

INTERNETEN, SZÁMÍTÓGÉPEN TÖRTENŐ NYOMRÖGZÍTÉS

Napjainkban több támadás is érte a rendőrséget, hogy törvénytelenül, vagy túlzottan súlyos eszközöket használ fel, amikor az Interneten előforduló bűncselekmények nyomozása során számítástechnikai eszközökről szerez be bizonyítékokat. Az Infomediator szerint több tucat olyan eset volt, amikor nem lett volna szükséges a számítástechnikai eszközök, szerverek lefoglalása, hanem elég lett volna csak azokon másolással az adatokat rögzíteni. Így – mivel a rendőrség a lefoglalást alkalmazta – az Infomediator álláspontja szerint sérült nagyon sok, ugyanazon a szerveren tárolt magánszemélynek, illetve cégnek az érdeke, mivel az ő honlapjaik is elérhetetlenné váltak, valamint sérült több százezer ember, az egész internetes közösség tájékoztatáshoz fűződő alapvető, alkotmányban rögzített joga.

IRÁSOMBAN IGYEKSEM FELVÁZOLNI, hogy a rendőrhatalóság, illetve más nyomozó hatóság mely esetekben és milyen módon rögzíti a számítástechnikai eszközökön lévő adatokat, mikor élhet vagy kell élnie a lefoglalással, és azt hogyan kell végrehajtania.

DIGITÁLIS BIZONYÍTÉKOK

Először is nézzük meg, hogy mely esetekben lehet szüksége a nyomozó hatóságnak arra, hogy digitális bizonyítékokat rögzítsen. Olyan bűncselekmények elkövetésének vizsgálatakor válik szükségessé számítástechnikai eszközről adatokat beszerezni, mely bűncselekményeknél valamilyen formában számítástechnikai eszközön tároltak, feldolgozott információkat a bűncselekménnyel kapcsolatban.

DIGITÁLIS DOKUMENTUMOK

Ezek lehetnek egyszerű dokumentumok, könyvelési adatok, képek, videó filmek, programok, illetve bármilyen olyan adat, mely számítástechnikai eszközzel rögzíthető. Nagyon gyakori, hogy a szellemi alkotások sérelmére elkövetett bűncselekményeknél az adathordozókon tárolt programok, gazdasági bűncselekményeknél a számítógé-

pes könyvelés adatai, tiltott pornográf felvétellel való visszaélésnél képek, videó anyagok, okmányhamisításoknál az eredeti okmányok digitalizált változatai, de más bűncselekményeknél is a kapcsolattartásra utaló levelezés, vagy egyéb adat található a számítógépes adattárolókon. Ezek az adatok legtöbbször minden számítógépet használó személy számára hozzáférhetők, előhívhatók, megismerhetők, nem kell hozzá különleges szakismeret. Még akkor sem, ha ezeket az adatokat valamilyen formában titkosították, jelszóval védték, de ezeket a jelszavakat ismerjük, vagy megtudjuk, a megtekintésük nem kíván különleges szakértelmet. Ilyenkor a számítástechnikai adathordozó ugyanolyan, mint a videó kazetta, vagy egy kockás füzet, egy papírlap. Ezekben az esetekben a számítástechnikai adathordozó tárolja azt az információt, amelyre a nyomozó hatóságnak a bűncselekmény bizonyításához szüksége van.

DIGITÁLIS NYOMOK

A következő esetkör, amikor a nyomozó hatóság valamilyen számítástechnikai adathordozóról, vagy számítástechnikai eszközről adatokat kíván beszerezni, nyomokat

rögzíteni. Ezekben az esetekben egyértelműen nem határozhatók meg a számítástechnikai eszközön lévő adatok, azok nem mindenki számára hozzáférhetőek, és az adatok, „digitális nyomok” előkeresése valamilyen szakértelmet igényel. Melyek lehetnek ezek az úgynevezett „digitális nyomok”, mit takarhat ez a fogalom? Ilyen esetekben a számítástechnikai eszközökön olyan – általában csak időlegesen – rögzült adatokat keresünk, amelyek a számítástechnikai eszköz működése közben keletkeztek, egy átlagos felhasználó nem szerez róluk tudomást, de a rendszer működéséhez ezek az adatok elengedhetetlenül szükségesek. Melyek lehetnek ezek az adatok? Nagyon sok program működése közben ideiglenes állományokat hoz létre a számítógép háttértárára, melyet a befejezést követően töröl. Azonban mint minden törölt állomány, ameddig nem írják felül újabb adatokkal, az a memóriaterület visszaállítható, elolvasható. Így ezekből a visszaállított ideiglenes állományokból, vagy a korábban törölt állományokból, vagy a számítógépen tárolt különböző adatállományok verzióiból nagyon sok információ kinyerhető egy kis szakismerettel, szaktudással, mely a bűncselekmény bizonyítását lehetővé teszi vagy könnyíti.

Ilyen digitális nyomokkal nem csak a számítógépek háttértárolóin találkozhatunk, hanem különböző perifériákon is. Ismert olyan eset, amikor úgy sikerült megállapítani, hogy egy nyomtatóval készített hamisítvány hány példányban készült, hogy a nyomtató festékpátrónjának elhasználtságát mérték meg, majd ebből következtettek a kinyomatott példányok számára, ismerve az egy nyomtatáshoz szükséges festékmennyiséget. Épp napjainkban jelentette be egy amerikai kutatócsoport, hogy jó eredményeket értek el azon kutatásaikkal, hogy egy kinyomatott papírlapról meghatározzák, milyen típusú nyomtatóval készült a nyomtatás. Ugyanígy adott esetben egy szkenner egyedisége is segítheti a bizonyítást.

A digitális nyomokat általában csak szakértelemmel rendelkező személyek képesek felkutatni és értelmezni. Nagyon sokszor nem csak különleges szakértelem, de

különleges eszközök is szükségesek ahhoz, hogy ezeket az információkat előhívjuk.

