SZABÓ IMRE

A számítástechnikai adat mint elektronikus bizonyíték

A magyar szabályozás elemzése az Európa Tanács számítástechnikai bűnözésről szóló egyezménye alapján

Az elektronikus bizonyítékok vonatkozásában a számítástechnikai adatoknak van kiemelt jelentőségük, amelyek körében három adatkör határolható el: a forgalomra vonatkozó adatok (traffic data)*, az előfizetőre vonatkozó adatok* (subscriber data) *és a tartalomra vonatkozó adatok* (content data) *köre. A különböző típusú adatok – tekintettel azok különböző szenzitivitására – eltérő eszközök igénybevételével ismerhetők meg a hatóságok által. A dolgozatban a számítástechnikai adatok megszerzésének jogintézményeit mutatom be.*

Bevezetés

A számítástechnikai hálózati környezetben megvalósuló bűnözés elleni harc egyik legnagyobb próbatétele az elkövető azonosítása és konkrét magatartásának, valamint a magatartása következményeinek a meghatározása. A probléma oka az informatika sajátosságaiból adódik, nevezetesen, hogy a számítástechnikai adatok könnyen megsemmisülhetnek, eltűnhetnek. Ráadásul a számítástechnikai adatok másodpercek alatt megváltoztathatók, mozgathatók vagy törölhetők. A nyomozás sikerének a kulcsa így annak hatékonyságában és a nyomozás titkosságában keresendő.

Az informatikai bűncselekmények nagy számban számítástechnikai rendszereken folytatott kommunikáció[1] továbbításának eredményeként valósulnak meg. Ezek a kommunikációs elemek tartalmazhatnak illegális tartalmakat (például tiltott pornográf felvételek), számítógépes vírusokat vagy más informatikai utasításokat, amelyek interferenciát okoznak a számítástechnikai adatokban vagy más rendszerfunkcióban.

Az informatikai bűncselekmények esetében az egyes cselekmények megtörténtét, az elkövetés körülményeit informatikai környezetből kell a hatóságoknak

[1] A kommunikáció a dolgozatban az informatikai adatközlésre vonatkozó kommunikációt jelöli.

megismerniük, amihez mind a felderítés szakaszában, mind a büntetőeljárás során speciális szabályok, jogintézmények állnak a rendelkezésükre.

Az esetek többségében a számítástechnikai rendszer adathordozója tárolja azt az információt, amelyre a nyomozó hatóságnak a bűncselekmény bizonyításához szüksége van. További információkat hordozhatnak például a különböző szoftverek által generált ideiglenes állományok (.temp fájlok stb.), de valamely input vagy output eszköz is szolgáltathat bizonyítékot az elkövetés körülményeire. Ezeken túlmenően fontos információkat hordozó számítástechnikai adatok vannak a hálózatok működéséért felelős számítógépeken, vagyis azokon a számítástechnikai rendszereken, amelyek elengedhetetlen szerepet játszanak a több számítástechnikai berendezés összekapcsolásával létrejövő számítástechnikai hálózatokban zajló kommunikáció szervezésében. Ezek az adatok arra vonatkozóan hordoznak információt, hogy a számítástechnikai rendszerek mikor milyen számítástechnikai adat közvetítésében vettek részt, az honnan érkezett hozzájuk, és melyik számítógépre kellett továbbirányítaniuk.

A számítástechnikai adat mint elektronikus bizonyíték

Az Európa Tanács számítástechnikai bűnözésről szóló egyezményének (Cyber-Crime Convention, a továbbiakban: CCC) definíciói között található a számítástechnikai adat fogalma. A definíció az ISO szabvány adatfogalmára épít. A CCC 1. cikke alapján a *számítástechnikai adat információknak, tényeknek, fogalmaknak olyan formában való megjelenése, mely a számítástechnikai feldolgozásra alkalmas, ideértve azon programot is, mely valamely funkciónak a számítástechnikai rendszer általi végrehajtását biztosítja*. Szemantikus síkon az adat az információt jelenti. Azonban nemcsak emberi közlést kell ezen érteni, hanem egy számítástechnikai berendezés által önállóan előállított és egy másik gép vagy szoftver számára nyújtott utasításokat is. A definíció értelmében tehát egy digitális fénykép ugyanúgy számítástechnikai adatnak minősül, mint egy szöveges dokumentum, vagy valamely operációs rendszer a maga egészében, vagy annak egy részfunkciót megvalósító programja is.

A számítástechnikai adatok adattípusai: a forgalomra, az előfizetőre és a tartalomra vonatkozó adatok[2]

Három tipikus adattípust lehet megkülönböztetni a számítástechnikai adatok körében, azok statikus állapotában: forgalomra vonatkozó adatok *(traffic data)*,

[2] A számítástechnikai adatok csoportosításának alapját a CCC szerinti adatkörök adják.

tartalomra vonatkozó adatok *(content data)* és az előfizetőre vonatkozó adatok *(subscriber data).* Az adatok azonban csoportosíthatók dinamikájuk szerint is: tárolt adatokra és a kommunikációs folyamatban részt vevő adatokra bonthatók. Ez utóbbi csoportosítás lényege, hogy a tárolt adatok vonatkozásában azok megismerését illetően más típusú jogintézmények állnak a hatóság rendelkezésére, mint a valós idejű kommunikáció során történő adattovábbítás megismerésére.

A forgalomra vonatkozó adatok közé tartoznak a különböző szerverek fel- és letöltését naplózó adatállományok, elektronikus postafiók elérését regisztráló adatállományok, biztonságtechnikai programokban tárolt információk stb., amelyek a kommunikáció forrása és címzettje számítógépeinek azonosítását segíthetik elő. A CCC ezen kívül megkülönbözteti még az előfizetői adatok, valamint a tartalomra vonatkozó adatok körét. Az előfizetőre vonatkozó adatok az adott kommunikáció címzettjének vagy forrásának a személyazonosításhoz szükséges adatai, míg a tartalomra vonatkozó adatok a kommunikáció információtartalmát takarják.

