Az elektronikus adatokat érintő eljárási cselekmények végrehajtása

Bevezetés

A lefoglalás és a kutatás a két leggyakrabban alkalmazott – vagyont érintő – kényszerintézkedés. Szerepük az elektronikus adatok és az azokat hordozó információs rendszerek tekintetében is megkérdőjelezhetetlen, szinte minden büntetőeljárásban sikerrel alkalmazhatók gondos tervezést követően.

Megjegyzendő azonban, hogy elektronikus adat nem kizárólag kényszerintézkedés során szerezhető be, hanem akár egy egyszerű adatkéréssel, vagy a hatóság önálló rögzítésével is. Az adatok kezelésével kapcsolatos kötelezettségek, az alapvető vizsgálati módszerek azonban minden esetben azonosak.

Az előkészületi szakaszban mind az eljárással érintett személy, mind pedig a helyszín tekintetében érdemes tájékozódni arról, hogy milyen információs rendszereket és elektronikus adatokat fog érinteni az eljárási cselekmény, és milyen szakismerettel rendelkezik az ezeket használó személy. Utóbbi rendkívül fontos információ, hiszen sokszor jóval összetettebb metodikai lépéseket kell követni abban az esetben, ha az eljárással érintett személy jártas az informatika világában.

Az elsődleges cél az eljárási cselekmény eredményes lefolytatása, eközben különös tekintettel kell lenni az eljárásban részt vevő személyek és vagyontárgyak biztonságára is. Közvetlenül a végrehajtás előtt pontosan meg kell határozni – az alapvető kriminál taktikai lépéseken túl –, hogy ki a felelős az eljárás vezetéséért, a jegyzőkönyvezésért, a hardver- és szoftverelemek átvizsgálásáért, illetve a tárgyak csomagolásáért. Elképzelhető, hogy ezek a személyek egybeessenek – például a hatóság épületében egy kihallgatás alkalmával lefoglalt adathordozó esetében –, azonban a helyszíni munkavégzés során a felelősségek konkretizálása nagyban növeli az eljárás sikerének és eredményességének esélyét is.

A helyszín szerepe a végrehajtásban

Fontos megkülönböztetni, hogy az eljárási cselekmény a hatóság hivatali helyiségében vagy külső helyszínen folyik, hiszen mindkét esetben más és más körülményekhez kell alkalmazkodni. A hatóság épületében rendelkezésre állnak

https://doi.org/10.36250/01004_08

a szükséges eszközök, amennyiben nehézség adódik, az a legtöbbször más eszköz vagy eljárási módszer alkalmazásával kiküszöbölhető. Ezzel szemben a külső helyszínen végrehajtott eljárási cselekmények esetében – kevés kivételtől eltekintve – kizárólag az ott rendelkezésre álló eszközök használhatók.

A hatóság épületében végrehajtott eljárási cselekmények már ismert eszközök tekintetében történnek meg – amelyre jobban fel lehet készülni, esetleg a megfelelő szakismeretekkel rendelkező szaktanácsadó igénybevételével –, azonban egy idegen helyen nem határozható meg előre az érintett eszközök köre, a hatóság eljáró tagjai legtöbbször saját magukra vannak utalva.

Általánosságban a helyszíni munka során érdemes olyan módszereket alkalmazni, amelyek kimenetele és idő-, illetve eszközigénye nagy bizonyossággal előre meghatározható.

A Nyer. arról rendelkezik, hogy az eljárási cselekményt úgy kell előkészíteni és lefolytatni, hogy az eljárás észszerű időn belül befejezhető legyen, az eljárási cselekmény megismétlése vagy újabb eljárási cselekmény elvégzése lehetőleg ne váljon szükségessé. Az eljárási cselekmény továbbá – jogszabály eltérő rendelkezése hiányában – csak kivételesen és csak rövid időre szakítható meg (Nyer. 38. §).

A helyszíni munka során könnyen előfordulhat olyan helyzet, amikor alaposan mérlegelni kell az „észszerű" időn belüli befejezés, valamint a jogszabály által biztosított egyéb eljárási cselekmények alkalmazása közötti választás lehetőségét, hiszen több nagykapacitású adathordozó helyszíni mentése – például egy rack-szekrényben elhelyezve – akár több napot is igénybe vehet.