NAPLÓ ÉS REGISZTRÁCIÓS ADATOK

A harmadik csoportba tartoznak azok az információk, melyek általában nem egyedi számítógépekkel kapcsolatosak, hanem egész számítástechnikai rendszerek működése és kommunikációja során keletkeznek. Ezek egy része az úgynevezett napló adatok (logok), melyek vagy törvényi kötelezettség vagy gazdasági ésszerűség, vagy rendszerbiztonsággal kapcsolatos követelmények alapján jönnek létre. Ide tartoznak a különböző szerverek fel- és letöltését naplózó adatállományok, a levelező szerverek postafiókokhoz kapcsolódó ki- és bejövő leveleket, valamint a postafiók elérését regisztráló adatállományok, de az egyes hálózatzbiztonsági programok, tűzfalak, behatolás-jelző eszközök naplóadatai is. A regisztrációs adatok azok az adatok, melyek egy-egy szolgáltatónál keletkeznek, amikor valaki igénybe veszi szolgáltatásukat. Ezek lehetnek valós ellenőrzött adatok, pl. hozzáférés-szolgáltatónál (ISP), előfizetői névvel, címmel, telephellyel, de lehetnek nem ellenőrzött adatok, amikor valaki regisztrálja magát egy szolgáltatás igénybevételénél (pl. ingyenes levelező rendszeren), de ez a szolgáltatás ingyenes, az adatok hitelességét nem ellenőrzi senki.

HOL TALÁLHATÓK EZEK A BIZONYÍTÉKOK

Nagyon fontos tudnunk, hogy ezek az állományok hol helyezkednek, honnan tudja a nyomozó hatóság beszerezni őket. A digitális dokumentumok minden esetben egy-egy adathordozón kerülnek rögzítésre. Ez lehet a számítógép háttértára, de ugyanúgy lehet hordozható adattároló (floppy-, CD-, DVD lemez, USB RAM, memória kártya, winchester, vagy egyéb adathordozó). Ezek az eszközök a digitális dokumentumokat szabványos formátumokban tárolják. Akkor is megőrzik a rajtuk lévő adatokat, ha a számítógépből kiveszik őket, illetve ezeket az eszközöket jellemzően éppen adattárolásra használják. Vannak köz-

tük olyanok, melyek újraírhatóak (floppy, winchester, USB RAM, stb.), vagyis nagyon könnyen megváltoztathatók rajtuk az adatok, de vannak olyanok is, melyeken a tárolt adatokat később nem lehet megváltoztatni (egyszer írható CD-, DVD lemez, optikai lemez).

A digitális nyomok is ilyen adathordozókon találhatóak, de jellemzően a winchestereken keletkeznek, melyeken a számítógép üzemszerű működése során jönnek létre ezek az állományok. A felsorolt adathordozók a leggyakrabban vizsgált eszközök, melyeken digitális nyomokat lehet találni. A különböző perifériák (nyomtatók, szkennerek, stb.) ritkábban őriznek digitális nyomokat, de bizonyos esetekben szükség lehet vizsgálatukra.

Szintén a számítógép háttértáron (winchesterén) keletkeznek azok a napló állományok is, melyek a számítógépen futó program beállításai miatt keletkeznek. Ezeknek a napló adatoknak témánk szempontjából két részét kell megkülönböztetni. Az egyik csoportba azok tartoznak, melyek azért keletkeznek, hogy a rendszert üzemeltetők védjék a rendszerüket, vagy annak működéséről adatokat szerezzenek, ezzel is törekedve annak jobb kihasználására, finomra hangolására.

SZOLGÁLTATÓK MEGŐRZÉSI KÖTELEZETTSÉGE

A másik csoportba azok a naplóadatok tartoznak, melyek azért kerülnek naplózásra és megőrzésre, mert törvény, jogszabály kötelezi az internet szolgáltatókat, távközlési szolgáltatókat, hogy bizonyos adatokat folyamatosan naplózzanak és őrizzenek meg. Tekintettel arra, hogy az interneten történő nyomozásoknál ezek a legalapvetőbb adatok, melyekből a nyomozó hatóság a bűncselekmény elkövetőjére fényt tud deríteni, nézzük meg jobban, hogy milyen szolgáltatóknak, mely adatokat és mennyi ideig kell megőrizniük, és azt milyen módon adhatják át a nyomozó hatóságoknak.

Először is azt kell eldönteni, hogy mely jogszabály helyen keressük ezeket a kötelezettségeket. A 2003. évi C. törvény (továbbiakban EHT) az elektronikus hírközlés-

ról a távközlési szolgáltatókra ró kötelezettséget. A 2001. évi CVIII. törvény (továbbiakban E-ker. törvény) az elektronikus kereskedelmi szolgáltatást és az információs társadalommal összefüggő szolgáltatást nyújtókra ró kötelezettségeket.

A 2003. évi C. törvény az elektronikus hírközlési szolgáltatóra ró adatmegőrzési kötelezettséget a szolgáltatás teljesítése vonatkozásában. A 188.§ 13. pontja értelmében az elektronikus hírközlési szolgáltatás: „olyan, más részére általában ellenszolgáltatásért végzett szolgáltatás, amely teljesen vagy nagyrészt jeleknek elektronikus hírközlő hálózatokon történő átviteléből, és ahol ez értelmezhető, irányításából áll, de nem foglalja magában az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások felhasználásával továbbított tartalmat szolgáltató vagy ilyen tartalom felett szerkesztői ellenőrzést gyakorló szolgáltatásokat, valamint nem foglalja magában az információs társadalommal összefüggő, más jogszabályokban meghatározott szolgáltatásokat, amelyek nem elsősorban az elektronikus hírközlő hálózatokon történő jeltovábbításból állnak.”, míg a szolgáltató pedig az „elektronikus hírközlő hálózat üzemeltetője, valamint elektronikus hírközlési szolgáltatást nyújtó természetes, illetőleg jogi személy vagy jogi személyiséggel nem rendelkező gazdasági társaság.” A fenti megfogalmazásból egyértelműen kiűnik, hogy ez a törvény azokra a szolgáltatókra ró kötelezettséget, akiknek az infrastruktúráján az internetes adatforgalom folyik. Ezek a szolgáltatók nyújtják – akár magánszemélyeknek, akár az elektronikus kereskedelmi szolgáltatást nyújtó cégeknek – azt a háttér infrastruktúrát, melyen keresztül csatlakoznak a világhálóra. Ezek a szolgáltatók sokszor nem csak tisztán elektronikus hírközlési szolgáltatást nyújtanak, hanem elektronikus kereskedelmi szolgáltatást is, de amikor adatokat kérünk tőlük, akkor a szolgáltatásnak megfelelő jogszabály hely alapján kell azt megtenni.