A forgalomra vonatkozó adat

A forgalomra vonatkozó adatot kommunikációs kapcsolatban lévő számítógépek generálják annak érdekében, hogy a kommunikációt az eredetéből a céljához irányítsák. A CCC definíciója szerint a forgalomra vonatkozó adat minden olyan, a számítástechnikai rendszeren átmenő és a számítástechnikai rendszer mint a kommunikációs lánc egyik eleme által létrehozott kommunikációra vonatkozó adat, amely jelzi a kommunikáció származási és rendeltetési helyét, útvonalát, óráját, napját, terjedelmét és időtartamát vagy a szolgáltatás típusát.[3]

A hazai jogban a forgalomra vonatkozó adatfogalom megnevezés helyett a kísérő adat került megfogalmazásra. E szerint kísérő adatokon az elektronikus hírközlési szolgáltató hálózatában és azzal összefüggő informatikai rendszereiben az adott kommunikációval összefüggésben az adott szolgáltatás teljesítésével kapcsolatban keletkező, illetve az elektronikus hírközlési szolgáltató hálózatában rendelkezésre álló adatokat kell érteni.[4]

Ez a megfogalmazás felveti azonban azt a kérdést, hogy mi a helyzet azokkal a közvetítő szolgáltatókkal, amelyek nem nyújtanak elektronikus hírközlési szolgáltatást, csak információs társadalommal összefüggő szolgáltatást. E szolgáltatók vonatkozásán keletkezhetnek a forgalomra vonatkozó adatok (például egy privát oldal fórumregisztrációja során keletkező adatok), a jelenlegi szabályok szerint

[3] 2001. évi CXXI. törvény miniszteri indokolása.
[4] 180/2004. (V. 26.) kormányrendelet (a továbbiakban: adatszolgáltatási rendelet) 2. § e) pont.

azonban velük kapcsolatosan nem alkalmazhatók azok a jogintézmények, amelyek az elektronikus hírközlési szolgáltatók vonatkozásában igen.

Az előfizetőre vonatkozó adat

Az előfizetőre vonatkozó adat[5] bármely számítástechnikai adat formájában vagy más formában megjelenő, az adott szolgáltató által birtokolt, előfizetőkkel kapcsolatos, a tartalomra vagy a forgalomra vonatkozó adatoktól eltérő információ, amely lehetővé teszi, hogy megállapítsák az előfizető által használt kommunikációs szolgáltatás típusát, az erre vonatkozóan tett technikai intézkedéseket, valamint a szolgáltatás időszakát. Ezeken túlmenően idesoroljuk az előfizető személyazonosságát, postai vagy földrajzi címét, telefonszámát vagy más elérhetőségét, a fizetésre és a számlázásra vonatkozó adatokat (amelyek szolgáltatási szerződés vagy megállapodás alapján állnak a szolgáltató rendelkezésére), valamint minden más, a kommunikációs berendezés helyére vonatkozó, akár ingyenes, akár visszterhes szolgáltatási szerződés vagy megállapodás alapján a szolgáltató rendelkezésére álló információt is.[6]

A tartalomra vonatkozó adat

A tartalomra vonatkozó adat a kommunikáció információtartalmát jelöli, azaz a kommunikáció értelme, jelentése. Tartalomra vonatkozó adat a kommunikáció üzenete, de minden olyan információ is, amelyet a kommunikáció szállít. Legegyszerűbb megfogalmazásban: a kommunikációhoz kapcsolódó minden adat, amely nem tartozik a forgalomra vonatkozó adatok körébe, tartalomra vonatkozó adatnak minősül.[7]

Az itt vázolt adatkörök eltérő szenzitivitásúak, ezért szükséges, hogy a felderítés és a büntetőeljárás során a magánszférát érintő hatósági beavatkozások lehetőségét is differenciáljuk a szerint, hogy melyik adat megismerésére jogosult a hatóság.

A számítástechnikai adatok összegyűjtésével és megismerésével kapcsolatos jogintézmények

A számítástechnikai adatok megismerhetők titkos információgyűjtés, titkos adatszerzés, megkeresés, valamint kényszerintézkedések alkalmazásával. A titkos információgyűjtés mind a felderítés, mind a büntetőeljárás során alkalmazható,

[5] A CCC 18. cikk 3. §-a szerint (az adott cikk vonatkozásában).
[6] CCC Explanatory Report 177. pont.
[7] Uo. 229. pont.

míg titkos adatszerzés, illetve kényszerintézkedés csak a büntetőeljárás keretében. A megkeresés a büntetőeljárás során (Be. 71. §; 178/A §) alkalmazható, míg a bűnfelderítés szakaszában adatkérésre (Rtv. 68. §) kerülhet sor. Itt jegyzem meg, hogy míg a megkeresést a büntetőeljárás általános szabályai körében szabályozzák, addig az adatkérést a titkos információgyűjtés keretében. Míg az előbbinél a nyomozó hatóságok mindenféle korlátozás nélkül, addig az utóbbinál szigorú megkötésekkel alkalmazhatják az adott jogintézményt. A kényszerintézkedések körében a számítástechnikai adatok megőrzésére kötelezésnek, a házkutatásnak és a lefoglalásnak van jelentősége.

