DOI: 10.38146/BSZ.2018.2.8

DORNFELD LÁSZLÓ

A kibertérben elkövetett bűncselekményekkel összefüggésben alkalmazható kényszerintézkedések*

A büntetőeljárás során, annak sikere érdekében az eljáró hatóság egyik kiemelkedően fontos eszköze a kényszerintézkedések alkalmazása. Ezek céljuk szerint többféleképpen csoportosíthatók, azonban témánk szempontjából a releváns szempont, hogy míg bizonyos kényszerintézkedések a terhelt, illetve más személy jelenlétét, addig mások a bizonyítékok beszerzését, illetve megőrzését, valamint a büntetőjogi szankció végrehajtását hivatottak szolgálni.[1] Elektronikus környezetben, kiberbűncselekményekkel összefüggésben elsősorban utóbbi két kategóriának van speciális jelentősége, hiszen az idetartozó kényszerintézkedések végrehajtása speciális szaktudást igényel.

A kényszerintézkedések minden esetben valamilyen alapjogot korlátoznak, ezért meg kell felelniük a szükségesség–arányosság Alkotmánybíróság által kidolgozott kritériumainak. Ez különösen fontos kérdés az informatikai bűncselekményeknél folytatott nyomozás esetén, hiszen a modern infokommunikációs eszközökön számos személyes adat található, amelyek alapján a felhasználó élete teljes egészében feltárható.[2]

Tanulmányom megírásának egyik apropóját az új büntetőeljárási törvény elfogadása adta[3], amely számos változást hozott a kényszerintézkedések rendszerében is, nem csak a digitális világ kihívásainak való megfelelés terén.[4] Elsősorban a magyar szabályozást kívánom vizsgálni, összehasonlítva a hatályos és az új törvény különbségeit az elektronikus tér szemszögéből, valamint e különbségek lehetséges hatásaival is foglalkozom. Emellett a hazai és külföldi szakirodalom által felvetett kérdéseket, javaslatokat is áttekintem.

* Köszönettel tartozom témavezetőmnek, prof. dr. Róth Erikának.

1 Király Tibor: Büntetőeljárási jog. Osiris Kiadó, Budapest, 2003, 401. o.

2 Berecz Péter: A Német Szövetségi Alkotmánybíróság „számítógép-határozata". Studia Juvenum, 2009/1., 71–72. o.

3 2017. évi XC. törvény

4 Ezekkel kapcsolatban bővebben lásd Róth Erika: A kényszerintézkedések változó rendszere és részletszabályai. Ügyészek Lapja, 2016/3–4., 39–50. o.

Az elektronikus bizonyítékgyűjtés

Az elektronikus bizonyíték fogalma

A kiberbűncselekményekkel kapcsolatban alkalmazható kényszerintézkedések jobb megértéséhez fontos megvizsgálni azt, hogy milyen specifikus problémák vetődnek fel az elektronikus bizonyítékok beszerzése során. E körülmények ismerete ugyanis elengedhetetlen a téma megfelelő áttekintéséhez.

Elsőként magának az elektronikus bizonyítéknak a fogalmát szükséges megmagyarázni. Az egyik leggyakoribb meghatározás szerint ideértendő minden olyan bizonyító erővel bíró adat, amelyet digitális formában tárolnak, feldolgoznak vagy továbbítanak.[5] *Casey* egy sokkal általánosabb megfogalmazással él, szerinte az elektronikus bizonyíték minden olyan bizonyító erővel bíró adat vagy információ, amelyet számítógép segítségével tárolnak vagy továbbítanak.[6] A fogalom meghatározása azonban – a kiberbűnözéshez köthető legtöbb fogalomhoz hasonlóan – igen bizonytalan, és a lehetőségek gyors fejlődése miatt nem is alkotható olyan definíció, amely minden aspektust magában foglal.[7]

Bizonytalanság mutatkozik például annak kérdésében, hogy a digitális- és elektronikusbizonyíték-fogalmak azonos értelműek-e.[8] Napjainkban ez egyértelműen megvalósul, hiszen a felhasználók kivétel nélkül digitális számítógépeket és egyéb infokommunikációs eszközöket (például okostelefon, tablet) használnak. Azonban korántsem biztos, hogy ez a tendencia a jövőben is folytatódik, és ez a fajta szűkítés a technológiasemlegesség kritériumának sem felel meg. Így véleményem szerint helyesebb az elektronikus bizonyíték kifejezést használni. Fontos szempont még az is, hogy az adathordozók körét nem lehet kizárólag a számítógépre redukálni, hiszen ma már számos egyéb eszköz is tartalmazhat releváns információkat.

A jogi szabályozásra áttérve, az elektronikus bizonyíték fogalmát használja több cikkében is az Európa Tanács számítástechnikai bűnözésről szóló egyezménye[9], azonban a fogalom meghatározásával adós marad. Hasonlóan a

5 Antonela Gropeneanu – Adrian Iacob: Investigative issues regarding cybercrime. European Journal of Public Order and National Security, no. 2, 2016, p. 10.

6 Eoghan Casey: Foundations of Digital Forensics. In: Eoghan Casey (ed.): Digital Evidence and Computer Crime. Academic Press, 2011, p. 7.

7 Ez magára a szabályozásra is igaz, amely így hamar anakronisztikussá válhat, ha túlságosan is technikai részletekbe bocsátkozik. Lásd Szádeczky Tamás: Az IT biztonság szabályozásának konfliktusa. Infokommunikáció és Jog, 2013/3., 149. o.

8 Sorbán Kinga: A digitális bizonyíték a büntetőeljárásban. Belügyi Szemle, 2016/11., 81. o.

9 Az Európa Tanács 2001. november 23-án, Budapesten kelt számítástechnikai bűnözésről szóló egyezménye (ETS No. 185). Kihirdette a 2004. évi LXXIX. törvény.

hatályos büntetőeljárásról szóló 1998. évi XIX. törvény (a továbbiakban: Be.) rendelkezései között is hiába keresnénk az erre vonatkozó szabályozást, és a bizonyítási eszközök között sem kerül sor a feltüntetésére. Kétféle elmélet alakult ki azt illetően, hogy mi tekinthető az elektronikus bizonyíték forrásának. Az egyik szerint azok a tárgyi bizonyítási eszközök, amelyek az adatokat hordozzák, képesek megjeleníteni, tárolni, továbbítani azt (például CD, DVD, számítógép stb.).[10] A másik, elsősorban angolszász területen elterjedt elmélet az elektronikus adatot tekinti a forrásnak.[11] Ez jelenti egyrészt a hardverelemeket irányító adatokat (például operációs rendszer, programok stb.), illetve a felhasználói adatokat (például képek, szöveges dokumentumok stb.), amelyek a felhasználó tevékenysége nyomán jönnek létre. *Peszleg Tibor* megközelítésében az adathordozó valóban szükséges az adatok rögzítéséhez, de ahogy egy nyomtatásban elkövetett bűncselekménynél, akként a digitális térben sem a rögzítő közeg, hanem a rögzített adat a lényeges a bizonyítás szempontjából.[12]

Jelentős változást hozott a büntetőeljárásról szóló 2017. évi XC. törvény (a továbbiakban: új Be.), amelynek 165. §-a már egyértelműen a bizonyítási eszközök közé sorolja az elektronikus adatot, és a 205. §-ban meg is határozza azt. Az új Be. szerint ideértendő *„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”*. Ez a megfogalmazás lényegét tekintve azonos a büntető törvénykönyvről szóló 2012. évi C. törvény (a továbbiakban: Btk.) 423. § (5) bekezdésében megtalálható meghatározással. Az információs rendszer fogalmát a Btk. 459. § (1) 15. pontja úgy határozza meg, hogy *„az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezés, vagy az egymással kapcsolatban lévő ilyen berendezések összessége”*.