A törvény 157.§ (2) bekezdése határozza meg azokat az adatokat, melyeket az elektronikus hírközlési szolgál-

azokra a tényekre terjed ki, amelyek a büntető és a büntetőeljárás jogszabályok alkalmazásában jelentősek.” A gyakorlatban ez azt jelenti, hogy egy olyan logikai sort kell végigjárni, mellyel logikai lépések során bizonyítható, hogy egy adott szerver elérése, a közbenső szerverek és távközlési szolgáltatók igénybevételével, a nyomozó hatóság által gyanúsított személy számítógépéről történt. A felderítés során általában fordítva történik a logikai sor felépítése. Ismert a sértett számítógépe és onnan haladunk vissza az elkövető számítógépéig, majd ha megtaláltuk azt a számítógépet, melyről elkövették a bűncselekményt, akkor megpróbáljuk a gépet és az elkövető személyét összekötni valamilyen adatok alapján.

Ezen bizonyítási tevékenység során felhasználhatóak a Be. 76. § (1) szerinti bizonyítás eszközei: „a tanúvallomás, a szakvélemény, a tárgyi bizonyítási eszköz, az okirat és a terhelt vallomása.” A korábban felsorolt digitális bizonyítékok közül megkereséssel szerezhetünk be okirati bizonyítékokat, a tárgyi bizonyítási eszközök beszerzése lefoglalással történik. Ezek vizsgálatát a szakértő végzi, valamint sokszor segíti a kihallgatásokat.

MEGKERESÉS

A nyomozások során leggyakrabban és legelőször a Be. 71. §-ban meghatározott megkereséssel él a nyomozó hatóság, hogy adatokat szerezzen be. A megkeresés során „a nyomozó hatóság állami és helyi önkormányzati szervet, hatóságot, köztestületet, gazdálkodó szervezetet, alapítványt, közalapítványt és társadalmi szervezetet kereshet meg tájékoztatás adása, adatok közlése, átadása, illetőleg iratok rendelkezésre bocsátása végett”. Az internetes nyomozások során így szerzi be a nyomozó hatóság a távközlési szolgáltatóktól, valamint az E-ker. törvény hatálya alá tartozó szolgáltatóktól és közvevítő szolgáltatóktól azokat az adatokat, melyek alapján a korábban felvázolt logikai lánc elemeit fel tudja építeni.

Ezek során a megkeresések során az E-ker. törvény hatálya alá tartalomszolgáltatóktól az ő szervereiken meg-

található honlapok, tárhelyek tartalmát kéri meg a nyomozó hatóság, valamint az ezekhez az oldalakhoz és tárhelyekhez tartozó regisztrációs adatokat és az oldal elérését dokumentáló napló adatokat.

A tárhely, illetve weboldal tartalmával általában a bűncselekmény elkövetését, az illegális adattartalom megjelenését bizonyítja a nyomozó hatóság. A regisztrációs és napló adatokat viszont már az elkövető felderítése érdekében szerez be. A regisztrációs adatokból ismerhető meg, hogy a feltételezett elkövető milyen adatokat adott meg a regisztráció során, a napló adatokból pedig, – melyek a belépésekre, fel- és sokszor a letöltésekre is tartalmaznak adatokat, – kideríthető, hogy az internet mely számítógépéről léptek be arra az oldalra, töltöttek fel vagy le adatállományokat arról az oldalról. Az oldal tartalma általában megtalálható, mivel a tárhelyszolgáltató sok esetben a megkereséskor értesül csak arról, hogy bűncselekményt követtek el a szerverei felhasználásával, míg más esetekben már korábban elérhetetlenné tette az oldalt, mivel jelezték számára a bűncselekmény elkövetését, de egyben azt is, hogy büntető feljelentés érdekében kérik, hogy ezeket az adatokat őrizze meg az eljárás sikeres lefolytatása érdekében.

A távközlési szolgáltatóktól arra vonatkozóan kérünk be adatokat, hogy egy bizonyos IP cím egy bizonyos időben kinek volt kiosztva. (1) Ez által tudjuk szűkíteni, hogy mely internetre csatlakozott számítógép érte el azt a szervert az adott időben. A távközlési szolgáltató ilyenkor azt tudja megmondani, hogy mely előfizetői névvel, mely behívószámát mely számról hívva (dial up-os, normál telefonos, modemes hozzáférés), vagy telepített és hova telepített széles sávú (ADSL, ISDN, bérelt vonal, kábelnet,) összeköttetésről érték el az internetet.

A megkeresés útján kapott adatokat a büntetőeljárás során okiratként használja fel a nyomozó hatóság, tekintettel arra, hogy azok megfelelnek a Be.-ben az okirattal szemben támasztott követelményeknek, vagyis „valamilyen tény, adat valóságának, esemény megtörténtének

vagy nyilatkozat megtételének bizonyítására készül, és arra alkalmas” és olyan tárgy, vagyis adathordozó „amely valamely tény, adat valóságának, esemény megtörténtének, vagy nyilatkozat megtételének igazolása céljából a 115. § (2) bekezdésében megjelölt módon készült.”

Egyes álláspontok szerint ezeket az adatokat, melyeket a nyomozó hatóság megkeresés útján szerez meg, ha tudja, hogy mely szolgáltatónál található, akkor nem megkereséssel, hanem adatlefoglalással kell élnie, vagy a későbbiekben kell lefoglalnia ezen adatokat, hogy bizonyítási eszközként fel tudja használni. Ezt támasztja alá a 11/2003. (V. 8.) IM-BM-PM együttes rendelet 67.§-nak meghatározása is, mely általános szabályként írja le, hogy „Az elektronikus úton rögzített adatot a hatóság adathordozóra történő rögzítés (átmásolás) útján foglalja le...”. Úgy gondolom azonban, hogy ez a gondolatmenet és megoldás nem helyes a következők miatt. A Be. 151. § (1) bekezdése értelmében „A lefoglalás a bizonyítás érdekében vagy az elkobzás, illetőleg a vagyoneklobzás biztosítására a dolog birtokának elvonása a birtokos rendelkezése alól.” Ez a fogalmi meghatározás teszi egyértelművé, hogy csak dolog lehet a lefoglalás tárgya. A következő bekezdés is csak a „számítástechnikai rendszernek vagy ilyen rendszer útján rögzített adatokat tartalmazó adathordozónak a lefoglalását” nevesíti. Ebből a fogalmi meghatározásból következik, hogy a lefoglalás tárgya csak adathordozó, vagyis dolog lehet. Ebből pedig az következik, hogy az adatokat a nyomozás során megkeresés útján kell beszereznie. A beszerzett adatokat a megkeresett fél a nyomozó hatóságnak, papír alapú adathordozón, vagy számítástechnikai adathordozón (CD lemez, winchester, stb.) adhatja át, és azt okiratként kell kezelni.