A nyomozás elrendelése előtt igénybe vehető egyrészt a nemzetbiztonsági célból végzett titkos információgyűjtés (1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról, a továbbiakban: Nbsztv.), másrészt pedig a (kijelölt) bírói engedélyhez kötött titkos információgyűjtés (1994. évi XXXIV. törvény a rendőrségről, a továbbiakban: Rtv., a nyomozás elrendeléséig ad erre lehetőséget) és bírói engedélyhez nem kötött titkos információgyűjtés (Rtv.). A nyomozási szakban a nyomozás elrendelésétől az iratismertetésig a (nyomozási) bírói engedélyhez kötött titkos adatszerzés (Be.) és a bírói engedélyhez nem kötött titkos információgyűjtés (Rtv.), az iratismertetés után pedig bírói engedélyhez nem kötött titkos információgyűjtés folyhat (Rtv.).

A CCC a II. fejezetében, *büntetőeljárási jog* címszó alatt szabályozza azokat a jogintézményeket, amelyek segítséget nyújthatnak a nyomozó hatóságok számára az informatikai bűnözés elleni harcban. Ennek keretében szabályozza a tárolt számítástechnikai adatok gyors megőrzésének és a forgalomra vonatkozó adatok gyors megőrzésének és részbeni átadásának (II. cím), a közlésre kötelezésnek (III. cím), a tárolt számítástechnikai adatok lefoglalásának és átvizsgálásának (IV. cím), valamint a forgalomra vonatkozó adatok valós idejű összegyűjtése és a tartalomra vonatkozó adatok kifürkészése (V. cím) szabályait.[8]

A CCC 14. cikke szabályozza a számítástechnikai bűncselekményekkel kapcsolatos azon eljárási szabályokat, amelyek minden a CCC-ben szabályozott jogintézmény vonatkozásában alkalmazandók. Ezeket az eljárási cselekményeket három esetkörben lehet alkalmazni:[9] egyrészt a CCC-ben meghatározott bűncselekményekkel kapcsolatban, másrészt a számítástechnikai rendszer útján elkövetett más bűncselekményekkel kapcsolatban, harmadrészt pedig bármilyen bűncselekménnyel összefüggő elektronikus bizonyítékok összegyűjtésével kapcsolatban.

[8] A CCC szabályai a büntetőeljárásra vonatkozó 1998. évi XIX. törvény módosításáról szóló 2002. évi I. törvény nyomán kerültek a Be.-be.
[9] A CCC 14. cikkének második pontja.

További fontos, minden eljárási jogintézmény esetén figyelembe veendő szabály, hogy a jogintézmények alkalmazásakor érvényesülnie kell az arányosság elvének. Az arányosság elvének lényege – különösen az Európa Tanácsnak az emberi jogok és alapvető szabadságok védelméről szóló egyezményére (1950) figyelemmel –, hogy a jogalkotás és a jogalkalmazás során végzett eljárási beavatkozásoknak is arányosnak kell lenniük a támadás természetével és körülményeivel.

Az adatok megismerése érdekében alkalmazható jogintézmények

A megkeresés (Be. 71. §)[10]

A bíróság, az ügyész és a nyomozó hatóság tájékoztatás adása, *adatok közlése, átadása,* illetve iratok rendelkezésre bocsátása céljából megkereshet állami és helyi önkormányzati szervet, hatóságot, köztestületet, gazdálkodó szervezetet, alapítványt, közalapítványt és társadalmi szervezetet.[11] Az adatszolgáltatási kötelezettséggel érintett szolgáltatóktól a nyomozó hatóság elsősorban a szolgáltatók szerverein található tárhelyek adattartalmát, a tárhelyekhez kapcsolódó regisztrációs adatokat, illetőleg a forgalomra vonatkozó adatokat kérheti. Az előbbiek bizonyítékul szolgálhatnak a terjesztési, illetőleg közzétételi deliktumokkal kapcsolatos jogellenes tartalmakra, míg a forgalomra vonatkozó adatok az elkövetési hely beazonosításához nyújtanak segítséget.

A CCC. 18. cikkében foglalt intézkedés lényege, hogy azok a bűncselekménynyel érintett harmadik személyek, akiknek releváns információjuk van egy informatikai bűncselekményről, a hatóságok számára információt szolgáltassanak. Az intézményt a CCC szerint két körben lehet alkalmazni. Egyrészt az illetékes hatóságok kötelezhetik a területükön tartózkodó személyt a birtokában vagy az ellenőrzése alatt lévő és számítástechnikai rendszerben vagy számítástechnikaiadattároló egységen tárolt, meghatározott számítástechnikai adatok közlésére. Másrészt pedig kérhetik a szolgáltatótól a birtokában vagy az ellenőrzése alatt lévő számítástechnikai adatok közlését. Ebből következik, hogy az intézmény a már meglévő – tárolt – előfizetőre vonatkozó és a szolgáltatást érintő adatokra, valamint tartalomra vonatkozó adatokra is alkalmazható. A tartalomra vonatkozó adat birtoklása vagy az afeletti ellenőrzés vonatkozásában a tényleges birtoklást, illetve ellenőrzést kell érteni. Az egyezmény értelmében nem tartozik ebbe a körbe például, ha a szolgáltató technikai képességeinél fogva hozzáférhet ugyan az adathoz, de nincs felhatalmazása arra, hogy az adat felett rendelkezhessen is.[12]

[10] Közlésre kötelezés: *production order* (CCC 18. cikk).
[11] Be. 71. § (1) bek.
[12] CCC Explanatory Report 173. pont.