A paragrafus (2) bekezdése arról rendelkezik, hogy az elektronikus adatot a tárgyi bizonyítási eszközzel azonosan kell kezelni, hacsak a törvény külön nem rendelkezik ettől eltérően. Az előbbiekben taglalt dogmatika szempontjából elmondható, hogy a jogalkotó az angolszász megoldást fogadta el, és a tárgyi bizonyítási eszközzel azonos szabályok alkalmazását mindössze praktikus szempontok vezérelték, mint az a szakaszhoz fűzött indokolásból is kitűnik.

10 Laczi Beáta: A számítógépes környezetben elkövetett bűncselekmények nyomozásának és a nyomozás felügyeletének speciális kérdései. Magyar Jog, 2001/12., 728–729. o.

11 Sorbán Kinga: i. m. 84. o.

12 Peszleg Tibor: A digitális bizonyítási eszközök megszerzésének elvei és gyakorlati érvényesítésük. Ügyészek Lapja, 2010/2., 25–26. o.

Az elektronikus környezetben elkövetett bűncselekményekre vonatkozó egyedi jellemzők közül a legfontosabb az, hogy a felhasználókat olyan veszélyek fenyegetik a kibertérben, amelyek újak, nehezen megelőzhetők és üldözhetők.[13] Az elkövetőknek sokszor jóval elmélyültebb az informatikai tudásuk, mint a nyomozó hatóság tagjainak, de az ügyészeknek és a bíróknak is, így a gyanúsított félrevezető védekezése sokszor nehezítheti az eljárást.[14] Napjainkban azonban már egyre több az olyan elkövető, akinek nincsenek különleges ismeretei, hanem mások által illegális célokra készített programokat használnak. Az ilyen igények kielégítésére elterjedőben vannak a bűnözést mint szolgáltatást *(Crime-as-a-Service)* kínáló csoportok, amelyek például rosszindulatú programokat készítenek, botneteket hoznak létre és használnak fel szolgáltatásmegtagadással járó támadásokra *(Distributed Denial of Service; DDos)* stb. A kis kockázat mellett magas profitszerzés lehetősége a hagyományos szervezett bűnözés érdeklődését is felkeltette.[15]

A kibertérben elkövetett bűncselekmények ügyében folyó nyomozás elején gyakran semmilyen más bizonyíték nem áll rendelkezésre, csakis az elektronikus adatok, így a kriminalisztika olyan hagyományos eszközei, mint a daktiloszkópia, itt még nem kapnak szerepet.[16] Az elektronikus adatok nagyon könnyen manipulálhatók, elrejthetők vagy megsemmisíthetők, így elengedhetetlen a megfelelő technikák ismerete a bizonyításhoz való biztosításuk érdekében.[17] Peszleg Tibor kiemeli, hogy akárcsak más bizonyítási eszközök beszerzésénél, a digitális térben is fontos a törvényesség és szakszerűség, és a zárt bizonyítási lánc megléte.[18] *Wang* szerint három alapvető kritériumot kell az ilyen nyomozások 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.[19] Az adatok bizonyí-

13 Vertes-Oltenau Andreea: Evolution of the Criminal Legal Frameworks for Preventing and Combating Cybercrime. Journal of Eastern-European Criminal Law, no. 1, 2014, p. 85.

14 Parti Katalin: Tiltott pornográf felvétellel visszaélés az interneten – az empirikus kutatás adatai. In: Virág György (szerk.): Kriminológiai Tanulmányok, 44. OKRI, Budapest, 2007, 98. o.

15 Nagy Zoltán, András – Mezei, Kitti: The organised criminal phenomenon on the Internet. Journal of Eastern-European Criminal Law, no. 2, 2016, pp. 137–140.

16 Laczi Beáta: i. m. 726. o.

17 Shiuh-Jeng Wang: Measures of retaining digital evidence to prosecute computer-based cyber-crimes. Computer Standards & Interfaces, no. 2, 2007, p. 216.

18 Peszleg Tibor: i. m. 26. o.

19 Shiuh-Jeng Wang: i. m. 218. o.

tó erejüket csak akkor tartják meg, ha megőrzik a beszerzésüket közvetlenül megelőző állapotukat, és így a vizsgálati eredmény reprodukálható marad.[20]

Házkutatás

A Be. 149. §-a ekként határozza meg a házkutatást: a ház, lakás, egyéb helyiség, az azokhoz tartozó bekerített hely vagy a jármű átkutatása, továbbá az ott elhelyezett információs rendszer vagy ilyen rendszerben tárolt adatokat tartalmazó adathordozó átvizsgálása az eljárás eredményessége érdekében. Az 1998-as Be. hatálybalépése előtt a felsorolás nem tartalmazott elektronikus adatokra vonatkozó kitételt, így vita folyt azzal kapcsolatban, hogy egy rendszer vagy adathordozó átvizsgálása házkutatásnak vagy pedig szemlének tekintendő-e.[21] Már az Európa Tanács R(95) 13. miniszteri bizottsági ajánlásának 6. pontja megfogalmazza azt az igényt, hogy a számítógépek átvizsgálására a házkutatás általános szabályai legyenek alkalmazhatók.

A Be. 152. § (1) bekezdés alapján a lefoglalás érdekében a házkutatás során – más keresett dolgokhoz hasonlóan – az információs rendszer vagy az ilyen rendszerben tárolt adatokat tartalmazó adathordozó birtokosát vagy az adat kezelőjét fel kell szólítani, hogy a tárolt adatot tegye hozzáférhetővé. A kért adatok átadása önmagában nem akadálya annak, hogy a házkutatás folytatódjon. A Be. 149. § (4) bekezdés szintén hasonló rendelkezést tartalmaz, itt azonban már szerepel az a kitétel, hogy a házkutatást be kell fejezni abban az esetben, ha a kért adatot a felszólítás után átadják. Ha más bizonyítási eszköz fellelése is valószínűsíthető, akkor azonban a kényszerintézkedés tovább folytatható.

A házkutatás fontos mozzanat a későbbi nyomozási cselekmények szempontjából, hiszen számos kérdés már ekkor eldönthető. Például vizsgálni kell azt, hogy ha található a házban wifi, akkor megfelelően védett-e jelszóval, ennek hiánya esetén ugyanis fennáll az a lehetőség, hogy valaki más kapcsolódott rá a vezeték nélküli hálózatra, és követte el az adott bűncselekményt.[22] A Nemzeti Nyomozó Irodánál töltött tudományos gyakornoki időm alatt elmondták, hogy ilyenkor gyakorlat az is, hogy az információs rendszerben olyan vizsgálatokat végeznek, amelyekre később már nem biztos, hogy lehetőség adódik. Például ha egy adatot felhőszolgáltatásban tárolnak, és a ház-

20 Tóth Fanni: Az informatikai bűnözéshez kapcsolódó kényszerintézkedések. Büntetőjogi Szemle, 2017/1., 79. o.

21 Laczi Beáta: i. m. 730. o.

22 Vadász Viktor: A számítógép demisztifikálása. Ügyészek Lapja, 2010/2., 30. o.

kutatás során a rendszerből elérhető, érdemes még akkor elvégezni a vizsgálatát, mivel később az internetre csatlakozás már veszélyeztetheti az adathordozón található adatok integritását.