Zavart az okozhat, hogy jogszabály szerkesztési problémák miatt a Be. 158/A § (8) bekezdése adat (2) lefoglalásáról beszél, valamint a korábban említett 11/2003. (V. 8.) IM-BM-PM együttes rendelet 67.§-a is

csak másodlagosan említi meg a Számítástechnikai rendszer útján rögzített adatok megőrzésére kötelezés jogintézményét. Úgy gondolom, hogy az előbb említett két jogszabályhely és az a gondolatmenet vezetheti a nyomozó hatóságokat a mindenáron való lefoglalásra való törekedésre, hogy kétséget kizáróan bizonyítékok csak lefoglalással szerezhetők be, valamint, hogy a lefoglalás egyes esetekben gyorsabb megoldást jelent, mint a megkeresés, és az információ kevésbé van kitéve változásoknak. Álláspontom szerint az okirati bizonyítás is megfelelő ezekben az esetekben, valamint garanciális szabályok alapján is jobb, ha megkeresés útján szerzi be a nyomozó hatóság ezeket az adatokat.

Eltérő értelmezéssel találkozhatunk akkor is, ha azt vizsgáljuk, hogy milyen alaki és tartalmi követelményeknek kell megfelelnie a megkeresésnek. Természetes, hogy a megkeresésben fel kell tüntetni az általános iratkezelési szabályokban megfogalmazottakon túl a megkeresés célját, jogalapját, a beszerzendő adatok körét is meg kell határozni. Abban van eltérés a jogértelmezések között, hogy szükséges-e a Be. 178/A. §-a szerint az ügyész jóváhagyása ilyen megkeresések esetén. Az E-ker. törvény hatálya alá eső szolgáltatók megkeresésekor ilyen jóváhagyásra nincs szükség, mivel a törvény csak a hírközlési szolgáltatók megkereséseire vonatkozóan ír elő ilyen kötelezettséget. Az EHT hatálya alá tartozó hírközlési szolgáltatóknál is kétségbevonható véleményem szerint az ügyési jóváhagyás kötelezővé tétele, bár a jelenlegi ügyési gyakorlatban nagyon sokszor találkozunk vele. A probléma az, hogy a törvényi megfogalmazás szerint ügyési jóváhagyás szükséges „a gyanúsítottról (feljelentettről, illetőleg az elkövetéssel gyanúsítható személyről) a tényállás felderítése érdekében adatok szolgáltatását igényelheti az adóhatóságtól, a hírközlési szolgáltatást nyújtó szervezettől”. Úgy gondolom, hogy ez nem okoz problémát, ha feljelentett személyről, vagy már meggyanúsított személlyel kapcsolatban kérünk adatokat a hírközlési szolgáltatótól. Az viszont jelentősen lassítja a

nyomozások menetét, valamint túlzott terheket is ró az ügyészségekre, ha az elkövetéssel gyanúsítható személyre való hivatkozással a rendőrség még a felderítés szakaszában minden hírközlési szolgáltatótól való adatkéréshez ügyészi jóváhagyást kér. Úgy gondolom ez csak akkor szükséges, ha olyan a rendőrhatalóság által már név szerint kébbe került személlyel kapcsolatban kérünk adatokat, akinek a vonatkozásában már elegendő adatunk van a megalapozott gyanúra, de a megkeresés időpontjáig még nem történt meg a gyanúsítottkénti kihallgatása. Amennyiben az eljárások korábbi szakaszában is szükségessé tesszük az ügyészi kontrollt, akkor gyakorlatilag az összes hírközlési szolgáltatótól való adatszerezésre kiterjesztjük, és így az ügyészségek munkaterhének növelésével automatikusan a gyanúsítható személyek, gyanúsítottak vonatkozásában előírt kontrollt csökkentenénk elhanyagolható szintűre. A felderítés korai szakaszában a nyomozó hatóság még konkrét személy ismerete nélkül igyekszik megállapítani, hogy honnan, mely számítógépről követték el a bűncselekményt. Az is vitatható, hogy az ekkor megkért adatok személyes adatoknak minősíthetők-e, mivel ezekből az adatokból csak az internetre csatlakozott számítógépet lehet beazonosítani, nem pedig személyt. A beazonosított számítógép személyhez, mint feltételezett elkövetőhöz kötése a nyomozás későbbi szakaszában történik.

A gyakorlatban még nem, de az elkövetkezendőkben majd valószínűleg problémát fog okozni, hogy a megkeresésre történő adatközlés ingyenes a Be. 71.§-a alapján. Sokszor jelentős adatmennyiségű adatot kell adathordozóra kiírni, a nagyobb szolgáltatókhoz jelentős mennyiségű megkeresés érkezik, így a megkeresések teljesítésének jelentős anyagi költségvonzata van.

A megkeresésben foglaltak teljesítéséhez az is hozzá tartozik, hogy a rejtjelezett, vagy egyéb módon titkosított adatokat értelmezhető formában kell átadni a nyomozó hatóság részére. Ez a gyakorlatban azt jelentené, hogy a napló adatokat úgy kell átadni, hogy az egyes oszlopok

adattartalmát vagy egyértelműen fel kell tüntetni, vagy a kíséző levélben jelezni, és ugyanígy kell tenni a regisztrációs állományokban lévő adatokat tartalmazó állománnyal is.

Az adatszolgáltatást minimum 8, maximum 30 napon belül teljesíteni kell a megkeresett szervnek, vagy közölnie kell, hogy milyen törvényhely zárja ki az adatszolgáltatást. Amennyiben jogosulatlanul tagadja meg az adatszolgáltatást akkor a Be.-ben meghatározott egyéb kényszerintézkedés is elrendelhető az adatok beszerzése céljából, így akár a házkutatás vagy a lefoglalás is, de ebben az esetben is – álláspontom szerint – nem az adatokat, hanem az adathordozót foglalja le a nyomozó hatóság.