Házkutatás és lefoglalás[13]

A Be. szerint *„A házkutatás a ház, lakás, egyéb helyiség vagy azokhoz tartozó bekerített hely, továbbá az ott elhelyezett jármű átkutatása, illetőleg számítástechnikai rendszer vagy ilyen rendszer útján rögzített adatokat tartalmazó adathordozó átvizsgálása az eljárás eredményessége érdekében"* (Be. 149. §). Abban az esetben, ha a számítástechnikai adat az intézkedéssel közvetlenül nem érintett másik számítástechnikai rendszerben található, amely legálisan elérhető a vizsgált számítógépen keresztül, akkor e másik számítástechnikai rendszer tekintetében is elvégezhető a kutatás.[14] Erre vonatkozóan is alkalmazni kell azonban azt a kitételt, hogy a jogintézményeket csak az adott állam büntető joghatóságához kapcsolódó területen lehet alkalmazni. A CCC értelmében a kommunikáció az adott állam területén zajlik, ha valamelyik kommunikáló fél (személy vagy számítástechnikai rendszer) az adott területen található, vagy ha a számítástechnikai rendszer, illetve telekommunikációs eszköz, amelyen keresztül a kommunikáció zajlik, az adott ország területén található.[15] A CCC 19. cikkét a tárolt adatok vonatkozásában lehet alkalmazni. Ebből a szempontból kérdéses lehet, hogy a még meg nem nyitott e-mail üzenet, amely a közvetítő szolgáltatónál található virtuális postaládában található, amíg az üzenet címzettje azt nem nyitja meg, tárolt adatnak tekintendő-e, vagy olyan adatnak, amely még továbbítás alatt áll. Abban az esetben ugyanis, ha a kommunikáció részeként kezeljük ezt az adatot, akkor nem tárolt tartalomra vonatkozó adatként ismerheti csak meg a hatóság, miközben ha tárolt adatként, akkor házkutatás és lefoglalás keretében is.[16]

„A lefoglalás a bizonyítás érdekében vagy az elkobzás, illetőleg a vagyonelkobzás biztosítására a dolog birtokának elvonása a birtokos rendelkezése alól. A bíróság, az ügyész, illetőleg a nyomozó hatóság elrendeli annak a dolognak, illetőleg számítástechnikai rendszernek vagy ilyen rendszer útján rögzített adatokat tartalmazó adathordozónak a lefoglalását, amely a) bizonyítási eszköz, b) a törvény értelmében elkobozható, vagy amelyre vagyonelkobzás rendelhető el" (Be. 151. §).

Bizonyítási eszköz lehet például az a merevlemez, amely tartalmazza a forgalomra vonatkozó adatokat. Az elkobzás alá eső dolgok vonatkozásában a Btk. 77. § (1) bekezdésének *a)* pontja jöhet szóba, különös tekintettel az informatikai bűncselekmények rendszertani osztályozására, amelynél külön kategória a számítástechnikai rendszer mint az elkövetés eszköze. Így például a jogosulatlan belépésnél

[13] Tárolt számítástechnikai adatok lefoglalása és átvizsgálása: *Search and seizure of stored computer data* (CCC 19. cikk).
[14] CCC. 19. cikk 2. bek.
[15] CCC Explanatory Report 222. pont.
[16] CCC Explanatory Report 190. pont.

az a számítástechnikai rendszer, ahonnan a belépés megvalósul, az elkövetés eszköze, míg az a számítástechnikai rendszer, amelybe a belépés történik, az a dolog, amelyre a bűncselekményt elkövették.

Az elektronikus úton rögzített adatot a hatóság adathordozóra történő rögzítés (átmásolás) útján foglalja le, vagy a helyszínen lefoglalt adathordozóról az adatokat szakértő bevonásával menti le.[17] A CCC szerint a lefoglalás keretében lehetőség van meghatározott számítástechnikai adatok lefoglalására, vagy pedig a teljes adathordozó lefoglalására is (ez célszerű például akkor, ha valószínű, hogy a keresett adatokat felülírták).

Érdekes intézményt tartalmaz a CCC 19. cikke 3. bekezdésének d) pontja, amely a lefoglaláshoz kapcsolódó műveletek között említi az átvizsgált számítástechnikai rendszer fenti számítástechnikai adatainak hozzáférhetetlenné tételét vagy eltávolítását. A számítástechnikai adatok lefoglalásának tehát két fő funkciója van, egyrészt bizonyíték szerzését szolgálja, amelyet az adatok másolásával biztosítani lehet, egyszersmind lehetővé teszi az adatok hozzáférhetetlenné tételét vagy eltávolítását.

Számítástechnikai rendszerben tárolt adatok megőrzésére kötelezés (Be. 158. §)[18]

Az adatok megőrzésére kötelezés jelentőségét az adja, hogy a tárolt adatok értékelhetősége, azok könnyű változtathatósága és manipulálhatósága miatt, gyorsan változik. Az adatok kezelői számára nem evidens az adatok büntetőeljárási célra való hatékony megőrzése, ezért akár a belső adatmentési gyakorlat, a rutinszerű törlési eljárások miatt is könnyen elveszhetnek a fontos információk. Emiatt a megőrzésre kötelezés elősegíti, hogy a fontos bizonyítékok ne vesszenek el.

A számítástechnikai rendszerben tárolt adatok megőrzésére kötelezés olyan ideiglenes biztosító jellegű kényszerintézkedés, amely az adatok birtokosának, kezelőjének az adatok feletti rendelkezési jogát ideiglenesen korlátozza. A lefoglalástól eltérően az adat kezelőjét azonban nem fosztja meg a birtoklás jogától.

A kényszerintézkedést azon adatok vonatkozásában lehet alkalmazni, amely számítástechnikai adatok tárolása már megtörtént. Nem tartozik az eszköz hatókörébe, hogy ez alapján a jövőben valaki összegyűjtsön forgalomra vonatkozó adatokat, illetve az sem, hogy valós időben kifürkéssze valamely kommunikáció

[17] 11/2003. (V. 8.) IM–BM–PM együttes rendelet 67. §.