Az eszközök szerepe a végrehajtásban

Jellegéből adódóan az informatikai rendszerekkel végzett helyszíni munka rendkívül sok eszközt, felszerelést igényel. Egy külső helyszínen végrehajtott eljárási cselekmény – például kutatás – esetében az eszközök helyszínre szállítását, majd azoknak a biztonságos üzemeltetését is lehetővé kell tenni. Csupán az alapvető adatmentő eszközök, valamint az alkalmazásukhoz elengedhetetlen szerszámok szállításához is minimum három nagyobb méretű táska (koffer) szükséges. A kutatás kezdetén nem célszerű minden felszerelést kézben tartani, hiszen az akadályozhatja a sikeres intézkedést.

A szükséges eszközök listája természetesen minden esetben más és más. Érdemes azonban előre összekészíteni egy olyan eszközparkot, amely a legtöbb

helyszínen eredményesen alkalmazható mind az információs rendszerek átvizsgálására, lefoglalására, mind pedig az elektronikus adatok lefoglalására.

Az információs rendszerekkel végzett munka során elengedhetetlenül szükséges:

- csavarhúzókészlet a lehető legtöbb fejtípussal, adapterrel, esetleg (flexibilis) hosszabbítóval;
- antisztatikus csomagolóanyag;
- nagy méretű csomagolóanyag, valamint zárócímkék, illetve buborékfólia a nem csomagolható eszközök biztonságos és hiteles lefoglalásához;
- zseblámpa;
- alkoholos jelölőfilc;
- különböző kapacitású adathordozók.

Az eszközök listája ideális esetben (és a helyszínen tervezett adatmentésre tekintettel) kiegészülhet:

- USB- és IDE/SATA-csatlakozású hardveres írásvédő eszközzel;
- mobil adatmentő eszközzel (például Cellebrite UFED Touch);
- több csatlakozóaljzattal rendelkező hosszabbítóval;
- bootolható külső HDD-meghajtóval (például Zalman VE350);
- Linux-alapú bootolható USB flash-meghajtóval (például Paladin);
- lemez- és memóriakép készítésére alkalmas szoftver önállóan futtatható változatával (például FTK Imager Portable).

Természetesen a rendelkezésre álló eszközök esetében igaz a mondás, miszerint minél több, annál jobb, így a lista a teljesség igénye nélkül tartalmazza a tapasztalatok szerint legtöbbször szükséges darabokat. A legfontosabb tényező az eszköz tekintetében is az azt kezelő személyzet, hiszen megfelelő szakismeret nélkül a legjobb rendelkezésre álló technika is használhatatlannak bizonyulhat. Amennyiben már a tervezési fázisban felmerül, hogy a helyszínen komplex rendszerekre kell számítani, vagy olyan tevékenységet kell végezni, amely különleges szakértelmet igényel, akkor célszerű szakértő vagy szaktanácsadó bevonásával eljárni.

Elektronikus adatok lefoglalása

Napjainkban az okoseszközök korszakát éljük, egy olyan korszakot, amelyben még a mosógép, a porszívó, de akár a hűtőszekrény is hordozhat elektronikus adatokat. Az adathordozók formai világa, megjelenése – akárcsak az információs rendszereké – rendkívül sokrétű, ami sok esetben megnehezíti azonosításukat, felderítésüket is.

Az információs rendszerekkel, illetve elektronikus adatokkal végzett munka első lépése ezek azonosítása és felkutatása, ezt követően kerülhet sor a hordozott elektronikus adatoknak vagy maguknak az eszközöknek a lefoglalására.

A Be. 315. § (1) bekezdése határozza meg, hogyan lehet az elektronikus adatokat lefoglalni. Ez alapján az elektronikus adat lefoglalását

- az elektronikus adatról másolat készítésével;
- az elektronikus adat áthelyezésével;
- az azt tartalmazó információs rendszer vagy adathordozó teljes tartalmáról történő másolat készítésével;
- az azt tartalmazó információs rendszer vagy adathordozó lefoglalásával; vagy
- jogszabályban meghatározott más módon lehet végrehajtani.

Az elektronikus adat lefoglalását tehát a hatóság a birtokában lévő adathordozóra történő mozgatással vagy az azt tartalmazó információs rendszer vagy adathordozó lefoglalásával hajtja végre.

A helyszínen az adatok mozgatása sokszor nehézkes, mivel az adatátviteli sebesség korlátozott, így egy nagyobb kapacitású adathordozóról hiteles másolat készítése több órát is igénybe vehet. Az eljárás során érdemes tájékoztatni az eljárás vezetőjét arról, hogy amennyiben helyszíni adatmentésre kerül sor, az az eljárás elhúzódását eredményezheti. Minden esetben egyedi megítélés kérdése, hogy szükség van-e az adatok helyszíni mentésére, vagy az információs rendszer, illetve adathordozó lefoglalásával elég, ha arra egy későbbi időpontban kerül sor.