A kiberbűncselekmények szakképzett elkövetői számos módon igyekeznek kijátszani a nyomozó hatóságot. Ezek közül az egyik, ha az illegális adatokat (például gyermekpornográfiát) elkülönített adathordozón vagy rendszerben tárolják, amit gondosan elrejtenek. Napjainkban például a pendrive-ok gyakran egyszerű hétköznapi tárgyaknak látszanak, így problémás lehet ezek mindegyikét felkutatni. További nehézséget okozhat az is, ha az eljárást megelőzően az elkövető a rendszerét vagy annak egy részét titkosítással látja el. A titkosított adatok nem megismerhetők a nyomozó hatóság számára, így a bizonyításban sem használhatók fel. Némelyik titkosítás könnyedén feltörhető a nyomozó hatóság által, míg például a VeraCrypt 256 bites titkosítása a gyakorlatban nem fejthető meg belátható időn belül. Kérdésként vetődik fel tehát, hogy a titkosítást feloldó kulcs átadására kötelezhető-e a terhelt. Bizonyos államokban, így például Franciaországban a btk. 434-15-2. szakasza szerint bűncselekményként értékelendő a jelszó hatóság részére történő átadásának megtagadása, míg például Németországban különleges rendőri egységek bevetésével, rajtaütésszerű házkutatással kívánják ennek elejét venni. Az Egyesült Államokban ezzel szemben az önvádra kötelezés tilalmába ütközőnek találták az ilyen kötelezést, hiszen ezzel a terhelt tulajdonképpen elismeri, hogy rendelkezik a rendszerben található jogsértő adatok felett.[23] Úgy gondolom, mindkét megoldás mögött fontos érvek állnak: míg az egyik álláspont az állam büntetőigényét, addig a másik a polgárok jogait tartja fontosabbnak. A különbség elsősorban értékrendbeli, így a kérdésben nehéz objektív módon állást foglalni.

Az új Be. 302. §-a immár kutatásként hivatkozik a kényszerintézkedésre, amely az indokolás szerint jobban illeszkedik annak tartalmához, hiszen nemcsak ház, de jármű és információs rendszer is lehet tárgya. A kutatás elrendelésének köre kibővül a hatályos törvényhez képest, így az eddigi esetek mellett akkor is alkalmazható, ha elkobozható, illetve vagyonelkobzás alá eső dolog megtalálására vagy információs rendszer, illetve adathordozó átvizsgálására vezet. Utóbbi abban különbözik a „bizonyítási eszköz megtalálása" esetétől, hogy itt az ezeken az eszközökön tárolt elektronikus adat tekinthető bizonyítási eszköznek, így a kitétel külön történő szerepeltetése indokolt.

23 Susan W. Brenner: Budapesti Law – A United States Perspective. In: Eoghan Casey (ed.): Digital Evidence and Computer Crime. Academic Press, 2011, pp. 115–118.

Lefoglalás

A Be. 151. § (1) alapján a lefoglalás célja a bizonyítási eszköz biztonságba helyezése a bizonyítás érdekében, illetve az elkobzás, vagyonelkobzás alá eső dolgok biztosítása, és ennek érdekében vonja el a rendelkezési jogot a birtokostól. A jogintézménynek nagyon fontos szerepe van a kibertérben elkövetett bűncselekmények üldözésében az elektronikus bizonyítékok megszerzésének és megőrzésének egyik eszközeként.

Kemény viták folynak azzal kapcsolatban, hogy pontosan mit is kell az eljárás során lefoglalni: a teljes információs rendszert, az adathordozót vagy pedig csak magát az adatot. A hatályos Be. 151. § (2) bekezdése mindháromra lehetőséget teremt, ezzel széles mozgásteret kínálva a nyomozó hatóságnak. Az adat lefoglalását a 2013. évi CLXXXVI. törvény 21. §-a illesztette be a törvény szövegébe, 2014. január 1-jei hatállyal. Ezt megelőzően bevett gyakorlat volt a számítógép egészét lefoglalni (sokszor a büntetőeljárás szempontjából lényegtelen hardvereszközökkel, például a monitorral, billentyűzettel együtt), később azonban sokszor már csak a merevlemezt, majd a Be. módosítása után csak magát az adatot foglalták le. *Vadász Viktor* ugyanakkor nem ért egyet ezzel a tendenciával, 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 folyamán.[24] Ezekkel a megállapításokkal egyetértve elengedhetetlen megjegyezni, hogy az adat lefoglalásának akkor lehet igazán jelentősége, ha azt olyan rendszerre alkalmazzák, amely nem az elkövetés eszköze volt, de valamilyen nyomozási szempontból fontos adatot tartalmazhat (például a bűncselekmény által érintett rendszer), hiszen ebben az esetben túlzott sérelmet okozhatna a használónak a rendszer hosszabb időre történő teljes lefoglalása. A törvény ugyanakkor nem él ezzel a distinkcióval, így ennek kidolgozása a gyakorlatra váró feladat.

Ennek gyakorlati végrehajtására kétféle megoldás létezik: a rendszer helyszíni átvizsgálása után meghatározzák az átmásolandó adatok körét vagy pedig az egész rendszerről készítenek hash kulccsal ellátott másolatot, így garantálva az adatok hitelességét.[25] Előbbi módszer kisebb mennyiségű információ esetén jól alkalmazható, ugyanakkor a bizonyításnál problémát okozhat, mivel az eredmény már nem reprodukálható az eredeti rendszerből.

24 Vadász Viktor: i. m. 20. o.
25 Sorbán Kinga: i. m. 88–89. o.

Adathordozók önmagában történő lefoglalása is problémás lehet, hiszen ha a merevlemezt eltávolítják az egyedi környezetéből, a programok nagy része már nem lesz elindítható, valamint a verziószám, és számos releváns tényező se lesz már megállapítható.[26] Az is elképzelhető, hogy a lefoglalt adathordozó inkompatibilis a vizsgáló rendszerével, és bizonyos eszközöknél (például RAID tömbök) az egység megbontása lehetetlenné teszi az adattartalom visszaállítását.[27] Előfordult, hogy bizonyos adatokat nem közvetlenül az adathordozón, hanem például egy felhőszolgáltatást igénybe véve tárolnak, és ezeket az adott rendszer segítségével lehet a legkönnyebben elérni.

Ez alapján egyértelműen kijelenthető, hogy a nyomozás érdekeit az szolgálja leginkább, ha az egész rendszert foglalja le a nyomozó hatóság, ez ráadásul különösebb informatikai szakértelmet sem igényel. Figyelembe kell azonban venni, hogy egy teljes rendszer lefoglalása súlyos jogsértésekkel, és akár károkkal is járhat. Egyrészt a technológia folyamatos avulása miatti jelentős értékvesztésként valósulhat meg egy elhúzódó eljárás, de akár egy vállalkozás működését is ellehetetlenítheti.[28] Másrészt, adatvédelmi szempontból is aggályos lehet a lefoglalás, főként ha az több személy adatait is tartalmazza. A rendőrségről szóló 1994. évi XXXIV. törvény 90. szakasza előírja, hogy bűnüldözési célra azok a személyes adatok kezelhetők, amelyek tényleges veszély elhárításához, illetve meghatározott bűncselekmény megelőzéséhez, felderítéséhez, bizonyításához szükségesek. Az adatvédelmi biztos 2009-es állásfoglalásában úgy találta, hogy az eljáráshoz nem szükséges adatokhoz való hozzáférés csak észszerű időtartamra korlátozható, és az ügyben felvetődő féléves lefoglalás már túlmutat ezen.[29]