[18] Számítástechnikai adatok megőrzésére kötelezés: a tárolt számítástechnikai adatok gyors megőrzése: *expedited preservation of stored computer data* – és a forgalomra vonatkozó adatok gyors megőrzése és részbeni átadása: *expedited preservation and partial disclosure of traffic data* (CCC 16–17. cikk).

tartalmát. A CCC kommentárjának[19] 151. pontja röviden vázolja, hogy mi a különbség az adatmegóvás, -megőrzés *(data preservation),* illetőleg az adatmegőrzés-adatmegtartás *(data retention)* jellemzői között. Informatikai környezetben a számítástechnikai adatok megóvása-megőrzése *(to preserve data)* azt jelenti, hogy megtartjuk a szóban forgó adatot, amelyet már korábban rögzítettek, megvédjük a külső behatásoktól (megváltoztatás, minőségromlás; *change or deteriorate)* mind minőségében, mind állapotában. Ehhez képest az adatmegőrzés-adatmegtartás *(to retain data)* az adat megtartását jelenti, és egy adott időszakban keletkező adatok rögzítését jelenti azok megsemmisülése előtt, annak érdekében, hogy a jövőben valaki azokat felhasználhassa. Az adatmegtartás az adatok elmentését jelenti, míg az adatmegóvás azt a tevékenységet jelöli, amely a tárolt adatot biztonságban tartja. Az alcímben szereplő két jogintézményt az adatmegóvás körében kell értelmezni, vagyis az az adatok megtartására vonatkozik. A hazai jogirodalomban használatos elnevezés miatt az adatok megőrzésére kötelezést tehát ebben a kontextusban kell értelmezni.

A megőrzésre kötelezés intézménye alkalmazásának nagy előnye, hogy a megőrzési intézkedés lényegesen kisebb hatással van az adott számítástechnikai szolgáltató tevékenységére, mint a házkutatás, a lefoglalás.

A CCC eltérő szabályokat határoz meg a tartalomra vonatkozó és a forgalomra vonatkozó adatok megőrzésére kötelezés körében. Ennek oka csupán az, hogy így lehetőség van arra, hogy a két adattípus eltérő szenzitivitása miatt az egyezményt aláíró országok különböző súlyú bűncselekményekhez kapcsolhassák a két különböző jogintézményt.

A tárolt számítástechnikai adatok gyors megőrzése (CCC 16. cikk)

A CCC 16. cikkében foglalt, a tárolt számítástechnikai adatok gyors megőrzése alkalmazására akkor van lehetőség, ha alappal feltehető, hogy a számítástechnikai rendszerben tárolt, meghatározott számítástechnikai adatok, ideértve a forgalomra vonatkozó adatokat, ki vannak téve a módosulás vagy megsemmisülés veszélyének.[20]

A megőrzés mindenfajta számítástechnikai adatra vonatkozhat. Az adatok tartalmazhatnak személyes és különleges személyes adatot egyaránt, figyelembe kell venni azonban, hogy csak akkor van mód az intézkedés megtételére, ha alappal lehet tartani az adatok időközbeni állapotváltozásától. Alappal lehet a megőrzést elrendelni például, ha az adott szolgáltató üzletpolitikája szerint az általa tárolt

[19] Explanatory Report.
[20] CCC Explanatory Report 159. pont.

adatokat rendszeres időközönként törlik, vagy az adattároló egység más adatok mentésére is szolgál, és így fennáll az adatok felülírásának veszélye. Ha az adatkezelő nem megbízható, akkor a lefoglalás és a házkutatás alkalmazása célszerűbb.[21]

A forgalomra vonatkozó adatok gyors megőrzése (megóvása) és részbeni átadása (CCC 17. cikk)

A CCC. 17. cikke átadási kötelezettséget ír elő a forgalomra vonatkozó adatok vonatkozásában annak érdekében, hogy azonosítani lehessen más közvetítő szolgáltató érintettségét a kommunikációtovábbításban.[22] Ennek amiatt lehet jelentősége, mert a kommunikációban gyakran több közvetítő szolgáltató is érintett. Mindegyik közvetítő szolgáltató birtokában lehet olyan forgalomra vonatkozó adatnak, amelyet a kommunikáció továbbításában szerepet játszó rendszer rögzíthetett. Általában a kommunikáció folyamatában érintett minden közvetítő szolgáltató lényegi információt birtokol a kommunikációs lánc során keletkezett forgalomra vonatkozó adatból. Ilyenkor a kommunikáció forrásának és céljának a meghatározásához mindig el kell jutni a soron következő közvetítő szolgáltatóhoz.[23] A CCC két megoldási lehetőséget javasol a kommunikációs lánc feltérképezéséhez. Az egyik, hogy a kommunikációs lánc újabb elemének felderítése után a hatóság ismételten határozatot hoz a soron következő közvetítő szolgáltató vonatkozásában, míg a másik megoldás szerint a megőrzésre kötelezett közvetítő szolgáltató értesíti a megőrzésre kötelezésről a soron következő közvetítő szolgáltatót. Utóbbi módszert nem alkalmazza a magyar joggyakorlat.

Számítástechnikai adatok megszerzése bírói engedélyhez kötött titkos információgyűjtés és adatszerzés, illetve bírói engedélyhez nem kötött titkos információgyűjtés keretében

Adatkérés az Rtv. alapján bírói engedélyhez nem kötött titkos információgyűjtés keretében

Az Rtv. 68. §-a bírói engedélyhez nem kötött titkos információgyűjtés keretében lehetőséget ad az elektronikus hírközlő szolgáltatók által az elektronikus hírközlésről szóló 2003. évi C. törvényben (a továbbiakban: Eht.) foglaltaknak megfelelően megőrzött adatok bekérésére adatkérés keretében.[24] Tekintettel arra, hogy ez a lehetőség már a felderítési szakban a rendőrség rendelkezésére áll, szinte minden bűncselekményhez kapcsolódóan bekérhetők ezek az információk a felderítés

[21] CCC Explanatory Report 161. pont.
[22] CCC Explanatory Report 165. pont.
[23] CCC Explanatory Report 167. pont.
[24] A bekérhető adatok körét a későbbiekben részletesen tárgyalom.