LEFOGLALÁS

A lefoglalás törvényi fogalmát már a korábbiakban elemeztem. A nyomozó hatóságok lefoglalással a Be.-ben meghatározott esetekben élhetnek. Ezek a következők: bizonyítási eszköz beszerzése, valamint ha „a törvény értelmében elkobozható, vagy amelyre vagyoneklobzás rendelhető el”.

Bizonyítási eszköz lefoglalásáról akkor beszélhetünk, ha a korábban meghatározott digitális nyomok rögzítése miatt válik szükségessé az adathordozó biztosítása a későbbi nyomozás, bizonyítás szempontjából. Ekkor a nyomoknak az adathordozóját eredetben kell lefoglalni a későbbi szakértői vizsgálatokhoz. Az adathordozón található nyomok azok, melyeket bizonyítási eljárás során felhasználhat a nyomozó hatóság, majd a vádképviseleti szerv a bíróság előtt.

Sok esetben lehetőség van arra is a technika fejlődése miatt, hogy ezeket a nyomokat hiteles formában, nem az eredeti adathordozó lefoglalásával rögzítse a nyomozó hatóság, hanem egyes adathordozókról hiteles másolatot készítsen, és azt vizsgálja a továbbiakban. Ilyenkor a szakértő vagy a nyomozó hatóság tagja egy speciális eszközzel úgymond „lefényképezi” az adathordozót és

ezt a „fényképet”, image másolatot írja ki egy másik adathordozóra, úgy, hogy az eredeti adathordozón semmilyen változást nem hajt végre. Az így rögzített digitális nyomokat tudja vizsgálni a szakértő vagy a bünyügyi elemző. Ezek a programok, speciális eszközök biztosítják azt is, hogy hitelessé tegyék az eljárás egész szakaszában az így biztosított digitális nyomokat, mert egy matematikai műveleten alapuló úgynevezett „hash” kulcsot generálnak az eredeti adathordozóról, mely amennyiben valamilyen változás történik és újra elvégzik ezt a „hash” kulcs generálást más eredményt ad. Ez a „hash” kulcs olyan karaktersorozat, amelyet csak a számítógépes program értelmez, és amit akár kinyomatva is tárolhat a nyomozó hatóság az ügyiratban, illetve megőrizheti a szakértő, valamint az a személy, akitől a digitális nyomokat rögzítették. Amennyiben így rögzít a nyomozó hatóság egy digitális nyomot, akkor nem szükséges az eredeti adathordozó lefoglalása. Tudomásom szerint a rendőrségnél jelenleg van folyamatban ilyen eszközök beszerzése, de egyes szakértők már rendelkeznek ilyen eszközökkel.

A lefoglalás másik lehetősége, ha olyan dolgot kell lefoglalni, mely elkobozható. Az elkobozandó dolgok körét a Btk. 77.§ (1) bekezdése határozza meg a következőképpen: „El kell kobozni azt a dolgot, a) amelyet a bűncselekmény elkövetéséhez eszközül használtak, vagy arra szántak, b) amelynek birtoklása a közbiztonságot veszélyezteteti, vagy jogszabályba ütközik, c) amely bűncselekmény elkövetése útján jött létre, d) amelyre a bűncselekményt elkövették”. Az a./ pontban meghatározott esetek miatt van szükség a nyomozások során lefoglalással élni, tekintettel arra, hogy a tiltott adattartalmak elhelyezése miatt indult büntetőeljárások (3) során az adott adathordozó, melyen ezek a tiltott adattartalmak találhatóak, az elkövetés eszközének minősül (4). A nagyobb tárterülettel rendelkező számítógép szerverek nagyon sok esetben nem csak egy adathordozót tartalmaznak, hanem az úgynevezett RAID technológia fel-

használásával több adathordozót egy számítógépes hardware eszköz segítségével összekapcsolnak, és azokon megosztva tárolják az adatokat. Ebből következően nem elég csak az adathordozót lefoglalni, hanem az egész eszközt biztosítani kell az eljárás során, hogy az adatok visszanyerhetőek legyenek erről az eszközről a szakértő számára, és az elkövetés eszközhöz a RAID vezérlő egység is hozzá tartozik.

Az elkövetés eszköze az a számítógépes konfiguráció, vagy akár számítógépes hálózat is, melyről egy távoli szervert irányítanak, arra adatokat feltöltenek, illetve azt feltörik, a rajta lévő adatállományt módosítják, vagy egy távoli szerver gépre illegálisan lépnek be róla.

Problémát okozhat az is, ha a gép egy „szerver hotelban” úgynevezett szerver hosting-on van. Ez azt jelenti, hogy a szerver tulajdonosa a gépet olyan távközlési szolgáltatónál helyezi el, aki vállalja, hogy biztosítja a szerver működését, de a rajta található adatokhoz nem fér hozzá. A távközlési szolgáltató, csak azt vállalja, hogy biztosítja a szünetmentes áramfelvételt a gépnek, széles sávú internet hozzáférést, klimatizált helyiséget, és egyéb feltételeket. Ilyenkor a szerverhotel üzemeltető szolgáltató nem is rendelkezik a nála elhelyezett géphez hozzáféréssel, nincs befolyása annak tartalmára. Ebben az esetben a nyomozó hatóság a lefoglalást bár a szervert üzemeltető céggel szemben, annak a birtokában lévő gépre hajtja végre, de a szerver tulajdonosa az a személy, aki üzemelteti és oda elhelyezte a számítógépet. Ezekben az esetekben nem lehet azzal érvelni a lefoglalás ellen, hogy a Btk. 77.§ (3) bekezdése alapján azt nem lehet elkobozni, így lefoglalás sem rendelhető el, mivel a lefoglalást szenvedő, akitől valójában elhozzuk a számítógépet, nincs befolyással annak tartalmára, de nem is tulajdonosa, csak megőrzésre és működtetésre volt a szerver termében.