A fő problémát véleményem szerint az jelenti ezzel összefüggésben, hogy az adatokat mindenképp át kell vizsgálni a büntetőjogi szempontból releváns információk (például gyermekpornográfiát ábrázoló felvételek) megtalálása és lefoglalása érdekében. Különösen igaz ez, ha feltehető, hogy az elkövetők valamilyen módszerrel, például szteganográfiával igyekeztek leplezni magukat.[30] Így az eljáró hatóság mindenképp megismeri az információs rendszerben található adatokat, legyenek azok bármennyire érzékenyek. Mint ko-

26 Vadász Viktor: i. m. 30. o.

27 Sorbán Kinga: i. m. 88. o.

28 Uo. 87. o.

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

30 A szteganográfia a rejtett üzenetek létrehozásának egy formája, informatikai környezetben úgy valósítható meg, hogy a tiltott tartalmat (például gyermekpornográfia) egy másik, legális tartalom mögé rejtik el. Mohamed Chawki: Online Child Sexual Abuse: The French Response. Journal of Digital Forensics, Security and Law, no. 4, 2009, pp. 11–12.

rábban utaltam már rá, ezek a rendszerek, adathordozók olyan adatokat tartalmazhatnak, amelyek alapján a birtokos teljes élete feltérképezhető. Személyes felvételek, elektronikus számlák és banki kivonatok, orvosi leletek, vallási, politikai meggyőződésre utaló információk, számos egyéb magánjellegű adat található a rendszerekben, és általában a használó kapcsolati köre is feltérképezhető ezek alapján.[31] A németországi szövetségi alkotmánybíróság az információs technika személyiség kibontakoztatására gyakorolt nagy hatása miatt döntött úgy 2008-ban, hogy új alapjogként az információs önrendelkezési jogból levezeti az információs rendszer bizalmasságához és integritásához való jogot.[32] A döntés külön tényezőként emelte ki azt a tényt is, hogy itt akár harmadik, a büntetőeljárásban nem érintett személyek adatai is megismerhetővé válnak.

Jelenleg nincs a világon sehol olyan megoldás, amely ezt a súlyos ellentétet feloldaná, és a tendenciák a lehetséges kár mérséklése irányába mutatnak. Az adatvédelmi biztos 2009-es jelentése kapcsán ismertté vált a kapitányságí rendőrségi gyakorlat is, amely szerint a személyes adatokhoz csak az igazságügyi informatikai szakértő, az ügy előadója és elöljárói férhetnek hozzá, és olyan vizsgálati környezetben dolgoznak, ahonnan kizárják az illetékteleneket.[33] A Nemzeti Nyomozó Iroda gyakorlata alapján a lefoglalt rendszerről teljes másolatot készítenek, és ennek átvizsgálására kerül sor az eljárásban, ami szintén korlátozza az érzékeny adatokhoz hozzáférő személyek körét. Jelenleg úgy tűnik, hogy nem zárható ki teljesen ezen adatok megismerése a büntetőeljárás során, így a legjobb megoldás valóban az azokhoz hozzáférők körének minél erőteljesebb szűkítése.

Az új Be. által hozott változások

Az új Be. számos változást hoz a lefoglalás kapcsán, elsősorban az elektronikus bizonyítékgyűjtéssel összefüggésben. A törvény először az általános szabályokat tartalmazza, majd külön foglalkozik az okirat, illetve az elektronikus adat lefoglalásáról. A 308. § (3) bekezdéséből kikerült a korábbi hármas felsorolás, a törvény már nem nevesíti külön a rendszert és az adathordozót, csak az elektronikus adatot mint a lefoglalás tárgyát.

31 Az emberi méltóság, a személyiségi és kegyeleti jogok tiszteletben tartásának fontosságát hangsúlyozza Peszleg Tibor is. Lásd Peszleg Tibor: i. m. 23. o.

32 Mohácsi Barbara: Bűnüldözési érdek contra emberi jogok – az online házkutatás alkotmányossági megítélése Németországban, néhány tanulsággal. Magyar Jog, 2008/12., 829. o.

33 Trócsányi Sára: i. m.

Új szabályként került a 309. § (3) bekezdésébe a vádemelés előtt kizárólag ügyész, azt követően bíró által elrendelhető lefoglalás körébe a címzettnek még nem továbbított, elektronikus hírközlési szolgáltatás során továbbítandó közlés vagy küldemény, amelyet a jogalkotó a postai küldeményektől külön kezel. A gyakorlatban nem világos, mi tekinthető még el nem küldött elektronikus közlésnek, ahogy a továbbítottnak tekintendőség időpontját se határozzák meg, és e kérdésekre vonatkozóan az indokolás sem tartalmaz iránymutatást.

A lefoglalást fő szabályként birtokba vétellel kell végrehajtani, ez alól az új Be. 311. § (2) bek. három kivételt ismer. A lefoglalást az érintett őrizetében hagyással vagy a megőrzés más módon történő biztosításával lehet végrehajtani, ha

– a dolog birtokba vételre nem alkalmas;
– a dolog vagy elektronikus adat birtokosának, kezelőjének azok használatához fűződő érdeke ezt indokolja; vagy
– más fontos ok ezt szükségessé teszi.

Ez az információs rendszerben tárolt adat megőrzésére kötelezés kényszerintézkedéshez hasonló megoldás, ahol szintén a birtokos vagy kezelő őrizetében hagyják az adatokat. A hasonlóságot tovább erősíti, hogy a törvény 316. §-a immár nem önálló kényszerintézkedésként, hanem a lefoglalás részeként szabályozza a megőrzésre kötelezést. Az indokolás szerint ennek alapja az, hogy ez a lefoglalással analóg kényszerintézkedés. A kettő között a fő különbség azonban az, hogy míg a megőrzésre kötelezés a hatályos szabályozáshoz hasonlóan legfeljebb három hónapig, illetve az átvizsgálásig tarthat, addig itt nem szerepel ilyen kitétel.

A törvény 315. §-a a hatályos Be.-nél jóval részletesebben tartalmazza az elektronikus adat lefoglalásával kapcsolatos szabályokat. A szakasz (1) bekezdése alapján elektronikus adat lefoglalásának módja lehet

– elektronikus adatról másolat készítése;
– elektronikus adat áthelyezése;
– információs rendszer vagy adathordozó teljes tartalmáról történő másolat készítése;
– információs rendszer vagy adathordozó lefoglalása;
– egyéb, jogszabályban meghatározott mód.

A törvény indokolásából kitűnik, hogy a különböző módszerek között fokozatosság áll fenn, és ezt a szakasz további rendelkezései is megerősítik. A paragrafus (4) bekezdése szerint a lefoglalást úgy kell végrehajtani, hogy a bün-

tetőeljárás céljából szükségtelen elektronikus adatra lehetőleg ne terjedjen ki, illetve az ilyen elektronikus adatot a legrövidebb ideig érintse. Az (5) bekezdés határozza meg, mely esetekben lehetséges az egész rendszert vagy adathordozót lefoglalni: ha elkobozható, illetve vagyonelkobzás alá esik; ha tárgyi bizonyítási eszközként bír jelentőséggel; vagy ha a bizonyítás érdekében előre nem meghatározható vagy jelentős mennyiségű elektronikus adat átvizsgálására van szükség. Az érdeksérelem további mérséklését célozza a (6) bekezdés, amely szerint ilyen esetekben az elektronikus adattal rendelkezni jogosult kérésére másolatot kell készíteni az általa megjelölt elektronikus adatról, amennyiben ez a büntetőeljárás érdekét nem veszélyezteti. Utóbbi, mivel nem a lefoglalt rendszer birtokosát, hanem az adattal rendelkezni jogosultat nevezi meg kérelmezőként, lehetővé teszi, hogy mindazok a nyomozó hatósághoz forduljanak, akiknek adatát az adott rendszerben vagy adathordozón tárolták.