érdekében.[25] Ezek az információk a nyomozás során is bekérhetők a nyomozó hatóság által. Érdekes azonban, hogy a büntetőeljárás megindítása után a nyomozó hatóság a *megkeresés* szabályai szerint jogosult bekérni ugyanezeket az információkat az *ügyész jóváhagyása nélkül* is.

Bírói engedélyhez kötött titkos információgyűjtés

Az Rtv. 69. §-a teremti meg a bírói engedélyhez kötött titkos információgyűjtés jogszabályi feltételeit. Az Rtv. szerinti bűnüldözési célból súlyos bűncselekmények esetén a nyomozás elrendeléséig a nyomozó hatóságnak lehetősége van arra, hogy levelet, egyéb postai küldeményt, valamint a telefonvezetéken vagy azt helyettesítő távközlési rendszerek útján továbbított közlés tartalmát megismerheti, azt technikai eszközzel rögzítheti, illetve az interneten vagy más számítástechnikai úton történő levelezés (e-mail stb.) során keletkezett adatokat és információkat megismerhet és felhasználhat. Az Rtv. szerint súlyos bűncselekmény az a bűntett, amelyet a törvény ötévi vagy ennél súlyosabb szabadságvesztéssel fenyeget.

Nemzetbiztonsági célból végzett titkos információgyűjtés

A nemzetbiztonsági szolgálatok külső engedélyhez kötött, illetve nem kötött titkos információgyűjtést is folytathatnak. A nemzetbiztonsági szolgálatok külső engedélyhez *nem kötött* titkos információgyűjtés során az Nbsztv. 54. § (1) bekezdésének i) és j) pontja alapján lehallgathatnak beszélgetést, és az észlelteket technikai eszközökkel rögzíthetik, valamint hírközlési rendszerekből és egyéb adattároló eszközökből információkat gyűjthetnek. Külső engedélyhez *kötött* titkos információgyűjtés keretében pedig az Nbsztv. 56. § (1) bekezdés c) és d) pontja alapján juthatnak informatikai adatokhoz.

Bírói engedélyhez kötött titkos adatszerzés

Hasonló feltételei vannak a büntetőeljárás megindítása után alkalmazott bírói engedélyhez kötött titkos adatszerzésnek is. Az ügyész és a nyomozó hatóság bírói engedély alapján az elkövető kilétének, tartózkodási helyének megállapítása, elfogása, valamint bizonyítási eszköz felderítése érdekében a nyomozás elrendelésétől a nyomozás iratainak ismertetéséig az érintett tudta nélkül információt gyűjthet.

A titkos adatszerzés számítástechnikai rendszert érintő esete, amikor *a)* levelet, egyéb postai küldeményt, valamint telefonvezetéken vagy más hírközlési rendszer útján továbbított közlés tartalmát ismeri meg a hatóság, amit technikai eszközzel

[25] Parti Katalin: Kerekasztal-beszélgetés az online-terrorizmusról. Ügyészek Lapja, 2010/2., 43–53. o.

rögzíthet is, és amikor *b)* a számítástechnikai rendszer útján továbbított és tárolt adatokat ismerheti meg a hatóság, amit fel is használhat.

A Be. is lehetőséget ad az elektronikus hírközlő hálózaton továbbított adatok, közlések kifürkészése kapcsán a rögzítés nélküli adattovábbításra. Az ügyész vagy a nyomozó hatóság rendelkezhet az elektronikus hírközlő hálózat útján továbbított közleménynek, illetve a számítástechnikai rendszer útján továbbított vagy tárolt adatoknak a megkereső tagállam igazságügyi vagy nyomozó hatóságának eszközére azonos titkossági fokon történő átirányításáról. Az Rtv. 69. §-a részletezi a bírói engedélyhez kötött titkos információgyűjtés szabályait. Felfedezhető némi ellentmondás a két jogszabály között a tekintetben, hogy mi is pontosan a titkos adatszerzés, illetve információgyűjtés tárgya informatikai környezetben.

A számítástechnikai adatok valós idejű összegyűjtése[26]

A számítástechnikai adatok valós idejű összegyűjtése a forgalomra vonatkozó és a tartalomra vonatkozó adatokkal kapcsolatban alkalmazható. A hazai szabályozásban nincs eltérés a kétféle adatgyűjtés alkalmazhatóságának feltételrendszerében. Az intézkedések elsősorban a telekommunikációs szolgáltatást nyújtó szolgáltatókra – a hazai terminológiában a hírközlési szolgáltatókra – vonatkoznak. A kifürkészés (lehallgatás) a telekommunikációs hálózatokon keresztül történik. Mindkét valós idejű adatrögzítéshez kapcsolódóan elmondható, hogy mind a privát, mind a közszolgálati rendszerek körében alkalmazhatók, és mindegyik közvetítő szolgáltatóra vonatkozik, amely számítástechnikai rendszeren keresztül kommunikációs lehetőséget kínál. A számítástechnikai adatok valós idejű összegyűjtésének lényege, hogy az éppen aktuálisan keletkező *(real time)* kommunikáció vonatkozásában ad lehetőséget az információgyűjtésre. A számítástechnikai adat intangibilis formában létezik, aminek köszönhetően az adatfolyamban lévő adatok gyűjtése nem befolyásolja azt, hogy ezek az adatok eljussanak a kommunikáció címzettjéhez.