Nagyon sok esetben azzal érvelnek a lefoglalás ellen szót emelő szervezetek, jogvédők, hogy az ilyen szervereken olyan személyek, szervezetek honlapjai,

levelező szolgáltatásai is működnek, melyek érdektelenek a bűncselekményben, ami miatt indult az eljárás, viszont alapvető alkotmányos jogaik sérülnek, valamint jelentős gazdasági káruk keletkezik egy olyan szerver lefoglalása miatt, melynél ők csak bérlők, szolgáltatást igénybe vevők. A lefoglalás miatt ezt a szolgáltatást nem tudják a továbbiakban igénybe venni. (5) Álláspontom szerint ekkor, bár közvetlenül a nyomozó hatósági fellépés okán jön létre a károkozás, de ezért nem a nyomozó hatóság felel, hanem az a szervezet, vagy személy, aki az illegális adattartalmat ezen a szerveren tárolta, ami miatt a nyomozó hatóságnak lefoglalással kellett élnie. Ettől függetlenül minden esetben vizsgálni kell, hogy a szerver tulajdonosa és az üzemeltető, működtető személy mennyire felelősek a bűncselekmény vonatkozásában, ki miről tudott, milyen anyagi érdekeik voltak. Természetesen más a megítélés akkor, ha például egy egyetemi hálózaton található illegális adattartalom, melyet a hálózatot üzemeltető informatikus az egyetem vezetésének tudta nélkül használt fel illegális tevékenységre, és más akkor, ha egy kisebb 2-3 alkalmazottat foglalkoztató családi vállalkozás egyik tagja használja fel a szerver tárterületét illegális adattartalom közlésére, és ezért az anyagi támogatást a családi vállalkozás bankszámlájára utalják át.

ELEKTRONIKUS LEVÉL BIZTOSÍTÁSA

A lefoglalás egy speciális esete, melyet a Be. 151.§ (4) bekezdése határoz meg, vagyis „A címzettnek még nem kézbesített postai és hírközlési küldeménynek, [...]lefoglalását a vádirat benyújtásáig az ügyész [...] rendeli el”. Alapvető kérdésként az merül fel, hogy mikor kell egy hírközlési küldeményt kézbesítettnek tekinteni. Ez a kérdés leginkább az elektronikus levelezés, biztosításának, lefoglalásának esetén merül fel. A postai küldeménynél a 2003. évi C1. törvény, mely a postáról szól a 3. § 28./ pontjában meghatározza, hogy „Postai küldemény kézbesítése: [...]a postai küldemény a postai hálózatról a küldemény címezésében megjelölt (jogszabá-

lyi rendelkezés alapján attól eltérő) helyen kikerül. A küldemény kézbesítése magában foglalja mind a címzett (illetve az egyéb jogosult átvevő) részére történő személyes átadást, mind a címhelyen történő elhelyezést.”. Ebből egyértelműen meghatározható, hogy ha a postaládába bedobták a küldeményt, akkor azt már kézbesítettnek kell tekinteni.

Az elektronikus levelezésre nincs ilyen jogszabályi meghatározás, de még a műszaki specifikációk sem írják elő kötelezően, hogy egy levélnek meg kell érkeznie, és ha igen, akkor mikor kell kézbesítettnek tekinteni. A Be. szerinti megfogalmazásból, rendszertani helyből viszont az tűnik elfogadhatónak, ha akkor tekintem a levelet kézbesítettnek – a postai analógia alapján is –, amikor az az internet hálózatról kikerül, vagy annak utolsó pontjához érkezik, ahol már a postafiók tulajdonosa szabadon hozzáférhet leveleihez. Ezt az elvet pontosítja és követi a 79/2004. (IV.19.) Korm. rendelet 14.§ (1) bekezdése is, mely kimondja, hogy „A postai szolgáltató a nem könyvelt küldeményeket [...]a címhelyen, levélszekrénybe kézbesíti.” Ez a gyakorlatban azt jelenti, hogy amennyiben a levél a postafiókot üzemeltető szolgáltató szerver gépén megjelenik, és ahhoz az internet bármely pontjáról a postafiók tulajdonosa szabadon hozzáfér, akkor azt kézbesítettnek kell tekinteni. Ellenkező esetben ez azt jelentené, hogy csak azokat az elektronikus leveleket foglalhatná le a nyomozó hatóság ügyészi engedély nélkül, melyek már a szolgáltató gépéről le lettek töelve. (6)

Más a helyzet az elektronikus postafiókok forgalmi és regisztrációs adataival. Ezeket az adatokat a korábban vázoltak alapján megkereséssel szerzi meg a nyomozó hatóság.

Alkotmányos problémát vethet fel az a helyzet, (ismereteim szerint erre már volt precedens) amikor egy postafiók tartalmát, akár naponta is lefoglalják. Ez egyenértékű az elektronikus postafiók bírói engedély nélküli lehallgatásával. Úgy gondolom, erre még az sem jelentene megoldást, ha csak az ügyészség foglalhatná le

a postafiók tartalmát, mivel ugyanúgy élhetne a többszöri lefoglalás lehetőségével, elvonva a bíróság jogkörét, és megszüntetve a bírói garanciát.

SZÁMÍTÁSTECHNIKAI RENDSZER ÚTJÁN RÖGZÍTETT ADATOK MEGŐRZÉSÉRE KÖTELEZÉS

A 2002. évi I. törvény hozta be ezt az új jogintézményt a Be.-be. A 158/A.§ (1) bekezdése meghatározza az új jogintézmény fogalmát: „A megőrzésre kötelezés a bűncselekmény felderítése és a bizonyítás érdekében a számítástechnikai rendszer útján rögzített adat birtokosának, feldolgozójának, illetőleg kezelőjének a számítástechnikai rendszer útján rögzített meghatározott adat feletti rendelkezési jogának ideiglenes korlátozása.”. A fogalomból is látszik, hogy ez a jogintézmény ideiglenesen kívánja biztosítani a nyomozó hatóságok részére a számítástechnikai rendszer útján rögzített adatok átvizsgálásának lehetőségét.