Bizonyos kérdésekben azonban az új Be. sem ad iránymutatást, így például arra vonatkozóan, hogy ha az információs rendszer vagy adathordozó és az adat más tulajdona, illetve ha egy rendszer több személy adatait is tartalmazza (például egy szervergép), akkor melyikre kell elrendelni a lefoglalást. Probléma lehet ilyen esetben annak eldöntése is, hogy kinek ad a törvény jogorvoslati lehetőséget. Ugyanis, ha a rendszerre nézve rendelik el a lefoglalást, akkor a nyomozó hatóság határozata csak annak tulajdonosára vonatkozóan tartalmaz közvetlen rendelkezést, de az adat tulajdonosára nem, így a hatályos Be. 195. §-a alapján csak ő jogosult panaszt tenni.

Bitcoin lefoglalása

Fontos új változtatást jelent még az új Be. 315. szakasz (2) bekezdése, amelyben a fizetésre használt elektronikus adat lefoglalásáról található rendelkezés. Ennek megértéséhez fontos megvizsgálni, pontosan mit is értünk az elektronikus pénz fogalmán. Többféle definíció létezik erre mind a szakirodalomban, mind jogszabályokban[34], én ezek közül az elektronikuspénz-kibocsátó intézmények tevékenységének megkezdéséről, folytatásáról és prudenciális felügyeletéről szóló 2009/110/EK irányelvet emelném ki, amely szerint az elektronikus pénz a kibocsátóval szembeni követelés által megtestesített, elektronikusan tárolt – ideértve a mágneses tárolást is – monetáris érték, ame-

34 Bővebben lásd Szathmáry Zoltán: Az elektronikus pénz és a bitcoin biztosítása a büntetőeljárásban. Magyar Jog, 2015/11., 639–641. o.

lyet pénzeszköz átvételével bocsátanak ki. Az egyik legismertebb a bitcoin, amely peer-to-peer hálózati működési elvű nyílt forráskódú úgynevezett kriptovaluta, amelynek alapja számítástechnikai rendszerek erőforrása. Maga a bitcoin egy generált adat, amely matematikai algoritmussal keletkezik a tranzakciók feldolgozása és jóváhagyása révén (ezt nevezik bányászásnak).[35] A bitcoin azonban nem tekinthető általános értelemben elektronikus pénznek, hiszen nincs kibocsátója, semmilyen szervezet nem gyakorol felügyeletet felette, és nem áll mögötte semmilyen vagyoni fedezet.[36] A bitcoin teljes anonimitást ad a használóknak, így sok esetben különböző bűncselekmények során használják fel azt, ami értelemszerűen a hatóságok figyelmét is ráirányítja a jelenségre.

A fő problémát a bitcoinnal – és minden más, hasonló technológián alapuló virtuális pénzzel – kapcsolatosan a hiányzó jogi dogmatika jelenti, hiszen mint Szathmáry is rámutat, vagyonelkobzás vagy polgári jogi igény biztosítása érdekében történő biztosítása tulajdonképpen legitimálja azt.[37] Az új Be. 315. § (2) bekezdése úgy szabályozza a kérdést, hogy a fizetésre használt elektronikus adat lefoglalását lehetővé teszi, végrehajtásáról pedig úgy rendelkezik, hogy annak során az elektronikus adattal olyan műveletet végeznek, amely megakadályozza az érintettnek az elektronikus adat által kifejezett vagyoni érték feletti rendelkezési lehetőségét. A törvény nem nevesíti kifejezetten a bitcoint, és az indokolás is csak példálózó jelleggel említi, de elterjedtsége miatt kijelenthető, hogy a rendelkezés apropóját a kriptovaluta egyre inkább elterjedt használata adta.

Elektronikus adat megőrzésére kötelezés

Eredete, fogalma

A jogintézmény alapja az Európa Tanács 2001-es, Budapesten aláírt, a számítástechnikai bűnözésről szóló egyezmény 16. cikke, amely a tárolt számítástechnikai adat gyors megőrzése elnevezést kapta. Ez előírja a tagállamoknak, hogy tegyék lehetővé az illetékes hatóságok számára számítástechnikai adatok megőrzésének elrendelését. A személy, akinek ellenőrzése alatt vagy birtokában az adatok vannak, legfeljebb kilencven napig kötelezhető megőrzésre. A

35 Lakatos Alexandra Anna: Az informatikai bűncselekmények és a bitcoin. Belügyi Szemle, 2017/1., 29. o.; Szathmáry Zoltán: i. m. 642– 643. o.

36 Lakatos Alexandra Anna: i. m. 30. o.

37 Szathmáry Zoltán: i. m. 645. o.

jogintézmény a lefoglalással ellentétben nem vonja el az adat birtoklásának jogát a kötelezettől. Fontos sajátossága még az is, hogy nemcsak bizonyítási eszközökre, de az azok begyűjtése érdekében a bűncselekménnyel összefüggésbe hozható bármilyen más adatra is kiterjed.[38]

A magyar Be.-be a 2002. évi I. törvény vezette be a jogintézményt számítástechnikai rendszer útján rögzített adatok megőrzésére kötelezés cím alatt, amely 2003. január 1-jén lépett hatályba, a törvény egészével együtt. A Be. 158/A §-ban szabályozott kényszerintézkedés elnevezése a bevezetése után tíz évvel megváltozott, és a *„számítástechnikai rendszer útján rögzített"* helyére *az „információs rendszerben tárolt"* kifejezés került (2013. évi CLXXXVI. törvény 72. §), mivel ez utóbbi jóval tágabb megfogalmazás, és a jogalkotó így igazodott a technika fejlődése által támasztott kihívásokhoz.[39] Hiszen napjainkban már nemcsak számítógépek, de más eszközök is érintettek lehetnek a kiberbűnözésben, például az okostelefonok. Az új Be. 316. §-a ismét változtat a megnevezésen, és az elektronikus adat megőrzésére kötelezést használja, amely összhangban áll a törvény többi változtatásával, vagyis az elektronikus adat mint bizonyítási eszköz megjelenésével.

A jogintézménnyel kapcsolatos fogalmi problémák korábban is jelen voltak, így például a nyomozás részletes szabályait tartalmazó 23/2003. (VI. 24.) BM–IM rendelet (a továbbiakban: Nyor.) 84. §-a még mindig a kényszerintézkedés 2013 előtti elnevezését használja. Hasonló módon felveti a módosítás igényét az új Be. megváltozott elnevezése is. A 2013. évi CLXXXVI. törvény a Btk. módosításával a 287. §-ban szabályozott zártörés tényállását módosítva kriminalizálta az információs rendszerben tárolt adatok megőrzésére kötelezéssel érintett adat jogosulatlan személy számára történő megismerhetővé tételét, eljárás alóli elvonását, illetve módosítását.

Szabályai

Az információs rendszerben tárolt adat megőrzését a nyomozó hatóság, az ügyész és a bíróság rendelheti el, ezzel ideiglenesen korlátozva az adat birtokosának, feldolgozójának, valamint kezelőjének az adat feletti rendelkezését. A Nyor. 84. §-a alapján az elrendelő határozatnak tartalmaznia kell a megőrzendő adatok körét, a Be. 158/A § meghatározott bekezdéseiben foglalt köte-

38 Villányi József: Az Európa Tanács Informatikai bűnözéssel kapcsolatos egyezményéről. Magyar Jog, 2001/8., 470. o.

39 Czine Ágnes: VIII. fejezet. In: Belegi József (szerk.): Büntetőeljárás I–III. Kommentár a gyakorlat számára. HVG-ORAC Kiadó, Budapest, 2014, 88. o.

lezettségeket, valamint fokozott biztonságú elektronikus aláírás vagy időbélyegző használata esetén az erre történő utalást. Ez utóbbira nem található utalás a Be. szövegében, gyakorlatilag annak igazolására szolgál, hogy az elhelyezése idején az adatok változatlan formában léteztek. A fokozott biztonságú elektronikus aláírást az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény 1. § 22. pontja a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról 910/2014/EU rendeletre utalással határozza meg. Ennek 26. cikke szerint a fokozott biztonságú elektronikus aláírás

– kizárólag az aláíróhoz köthető;
– alkalmas az aláíró azonosítására;
– olyan, elektronikus aláírás létrehozásához használt adatok felhasználásával alkotják meg, amelyeket az aláíró nagy megbízhatósággal kizárólag saját maga használhat;
– olyan módon kapcsolódik azokhoz az adatokhoz, amelyeket aláírtak vele, hogy az adatok minden későbbi változása nyomon követhető.