A forgalmi adatok valós idejű összegyűjtésének jelentőségét az adja, hogy segítségével megkerülhetők az informatikai bűncselekmények nyomozásának ama problémái, amelyek a forgalomra vonatkozó adatok elérhetőségének hiányából vagy az identitáselrejtésből adódnak. Tradicionálisan a forgalomra vonatkozó adatok összegyűjtése – figyelemmel a telekommunikáció (telefonbeszélgetés) jellemzőire – a megfelelő eszköz arra, hogy meghatározzuk a kommunikáció forrásának vagy céljának helyét (például telefonszámok) és a kapcsolódó adatokat (idő,

[26] Forgalomra vonatkozó adatok összegyűjtése és a tartalomra vonatkozó adatok kifürkészése: *real-time collection of computer data* (CCC 20–21. cikk).

dátum, kommunikáció ideje), egyúttal pedig bizonyítékul szolgálnak a már elkövetett bűncselekményekhez, valamint segítenek további bűncselekmények elkövetésének megelőzésében.[27]

A CCC nem követeli meg, sőt nem is nyújt lehetőséget a hatóságok számára az általános és válogatás nélküli megfigyelésre, adatgyűjtésre *(fishing expeditions).* A bíróságnak minden esetben meg kell határoznia az adatgyűjtés vonatkozásában azt a kommunikációt, amelyhez kapcsolódóan a forgalmi adatok jelentőséggel bírnak.[28] A Be. 202. § (2) bekezdése szerint azonban a titkos adatszerzésnek nem akadálya, ha az kívülálló személyt érint. Például egy háztartásban, ahol többen használják ugyanazt a telekommunikációs eszközt, szükség lehet arra, hogy több kommunikáció kapcsán is megtörténjen a forgalomra vonatkozó adatok összegyűjtése, amelyek aztán később összefüggésbe hozhatók az egyes személyekkel a szerint, hogy kinek volt lehetősége az adott időben a vizsgált kommunikációban részt venni.

A titkos információszerzés végrehajtása a hazai jog alapján

A titkos információgyűjtést és adatszerzést – ez utóbbinál a Be. 204. § (1) bekezdésében foglalt utaló rendelkezés alapján – az Nbsztv. 8. § (1) bekezdés a) pontjában foglaltak szerint a Nemzetbiztonsági Szakszolgálat (a továbbiakban: szakszolgálat) hajtja végre. A szakszolgálat feladata ellátásához az Eht. 92. § (1) bekezdése alapján a hírközlési szolgáltatók kötelesek együttműködni a titkos információgyűjtésre, illetve titkos adatszerzésre felhatalmazott szervekkel.[29] Az Eht. hatálya alá nem tartozó elektronikus szolgáltatásokra vonatkozó szabályokat az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény (a továbbiakban: Ekertv.) tartalmazza.

Az Ekertv. adatkezelési szabályai (13/A §) szerint a szolgáltató az információs társadalommal összefüggő szolgáltatás nyújtására irányuló szerződés létrehozása, tartalmának meghatározása, módosítása, teljesítésének figyelemmel kísérése, az abból származó díjak számlázása, valamint az azzal kapcsolatos követelések érvényesítése céljából kezelheti az igénybe vevő azonosításához szükséges és elégséges azonosító adatokat. Az Ekertv. ezen túlmenően nem ír elő adatkezelési kötelezettséget, illetőleg jogosultságot. Ebből tehát az is következik, hogy a hírközlési szolgáltatók esetében előírt kötelező adatmegtartás nem vonatkozik azokra az információs

[27] CCC Explanatory Report 217. pont.
[28] CCC Explanatory Report 219. pont.
[29] Lásd még: Be. 204. § (2) bekezdés.

társadalommal összefüggő szolgáltatást nyújtó szolgáltatókra, amelyek nem nyújtanak hírközlési szolgáltatást.

A hírközlési szolgáltatók és a szakszolgálat közötti együttműködés módját az elektronikus hírközlési feladatokat ellátó szervezetek és a titkos információgyűjtésre, illetve titkos adatszerzésre felhatalmazott szervezetek együttműködésének rendjéről szóló 180/2004. (V. 26.) kormányrendelet (a továbbiakban: adatszolgáltatási rendelet) szabályozza.

Külső engedélyhez nem kötött titkos információgyűjtés

Az adatszolgáltatási rendelet 5. § (1) bekezdése szerint a külső engedélyhez nem kötött titkos információgyűjtés során a titkos információgyűjtésre[30] felhatalmazott szervezetek a szakszolgálaton keresztül vagy közvetlenül az elektronikus hírközlési szolgáltatótól kérelmezik az Eht. 156. §-ának (9) bekezdésében, 157. §-ának (10) bekezdésében, illetve 159/A §-ának (1)–(2) bekezdésében meghatározott adatok szolgáltatását. E szakaszok alapján a helymeghatározási adatokról, a forgalmi és számlázási adatokról, valamint az adatmegőrzési kötelezettséggel érintett adatokról lehet információkat szerezni.

Az Eht. 156. §-ának (9) bekezdése szerint az elektronikus hírközlési szolgáltató az adatkérésre jogosultak részére köteles megállapítani és részükre továbbítani a felhasználóval, illetve az előfizetővel kapcsolatos, a forgalmi adatokon kívüli *helymeghatározási adatokat*. Helymeghatározási adat az Eht. 188. § 49. pontja alapján az elektronikus hírközlő hálózatban feldolgozott bármely adat, amely egy elektronikus hírközlési szolgáltatás felhasználója végberendezésének földrajzi helyzetét jelzi.