Amennyiben az eljárás során ezek közül az adatok közül szükség lenne valamely adatra a bizonyításhoz vagy a felderítéshez, akkor azt lefoglalással kell megszerezni. Ez az ideiglenes intézkedés csak azt biztosítja a nyomozó hatóságnak, hogy ezeket az adatokat vizsgálni tudja. Ebből következik, hogy ezt a jogintézményt akkor alkalmazhatja a nyomozó hatóság, ha nagyobb terjedelmű adathalmazt kell átvizsgálnia, és nem lehet meghatározni, hogy mely adatokra van szükség, így az egész adathalmazra vonatkozóan se megkereséssel, se lefoglalással nem tud élni.

A szabályozásból is kiűnik, hogy alapvetően egy a nyomozás felderítési szakaszában alkalmazhatja sikerrel a hatóság ezen jogintézményt, amikor még nagyszámú adatból kell megkeresnie azt, hogy melyre van szüksége a nyomozás, felderítés során. Ezzel az intézkedéssel biztosítható, hogy akár az ország különböző területein bűncselekmény felderítése során szükséges különböző szervek adatai a nyomozó hatóság rendelkezésére álljanak. Az adatokat összevetve, „összefésülve” és

kigyűjtve a releváns adatokat, csak a szükséges adatokat kelljen lefoglalni a bizonyítás érdekében.

A másik lehetséges alkalmazása, amikor egy olyan számítógépről kívánunk adatokat megőrizni, mely nem érintett a bűncselekményben, de a rajta lévő adatok segíthetik a felderítést. Ebben az esetben a számítógép birtokosától kellene lefoglalni a számítógépet, hogy arról adatokat szerezzünk be. A megőrzésre kötelezés a lefoglalásnál enyhébb, és a véltlen birtokosnak kisebb joghátrányt okozó kényszerintézkedés, mellyel elérjük, hogy a számítástechnikai eszközén, rendszerén lévő adatokat a nyomozó hatóság átvizsgálhassa, majd a releváns adatokat róla lefoglalja.

Ez a megoldás garanciát nyújt abból a szempontból, hogy a nyomozó hatóság nem foglal le, vagy megkereséssel nem biztosít olyan személyes adatokat, melyek a felderítés szempontjából irrelevánsak, tehát adatvédelmi szempontból is üdvözlendő. Másik garanciális szabály, hogy az adatok feletti korlátozás csak 3 hónapig tarthat. Ez lényeges azért is, mert a megőrzésre kötelezettre akár komoly anyagi terheket is róhat, üzemserű működését akadályozhatja, hogy neki kell gondoskodnia az adatok tárolásáról, és hozzáférhetetlené tevéséről mások számára. Az adatok sérthetlenségét hivatott biztosítani az is, hogy az elrendelő szerv az „adatot fokozott biztonságú elektronikus aláírással láthatja el”.

Sajnos a jogszabály, mivel utólag került be a Be.-be nem egészen illeszkedik annak rendszerébe. Nem határozza meg az adat fogalmát, valamint az egész Be.-ben csak itt beszél adatlefoglalásról. Tekintettel arra, hogy egy új, előzmények nélküli jogintézményről van szó, a gyakorlati alkalmazásának lehetőségei és szabályai még nem kristályosodtak ki. Az már most is látszik, hogy az elkövetkezendőkben igen nagy szerepe lehet ennek az intézkedésnek olyan nagyobb hálózatok sérelmére, vagy azok felhasználásával elkövetett bűncselekmények nyomozása során, ahol szükséges az adatok gyors biztosítása az eljárás sikere érdekében, de nem határozható

meg egyértelműen az elrendelés pillanatában, hogy pontosan mely adatokra van szükség, azoknak csak egy széles körét lehet meghatározni. Továbbá ezzel a jogintézménnyel a bűncselekményben vétlen személyektől szerezhet be a nyomozó hatóság releváns információkat úgy, hogy nem kell egy súlyosabb, nagyobb hátrányt okozó jogintézménnyel – a lefoglalással – élnie.

SAKÉRTŐK SZEREPE

Az interneten, számítástechnikai eszközzel elkövetett bűncselekmények nyomozása az egyik leginkább szakértőigényes nyomozások közé tartozik. Sajnos, a gyakorlatban sok esetben akkor is szakértőt rendel ki a nyomozó hatóság, ha arra nincs szükség, illetve olyan kérdéseket tesz fel számára, melyek nem szakkérdések. Ennek az ellenkezőjével is találkoztam már, amikor a számítástechnikához valamilyen szinten értő nyomozók vagy rendszergazdák úgy nyúltak a lefoglalt számítógépekhez, hogy azzal a bizonyítási eszköz hitelességét tették kétségessé. Egyik gyakorlat sem jó. Ha olyan kérdésekre is szakértőt rendel ki a nyomozó hatóság, melyre nem lenne szükség, akkor fölöslegesen drágítja meg a nyomozásokat a tetemes szakértői költségekkel, illetve azok gyorsasága, naprakészsége is sérelmet szenved. Amennyiben viszont nem rendel ki szakértőt olyankor, amikor szakkérdésről van szó, mert bízik saját tudásában, akkor viszont a bizonyítási eszközök hitelessége kérdőjeleződik meg, illetve a szakértőkre esetleg nem a megfelelő választ kapja a nyomozó hatóság.

Az egyik legfontosabb alapelv, hogy csak abban az esetben lehet vizsgálni egy adathordozót, ha az csak egyszer írható, azon semmilyen adatmódosítást a vizsgálattal nem végezhetünk el. A számítástechnikai rendszerek egyikét speciális eszköztől eltekintve módosítható adathordozókat alkalmaznak, még ha csak olvassuk is őket, akkor is rendszerszinten módosítják a rajtuk lévő adatállományt. Ebből következik, hogy még a szakértőnek sem szabad az eredeti adathordozót vizsgálnia,

azon adatokat keresni, ha módosítható adathordozóról van szó. A már korábban említett image másolati technikával kell speciális, hardveresen biztosított írásvédettség mellett másolatot készíteni az adathordozóról. Ezt követően ezt a másolatot vizsgálja a szakértő vagy akár a nyomozó, ügyész vagy bíró.

Nézzük, hogy mely kérdések tartoznak a szakértőnek felteendő kérdések közé. A Be. 99.§-a alapján „Ha a bizonyítandó tény megállapításához vagy megítéléséhez különleges szakértelem szükséges, szakértőt kell alkalmazni”. Ezen törvényhely alapján szakértőt kell alkalmazni tény megállapításához, vagyis ahhoz, hogy mi található az adathordozón, illetve tény megítéléséhez, vagyis ahhoz, hogy az adott tényt hogyan kell értelmezni. Ez igaz abban az esetben, ha különleges szakértelemre van szükség.