Ha az adatok kizárólag egy belső hálózaton (intranet) elérhetők, akkor a rendszergazdát kell kötelezni a megőrzésükre.[40]

A kényszerintézkedés célja nagyobb mennyiségű adat biztosítása a nyomozó hatóság számára átvizsgálás céljából. Ennek oka, hogy jelentősebb adathalmazra nem rendelhető el lefoglalás, hiszen meghatározhatatlan, mely adatok szükségesek[41], és ennek technikai végrehajtása is jelentős problémákba ütközne. A Be. 158/A § (7) bekezdésből kitűnik, hogy az elrendelés után az elrendelőnek haladéktalanul meg kell kezdenie az adatok átvizsgálását, és ennek nyomán az adatot információs rendszerbe vagy más adathordozóra történő átmásolással lefoglalni.

Ez előnyös lehet a nyomozó hatóság számára, hiszen nem kell nagyobb mennyiségű adat lefoglalásáról gondoskodniuk, és a kötelezett számára is, mivel a lefoglalással ellentétben itt hozzáférhet a kényszerintézkedés által érintett adatokhoz. A (3) bekezdés alapján azonban köteles az adatot változatlanul megőrizni, és – szükség esetén más adatállománytól elkülönítve – gondoskodni annak biztonságos tárolásáról. Ezen kívül meg kell akadályoznia az adat megváltoztatását, törlését, megsemmisülését, továbbítását, másolat jo-

40 Uo. 806. o.
41 Tóth Fanni: 77. o.

gosulatlan készítését, illetve az adathoz való jogosulatlan hozzáférést. A Nyor. 85. §-a arról rendelkezik, hogy a végrehajtásról jegyzőkönyvet kell felvenni. A Be. 158/A § (4) bekezdése további kötelezettségként állapítja meg a megőrzésre kötelezett részére, hogy tájékoztassa az elrendelőt arról, ha az érintett adatot jogosulatlanul megváltoztatták, törölték, átmásolták, továbbították, megismerték, vagy ha ezek megkísérlésére utaló jelet észlelt.

Mindezekből következik, hogy elrendelésre csak az elkövetésben nem érintett személyek esetén kerül sor, hiszen egyébként az eljárás sikerét veszélyeztetné az adatok birtokos rendelkezési körében történő hagyása. Erre utal a Kúria vonatkozó ítélete is[42], amely kimondja, hogy valaki *„a számára egyébként terhelő adatok megőrzésére nem kötelezhető”*. A gyakorlat is abba az irányba mutat, hogy csak a bűncselekményben nem érintett számítógépek esetén írják elő az adatok megőrzésére kötelezést, míg egyéb esetekben lefoglalásra kerül sor.[43]

Mivel a kötelezett általában nem kapcsolódik a büntetőeljáráshoz, így a méltányosság különösen fontos szerepet kap. Akárcsak más, bizonyítékok beszerzésére és biztosítására vonatkozó kényszerintézkedések esetén, itt is hangsúlyosan megjelenik a kötelezett kíméletének szándéka. Egyrészt a Be. 158/A § (8) bekezdése kilencven napban maximálja a megőrzési kötelezettség időtartamát, másrészt a (4) bekezdés lehetőséget teremt arra, hogy ha az adat eredeti helyen történő megőrzése a fő tevékenységet jelentősen zavarná, akkor az elrendelő engedélyével az adatokat másik adathordozón vagy rendszerben is tárolhatja.

Elektronikus adat ideiglenes hozzáférhetetlenné tétele

A tartalombűncselekmények elleni fellépés szükséges lehet, különösen az olyan súlyosan sértő tartalmak esetén, mint a gyermekpornográfia. Ennek napjainkban preferált eszköze a tartalomszűrés, vagyis a jogsértő tartalmak kiszűrése, majd eltávolítása vagy más módon történő elérhetetlenné tétele. A gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről szóló 2011/93/EU irányelve a gyermekpornográfiát tartalmazó vagy azt terjesztő weboldalak elleni intézkedések címet viselő 25. cikke teremt lehetőséget az állami tartalomszűrés bevezetésére. A

42 Kúria Pfv.IV.21.941/2012/5.
43 Tóth Fanni: i. m. 79. o.

cikk (2) bekezdése ugyanis kimondja, hogy a tagállamok – átlátható eljárás keretében, a megfelelő garanciák mellett, arányos és szükséges módon – intézkedéseket tehetnek a gyermekpornográfiát tartalmazó vagy azt terjesztő weboldalakhoz való hozzáférés meggátlására.

Az e rendelkezésnek való megfelelés érdekében került be a Btk. hatálybalépésével egy időben, 2013. július 1-jei hatállyal a Btk. 77. §-ba intézkedésként az adat végleges hozzáférhetetlenné tétele, valamint ennek eljárásjogi párjaként a Be. 158/B–D §-ba kényszerintézkedésként az elektronikus adat ideiglenes hozzáférhetetlenné tétele.[44] Utóbbival a jogalkotói cél az volt, hogy még a büntetőeljárás ideje alatt megszüntethető legyen a jogsértő állapot. A 158. § (1) bekezdése úgy határozza meg a kényszerintézkedést, mint az elektronikus hírközlő hálózat útján közzétett adat feletti rendelkezési jog ideiglenes korlátozását, és az adathoz való hozzáférés ideiglenes megakadályozását. A kényszerintézkedés kapcsán fogalmi pontatlanság érhető tetten: míg a kényszerintézkedés elnevezése *„elektronikus adat ideiglenes hozzáférhetetlenné tétele”,* addig a cím, amely alá tartozik, az *„elektronikus hírközlő hálózat útján közzétett adat”* fogalmát használja. Mint a bekezdésből is kitűnik, a kettő a törvény szerint felcserélhető, mindazonáltal az eltérő elnevezés használata indokolatlan, és valószínűleg jogalkotói figyelmetlenség következménye.

A kényszerintézkedés elrendelésének feltételeit a paragrafus (2) bekezdése tartalmazza. E szerint az adat ideiglenes hozzáférhetetlenné tétele alkalmazásának akkor van helye, ha az eljárás olyan közvádra üldözendő bűncselekmény miatt folyik, amellyel kapcsolatban elektronikus adat végleges hozzáférhetetlenné tételének van helye, és az a bűncselekmény folytatásának megakadályozásához szükséges. A Btk. 77. § (1) bekezdése alapján véglegesen hozzáférhetetlenné kell tenni az olyan elektronikus adatokat,

– amelynek hozzáférhetővé tétele vagy közzététele bűncselekményt valósít meg;
– amelyet a bűncselekmény elkövetéséhez eszközül használtak; vagy
– amely bűncselekmény elkövetése útján jött létre.