Az Eht. 157. §-ának (10) bekezdése szerint az elektronikus hírközlési szolgáltató az adatkérésre külön törvény szerint jogosultak részére köteles átadni vagy hozzáférhetővé tenni az Eht. 157. § (2) bekezdés alapján az elektronikus hírközlési szolgáltatónál rendelkezésre álló adatokat. Az Eht. 157. § (2) bekezdése szerint az elektronikus hírközlési szolgáltató az előfizetők és a felhasználók részére történő számlázás és a kapcsolódó díjak beszedése, valamint az előfizetői szerződések figyelemmel kísérése céljából kezelheti a *forgalmi és számlázási adatokat, amelynek részei az előfizetői adatok is*. Az Eht. 159/A §-a foglalkozik a bűnüldözési, nemzetbiztonsági és honvédelmi célú *adatmegőrzési kötelezettség* kérdésével. Az adatok megőrzésére az elektronikus hírközlési szolgáltató és az elektronikus hírközlő hálózat üzemeltetője köteles, a szolgáltató mérlegelési lehetősége kizárt.[31]

[30] Az Eht. értelmező rendelkezésének 105. pontja.

[31] Az adatmegőrzési kötelezettséget az adatmegőrzési irányelvből fakadó kötelező jogalkotási feladat nyomán, a magyar és az uniós szabályozás harmonizációjának megteremtése

Az Eht. 159/A § (1) bekezdése szerint az elektronikus hírközlő hálózat üzemeltetője, illetve az elektronikus hírközlési szolgáltatás szolgáltatója – az adatkérésre külön törvény szerint jogosultak részére nyújtandó adatszolgáltatás érdekében – megőrzi az elektronikus hírközlési szolgáltatás előfizető, illetve felhasználó általi igénybevételével kapcsolatos, az érintett elektronikus hírközlési szolgáltatás nyújtásával összefüggésben a szolgáltató által előállított vagy kezelt adatokat.[32]

Az Eht. a hatályos szabályozás szerint is megőrzendő adatok vonatkozásában a korábbi három év helyett egyéves, a sikertelen hívások során keletkező adatok megőrzésére vonatkozó új kötelezettség esetében pedig az adatmegőrzési irányelv szerinti minimális megőrzési idő alkalmazását rendeli el.[33]

Összegzés

Az elektronikus bizonyítékok vonatkozásában a számítástechnikai adatoknak van kiemelt jelentőségük. A CCC-ben és a hazai jogalkalmazásban azonban ugyanazon adatkörök vonatkozásában eltérő terminus technicusok alkalmazására került sor, ezért fontos feladat volt a releváns adatkörök elkülönítése. Az adatkörök tipizálásánál három adattípust különböztettem meg a számítástechnikai adatok körében, azok statikus állapotában: forgalomra vonatkozó adatokat *(traffic data),* az előfizetőre vonatkozó adatokat *(subscriber data)* és a tartalomra vonatkozó adatokat *(content data).* Emellett az adatok csoportosíthatók dinamikájuk szerint is, e szerint léteznek tárolt adatok és kommunikációs folyamatban részt vevő adatok. Míg az előbbi esetében már valamely lezajlott kommunikációhoz kapcsolódó adatkört kell érteni, az utóbbinál a folyamatban lévő kommunikációhoz kapcsolódó adatkört.

A dolgozat elkészítésénél fontos cél volt, hogy összefoglaljam azokat a hazai jogban jelen lévő jogintézményeket, amelyek lehetőséget nyújtanak az informatikai környezetben megvalósuló bűncselekmények nyomozása során az elektronikus bizonyítékok megszerzésére, megismerésére. A hazai jogban található jogintézmények (titkos információszerzés, megkeresés, számítástechnikai adatok megőrzésére

érdekében alkották. (Adatmegőrzési irányelv: Az Európai Parlament és a Tanács 2006. március 15-i 2006/24/EK irányelve a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról. HL. L105/54, 2006. 4. 13.

[32] Az adatkezelés kiterjed a sikertelen hívásokra vonatkozó adatokra is.

[33] Az irányelv legalább hat hónap és legfeljebb két év időkorláttal állapítja meg az adatmegőrzés idejét, a tagállamok ezen belül úgy is dönthetnek, hogy a megőrzési idő szolgáltatásonként, illetőleg adatfajtánként akár különböző.

kötelezés stb.) bemutatása során minden esetben megvizsgáltam, hogy azok a CCC-ben található mely instrumentumnak felelnek meg. A vizsgálatot kiegészítettem az Európa Tanács által a CCC-hez készített kommentárban található jogértelmezéssel is.

Felhasznált irodalom és dokumentumgyűjtemény

Bócz E. (szerk.): *Kriminalisztika I–II.* BM Duna Palota és Kiadó, Budapest, 2004

Parti K.: *Kerekasztal-beszélgetés az online-terrorizmusról.* Ügyészek Lapja, 2010/2.

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

2006. évi XIV. törvény a rendőrségről szóló 1994. évi XXXIV. törvény módosításáról

2003. évi C. törvény az elektronikus hírközlésről

2002. évi I. törvény a büntetőeljárásról szóló 1998. évi XIX. törvény módosításáról

2001. évi CVIII. törvény az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről

1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról

1994. évi XXXIV. törvény a rendőrségről

11/2003. (V. 8.) IM–BM–PM együttes rendelet a lefoglalás és a büntetőeljárás során lefoglalt dolgok kezelésének, nyilvántartásának, előzetes értékesítésének és megsemmisítésének szabályairól, valamint az elkobzás végrehajtásáról

17/2003. (VII. 1.) PM–IM együttes rendelet a pénzügyminiszter irányítása alá tartozó nyomozó hatóságok nyomozásának részletes szabályairól és a nyomozási cselekmények jegyzőkönyv helyett más módon való rögzítésének szabályairól

23/2003. (VI. 24.) BM–IM együttes rendelet a belügyminiszter irányítása alá tartozó nyomozó hatóságok nyomozásának részletes szabályairól és a nyomozási cselekmények jegyzőkönyv helyett más módon való rögzítésének szabályairól

Explanatory Report on the Convention on Cybercrime (ETS no. 185). Adopted on 8 November 2001

Explanatory Report on the Convention 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union, Official Journal C 379, 29.12.2000.