Úgy gondolom, hogy az írásom elején felvázolt három digitális bizonyíték közül a digitális dokumentumok olvasásához, értelmezéséhez nem szükséges szakértő. Ezt egy bünyügyi nyomozó, egy bünyügyi elemző is el tudja végezni, sőt el is kell végeznie, mivel ezekben az esetekben kriminalisztikai, jogi kérdésre keres választ. Bünyügyi szempontból van annak relevanciája, hogy egy elektronikus levélben, egy dokumentumban mit írtak, a könyvelési dokumentumokban, file-okban milyen adatok találhatóak. Az is jogkérdés, hogy egy képfelvétel pornográfnek minősül-e vagy sem.

A regisztrációs adatok elemzése szintén nem kíván szakértői tudást, tekintve, hogy a szolgáltató köteles a megkeresést a kérő szerv részére értelmezhető formában átadni az adatokat. Ilyenkor általában azokat a „személyes adatokat” kapjuk meg, melyekkel valaki regisztrálta magát egy szolgáltatás igénybevételéhez. A napló adatok esetében is úgy gondolom, hogy egyszerűbb esetekben, amikor csak egy feljelentkezés, feltöltés vagy letöltés időpontját és az ahhoz tartozó IP címet kell megállapítani, akkor azt elvégezheti a nyomozó vagy egy bünyügyi elemző is. Azonban szakértőt kell alkalmazni, ha ezekből a napló adatokból egy rendszer működéséről, megtámadottságáról kívánunk következtetést levonni.

A digitális nyomok vizsgálata szinte minden esetben szakértő közreműködését igényli, bár speciálisan képzett és speciális felszereléssel rendelkező bűnügyi elemzők is megfelelő dokumentálás mellett sok értékes információval tudják szolgálni a nyomozást.

ÖSSZEGZÉS

Úgy gondolom, hogy az internetes, számítástechnikai környezetben elkövetett bűncselekmények nyomozása során történő nyomrögzítés jogi szabályai az itt vázolt módon alkalmazhatók. Igyekeztem rávilágítani írásomban arra is, hogy hol található jogi szabályozatlanság, vagy nem egyértelmű meghatározás.

Véleményem szerint indokolt lenne az E-ker. törvény módosítása, hogy az EHT-hoz hasonlóan egyértelműen legyen meghatározva, hogy a törvény hatálya alá tartozó szolgáltató milyen adatokat köteles megőrizni és meddig.

1. Az interneten a számítógépeket IP (internet protokoll) cím alapján azonosítják. Ez leegyszerűsítve az interneten található számítógépek „telefonszáma”. Ezek az IP címek lehetnek statikus kiosztásúak, vagyis mindig ugyanaz a cím tartozik egy-egy számítógéphez, vagy lehetnek dinamikus kiosztásúak, amikor az internetre felcsatlakozó számítógép minden egyes feljelentéskor más és más IP címet kap. Dinamikus kiosztás esetén az IP cím és az időpont alapján lehet beazonosítani, hogy melyik számítógépről is van szó.
2. (8) A megőrzésre kötelezés az adat lefoglalásáig, de legfeljebb három hónapig tart. A megőrzésre kötelezés megszűnik, ha a bűnteljárást befejezték. A büntetőeljárás befejezéséről a megőrzésre kötelezettet értesíteni kell.
3. Btk. 329/A. § Szerzői és szerzői joghoz kapcsolódó jogok megsértése.
4. BH2000. 288. III. Ha a szerzői és szomszédos jogok megsértése bűncselekményének az elkövetési tárgya az átmásolt program, az adathordozó volt: ennek elkobzása nem mellőzhető [Btk. 77. § (1) bek. a) és e) pont, 329/A. §].
5. Akkor fordul elő ez a helyzet, ha egy cég tárhelyszolgáltatással, honlap üzemeltetéssel, levelező szolgáltatás üzemeltetésével is

Fontosnak tartom, hogy a Be. 158/A.§-ban meghatározott számítástechnikai rendszer útján rögzített adatok megőrzésre kötelezés szóhasználatát hangolják össze az eljárásjogi törvény egyéb rendelkezéseivel.

Szükséges továbbá az egységes gyakorlat kialakítása és iránymutatás kidolgozása a megkeresések ügyészi engedélyhez kötése tekintetében, valamint az elektronikus levelek lefoglalásának kérdésében is. Álláspontom szerint ezt megnyugtatóan jogszabály módosításával lehetne csak rendezni.

*Dr. Peszleg Tibor r. őrnagy
ORFK NNI
Terrorizmus és Extrémizmus
Elleni Osztály*

Az írás másodközlés, megjelent az *Ügyészek Lapjának* 2005. februári számában.

- foglalkozik, és ezt egy szerveren vagy számítógépes hálózaton üzemelteti. Ilyenkor nem egy esetben egy bizonyos tárterületen található illegális tartalom, mely miatt a nyomozó hatóság eljárást kezdeményez és az egész szervert vagy számítógépes hálózatot lefoglalja. Ilyenkor azok a szolgáltatások is elérhetetlenek, melyek ugyanazon a szerveren vagy számítógépes hálózatban üzemeltek.
6. Természetesen annak a nézetnek is van jogosultsága, hogy elektronikus postafiók adatait csak ügyészi engedéllyel foglalhassa le a nyomozó hatóság, mivel csak akkor tekinthető kézbesítettnek, ha azt már a saját számítógépére letöltötte, és az nem az internet valamelyik szervergépén található. Úgy gondolom, hogy akár ez a fajta felfogás és gyakorlat is alkalmazható, hiszen ez nagyobb kontrollt ad az ügyészség kezébe, ami a jogbiztonság szempontjából hasznosnak mondható. Azonban ez a nézet nem veszi figyelembe következetesen azt a gyakorlatot és elvet a kézbesítés szabályainál, amit a postatörvényben megfogalmaztak: hogy alapesetben a szolgáltató rendszerének az utolsó pontja legyen az a pont ahol kézbesítettnek kell tekinteni egy postai küldeményt, ahol a címzett dönti el, hogy mikor veszi azt kézbe...