A Be. 159/C § (1) bekezdése alapján a kényszerintézkedés kötelezettje nem az adat birtokosa, hanem a tárhelyszolgáltató, az ő együttműködése híján pedig az elektronikus hírközlési szolgáltató. A közvetítő szolgáltató fogalmát az elektronikus kereskedelmi szolgáltatások, valamint az információs társada-

44 Uo. 81. o.

lommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény 2. § l) pontja határozza meg, ennek a körnek a része az igénybe vevő által biztosított információt tároló tárhelyszolgáltató is. Mivel mind a Be., mind az e törvény 12/A §-a is csak ezt a szűkebb kört jelöli ki a kényszerintézkedés kötelezettjeként, arra más közvetítő szolgáltatók (például gyorsítótárat kínáló) nem kötelezhetők.[45]

A Be. 158/B § (4) bekezdése alapján a kényszerintézkedés elrendelhető elektronikus adat ideiglenes eltávolításával (158/C §), illetve elektronikus adathoz való hozzáférés ideiglenes megakadályozásával (158/D §), és a rendelkezést a magyar jogrendbe beiktató 2013. évi LXXVIII. törvény indokolása egyértelművé teszi a kettő közötti fokozatosság meglétét.[46] A törvény az eltávolítást preferálja, és a bíróság először a tárhelyszolgáltatót kötelezi a tartalom eltávolítására, aminek egy munkanapon belül eleget kell tennie. A határozat tartalmát az 11/2014. (XII. 13.) IM rendelet 142. §-a tartalmazza, e szerint az elektronikus adat forrását a következők megadásával kell azonosítani:

– IP-cím ipv4 vagy ipv6 szabvány szerint és alhálózati maszk;
– doménnév;
– URL-cím;
– portszám.

A szolgáltató kötelezettsége nemcsak az adat eltávolítására, de a Be. 158/C § (4) bekezdése alapján az adat visszaállítására is kiterjed, a határozat közlésétől számított egy munkanapon belül. A bíróság a (2) bekezdés alapján elrendeli az adat visszaállítását, amennyiben megszűnt az elrendelés oka, vagy ha megszüntetik a nyomozást, és nem rendelik el a Btk. 77. § szerinti végleges hozzáférhetetlenné tételt. Hasonlóan megszűnik az ideiglenes eltávolítás, hogyha befejeződik a büntetőeljárás. Amennyiben a szolgáltató valamely kötelezettségét elmulasztja teljesíteni, rendbírsággal sújtható, amelynek összege eltér a rendbírság általános szabályainál meghatározottól.

Ha a tárhelyszolgáltató eltávolítási kötelezettségét nem teljesítette vagy az eltávolításra vonatkozóan külföldi jogsegély iránti megkeresés harminc napon belül nem vezetett eredményre, akkor a Be. 158/D § (1) bek. b) pontjában taxatíve felsorolt kilenc bűncselekményi kör esetén helye van a hozzáférés ideiglenes megakadályozása elrendelésének. Ennek kötelezettje már nem a tárhelyszolgáltató, hanem az elektronikus hírközlési szolgáltatók, a végre-

45 Gaiderné Hartmann Tímea: Elektronikus adatok ideiglenes és végleges hozzáférhetetlenné tétele – egy új intézmény első évei. Magyar Jog, 2015/2.,109. o.
46 http://www.parlament.hu/irom39/09246/09246.pdf

hajtást pedig a Nemzeti Média- és Hírközlési Hatóság felügyeli, a határozat és az elektronikus adat elérésének a központi elektronikus hozzáférhetetlenné tételi határozatok adatbázisában történő rögzítéssel.[47]

Az új Be. 335–338. §-a tartalmazza a kényszerintézkedésre vonatkozó szabályokat. Az észrevehető legnagyobb különbség, hogy már élesen elkülönül egymástól az adat ideiglenes eltávolítása és a hozzáférés ideiglenes megakadályozása. A fejezet első része a két elrendelési mód közös szabályait tartalmazza, majd ezt követően külön-külön foglalkozik a specifikus szabályokkal. A hozzáférés ideiglenes megakadályozásának szövegezése módosult, és véleményem szerint a zárt bűncselekményi lista előrébb helyezése, és az eddig nehezen érthetően megfogalmazott két konjunktív feltétel egyben történő megfogalmazása mind dogmatikailag, mind közérthetőség szempontjából is jóval előnyösebb szerkesztési megoldás.[48] A lényegi változások körében kiemelendő, hogy a hozzáférés megakadályozását megelőző eltávolítás sikertelenségével kapcsolatos listát két új tétellel is kiegészíti a törvény. Így megalapozhatja az alkalmazását az is, ha az eltávolításra kötelezett azonosítása lehetetlen vagy aránytalan nehézséggel járna, illetve ha az elektronikus adat ideiglenes eltávolítására vonatkozóan a külföldi hatóság jogsegély iránti megkeresésétől eredmény nem várható vagy a megkeresés aránytalan nehézséggel járna.

A jogintézményt már javaslatként való felvetésének pillanatától kezdve kemény viták övezték. Egyebek között a Társaság a Szabadságjogokért (TASZ) részéről, amely túlságosan tágnak gondolta az eltávolítható tartalmak meghatározását, és zárt felsorolást javasolt alkalmazni, amely végső soron meg is jelent a fokozatosság formájában.[49] Azonban míg a tételes felsorolás kezdetben a gyermekpornográfiát, az állam elleni bűncselekményt és a terrorcselekményt foglalta magában, később a 2015. évi LXXVI. törvény tágította ennek körét, így napjainkban már kilenc bűncselekmény esetén rendelhető el az ideiglenes hozzáférhetetlenné tétel. A legnagyobb vitát az internetes tartalomszűrés szólásszabadságot befolyásoló lehetséges következményei szülték, hiszen a jogintézményt a világ számos országában – mint például Oroszország, Kína és Törökország – használják különböző mértékű politikai cenzúrára. Hazánkban – mivel a határozatokat tároló központi elektronikus hozzáférhetetlenné tételi határozatok adatbázisa csak a Nemzeti Mé-

47 Az eljárás pontos részleteiről bővebben lásd Gaiderné Hartmann Tímea: i. m. 113. o.

48 Így például elkerülhetők az olyan félreértések is, miszerint a két feltételt külön-külön esetkörnek, és nem összetartozónak vélik. Például lásd Gaiderné Hartmann Tímea: i. m. 112.

49 A Társaság a Szabadságjogokért véleménye. https://tasz.hu/files/tasz/imce/2011/tasz_velemeny_20121026.pdf

dia- és Hírközlési Hatóság és az elektronikus hírközlési szolgáltatók számára hozzáférhető – hiányzik a jogintézmény feletti társadalmi kontroll, ami aggályokat vet fel. További probléma a rendszer technikai kiforratlansága, és a jogintézmény kiforratlanságát mutatja az is, hogy 2016-ban a központi elektronikus hozzáférhetetlenné tételi határozatok adatbázisának rendszerében nulla bejegyzés szerepelt.[50]

Mindamellett technikai nehézségek is bőségesen felvetődnek, így például, hogy a szűrés technikájától függően nagy az esélye annak, hogy túlszűrés (vagyis nem jogsértő tartalmak korlátozása), illetve alulszűrés (jogsértő tartalmak továbbra is elérhetők) valósuljon meg. A szűrés bevezetése pontosan ezen bukott meg Németországban.[51] Ez a fajta hibalehetőség kikerülhető, ha – mint azt például véleményében a TASZ is megfogalmazza – a hozzáférhetetlenné tétel csak az URL-címre terjed ki. Ugyanakkor ez a megoldás a legkönnyebben kijátszható, hiszen elegendő a tartalmat egyszerűen más URL-címre mozgatni, hogy újra mindenhol, bárki számára elérhetővé váljon. *Gaiderné Hartmann Tímea* és *Ficsór Gabriella* véleménye szerint azonban ez kiküszöbölhető lenne azzal, ha a bírósági határozat nem a hozzáférhetetlenné tenni rendelt adatelérés útját, hanem az adattartalmat jelölné meg.[52]

