabadságjogok, a lakosság tolerancia szintje és más körülmények különbözők.