A legsúlyosabb gond azonban, hogy a tartalomszűrés napjainkra egyre kevésbé alkalmas az eredetileg kijelölt céljára, az online gyermekpornográfia elleni fellépésre, hiszen annak fő területe már nem a tartalomszűrés által érintett nyílt web. A jogintézmény által érintett területek folyamatos kiterjesztése (például a tiltott szerencsejáték-szervezést megvalósító és a hamis vagy nem engedélyezett gyógyszert forgalmazó oldalakra) is egyre inkább eltolódást mutat az eredeti alkalmazási körtől, és ennek kapcsán sokan kifejezték az aggályaikat.[53]

Összegzés

Tanulmányomban igyekeztem átfogó képet nyújtani a kibertérben elkövetett bűncselekményekkel kapcsolatban alkalmazható kényszerintézkedések sza-

50 Gyömbér Béla: Így működik az állami internetcenzúra Magyarországon. 2017 https://jogalappal.hu/igy_mukodik_az_internetcenzura_magyarorszagon/

51 Parti Katalin: „10 dolog, amit utálok benned", avagy a kormányzati szintű internet-blokkolás kritikája a német törvény kapcsán. Infokommunikáció és Jog, 2010/38., 97–98. o.

52 Gaiderné Hartmann Tímea: i. m. 115. o.

53 Detrekői Zsuzsa: Blokkolás Magyarországon – hogyan jutottunk el a gyermekpornográfia elleni küzdelemtől a szerencsejáték-oldalak blokkolásáig. Infokommunikáció és Jog, 2014/60., 185–187. o.; Tóth Fanni: i. m. 85. o.

bályairól, kihívásairól, esetleges hibáiról. Mint a büntetőeljárás-jog sok más, a digitális forradalom által érintett területén, itt is elengedhetetlen a technika fejlődésével egyszerre történő haladás, méghozzá úgy, hogy ne szülessen belőle túlzottan nagy terjedelmű és követhetetlen, és így alkalmazhatatlan joganyag.

Véleményem szerint az új Be. szabályozása szinte minden kapcsolódó jogintézménynél a megfelelő irányba tett lépéseket, régóta fennálló dogmatikai vitákat és nehezen megítélhető helyzeteket szüntetve meg. Példaként említeném az elektronikus adat önálló bizonyítási eszközként való megjelenését, illetve az adatok lefoglalásával kapcsolatos szabályok sokkal részletesebb kidolgozását.

Bizonyos kérdésekben azonban nem tartalmaz új rendelkezéseket a törvény, így például arra, a mindennapi életben gyakran előforduló esetre, amikor más az információs rendszer és az adat tulajdonosa, illetve több személy adatai is ugyanabban a rendszerben találhatók. Ez különösen a lefoglalásnál idézhet elő jogilag nehezen feloldható helyzeteket. Mindamellett, ahogy az új Be. is bizonyítja, ezek a problémák nem megoldhatatlanok, és reményeim szerint a mostani tendencia a jövőben is folytatódik, tovább javítva a kapcsolódó kényszerintézkedések szabályrendszerén, illetve ezek gyakorlatán.

IRODALOM

Andreea, Vertes-Oltenau: Evolution of the Criminal Legal Frameworks for Preventing and Combating Cybercrime. *Journal of Eastern-European Criminal Law,* no. 1, 2014

Berecz Péter: A Német Szövetségi Alkotmánybíróság „számítógép-határozata". *Studia Juvenum,* 2009/1.

Brenner, Susan W.: Budapesti Law – A United States Perspective. In: **Casey, Eoghan (ed.):** Digital Evidence and Computer Crime. Academic Press, 2011, pp. 115–118.

Casey, Eoghan: Foundations of Digital Forensics. In: **Casey, Eoghan (ed.):** Digital Evidence and Computer Crime. Academic Press, 2011

Chawki, Mohamed: Online Child Sexual Abuse: The French Response. *Journal of Digital Forensics, Security and Law,* no. 4, 2009

Czine Ágnes: VIII. fejezet. In: **Belegi József (szerk.):** Büntetőeljárás I–III. Kommentár a gyakorlat számára. HVG-ORAC Kiadó, Budapest, 2014

Detrekői Zsuzsa: Blokkolás Magyarországon – hogyan jutottunk el a gyermekpornográfia elleni küzdelemtől a szerencsejáték-oldalak blokkolásáig. *Infokommunikáció és Jog,* 2014/60.

Gaiderné Hartmann Tímea: Elektronikus adatok ideiglenes és végleges hozzáférhetetlenné tétele – egy új intézmény első évei. *Magyar Jog,* 2015/2.

Gropeneanu, Antonela – Iacob, Adrian: Investigative issues regarding cybercrime. *European Journal of Public Order and National Security,* no. 2, 2016

Gyömbér Béla: Így működik az állami internetcenzúra Magyarországon. 2017. https://jogalappal.hu/igy_mukodik_az_internetcenzura_magyarorszagon/

Király Tibor: Büntetőeljárási jog. Osiris Kiadó, Budapest, 2003

Laczi Beáta: A számítógépes környezetben elkövetett bűncselekmények nyomozásának és a nyomozás felügyeletének speciális kérdései. *Magyar Jog,* 2001/12.

Lakatos Alexandra Anna: Az informatikai bűncselekmények és a bitcoin. *Belügyi Szemle,* 2017/1.

Mohácsi Barbara: Bűnüldözési érdek contra emberi jogok – az online házkutatás alkotmányossági megítélése Németországban, néhány tanulsággal. *Magyar Jog,* 2008/12.

Nagy Zoltán, András – Mezei, Kitti: The organised criminal phenomenon on the Internet. *Journal of Eastern-European Criminal Law,* no. 2, 2016

Parti Katalin: Tiltott pornográf felvétellel visszaélés az interneten – az empirikus kutatás adatai. In: **Virág György (szerk.):** Kriminológiai Tanulmányok, 44. OKRI, Budapest, 2007, 98. o.

Parti Katalin: „10 dolog, amit utálok benned", avagy a kormányzati szintű internet-blokkolás kritikája a német törvény kapcsán. *Infokommunikáció és Jog,* 2010/38.

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

Róth Erika: A kényszerintézkedések változó rendszere és részletszabályai. *Ügyészek Lapja,* 2016/3–4.

Sorbán Kinga: A digitális bizonyíték a büntetőeljárásban. *Belügyi Szemle,* 2016/11.

Szádeczky Tamás: Az IT biztonság szabályozásának konfliktusa. *Infokommunikáció és Jog,* 2013/3.

Szathmáry Zoltán: Az elektronikus pénz és a bitcoin biztosítása a büntetőeljárásban. *Magyar Jog,* 2015/11.

Tóth Fanni: Az informatikai bűnözéshez kapcsolódó kényszerintézkedések. *Büntetőjogi Szemle,* 2017/1.

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

Vadász Viktor: A számítógép demisztifikálása. *Ügyészek Lapja,* 2010/2.

Villányi József: Az Európa Tanács Informatikai bűnözéssel kapcsolatos egyezményéről. *Magyar Jog,* 2001/8.

Wang, Shiuh-Jeng: Measures of retaining digital evidence to prosecute computer-based cyber-crimes. *Computer Standards & Interfaces,* no. 2, 2007