Fontos azonban tekintettel lenni a – fentebb említett – Be. 315. § (5) bekezdésére, amely szerint az elektronikus adatot tartalmazó információs rendszer vagy adathordozó akkor foglalható le, ha az elkobozható, illetve vagyonelkobzás alá esik; az tárgyi bizonyítási eszközként bír jelentőséggel; vagy a bizonyítás érdekében az abban tárolt, előre meg nem határozható vagy jelentős mennyiségű elektronikus adat átvizsgálására van szükség.

Könnyen belátható, hogy az eljárások többségében előre meg nem határozható mennyiségű elektronikus adat átvizsgálására van szükség, így az információs rendszer lefoglalása a legtöbb esetben megalapozott.

Különbséget kell tenni azonban az elektronikus adat és az azt tartalmazó adathordozó adattartalma között is. Attól, hogy az elektronikus adat egy adathordozón van jelen, még nem indokolt sem az adathordozó, sem pedig teljes adattartalmának lefoglalása sem.

Kiemelendő, hogy amennyiben elektronikus adatokat foglal le a hatóság, az nem kötődik fizikailag egyetlen adathordozóhoz sem, így az adathordozót nem is feltétlenül kell lefoglalni. Az adathordozó az elektronikus adatnak csupán hordozója, amennyiben az adat lefoglalásáról intézkedett a hatóság, úgy az adathordozótól külön kezelendő.

Amennyiben a Btk. 72. §-ában szabályozott elkobzás, illetve a Btk. 74. § szerinti vagyonelkobzás szabályai fennállnak, az információs rendszer lefoglalásáról is intézkedni kell.

Azokban az esetekben, amikor

- a bűncselekmény elkövetéséhez az információs rendszert eszközül használták;
- annak birtoklása jogszabályba ütközik;
- azt a bűncselekmény elkövetése során vagy azzal összefüggésben szerezték (akkor is, ha azzal más gazdagodott), vagy ennek a vagyonnak a helyébe lépett;
- azt a bűncselekmény elkövetése céljából az ehhez szükséges vagy ezt könnyítő feltételek biztosítása végett szolgáltatták, vagy arra szánták;
- az adott vagy ígért vagyoni előny tárgya volt,

az információs rendszert is le kell foglalni. Különös tekintettel kell tehát eljárni az olyan bűncselekmények esetében, ahol az elkövetés eszköze az információs rendszer volt, hiszen ebben az esetben nem elegendő csupán az elektronikus adat vagy az azt tartalmazó adathordozó lefoglalása.

Az elektronikus adat lefoglalásának módjai

Az új Be. rendelkezései közé emelt több, rendkívül fontos eljárási részletszabályt is, amelyeknek az elektronikus adat lefoglalása esetében bármely végrehajtási mód tekintetében érvényesülniük kell.

Erre tekintettel az elektronikus adat lefoglalását úgy kell végrehajtani, hogy az a büntetőeljárás céljából szükségtelen elektronikus adatra lehetőleg ne terjedjen ki, illetve az ilyen elektronikus adatot a lefoglalás a legrövidebb ideig érintse.

A lefoglalás végrehajtásához indokolt esetben szaktanácsadót kell igénybe venni.

Lefoglalás másolat készítésével

Számítástechnikai értelemben a másolás valamely adathalmaz duplikálását jelenti, amelynek tartalma ugyan azonos lesz az eredeti állománnyal, bizonyos jellemzői – így a hozzáférésre és létrehozásának idejére vonatkozó információk – a használt fájlrendszernek megfelelően változhatnak. Ezek a tulajdonságok a fájlrendszerekben az adatállományhoz kapcsolódóan vannak rögzítve, így a továbbiakban mégsem beszélhetünk az eredetivel teljesen megegyező, azonos állományról.

A lefoglalás során azonban minden pillanatban biztosítani kell azt, hogy a lefoglalt adatállomány pontosan megegyezzen azzal az adattartalommal, amely eredeti formájában a lefoglalással érintett adathordozón a lefoglalás pillanatában megtalálható. Utóbbi feltételeknek külön-külön is kiemelkedő jelentősége van.

A lefoglalás tekintetében a 11/2003. (V.8) IM-BM-PM együttes rendelet is alapvető követelményként fogalmazza meg, hogy a másolt adatállomány ne legyen megváltoztatható – ezzel is biztosítva az eredetivel való egyezést. Így a másolásra alapvetően nem kerülhet sor a szokványos – az operációs rendszerbe épített – másolási algoritmusok alkalmazásával. Szintén követelményként határozza meg a rendelet, hogy az elektronikus adat lefoglalásakor az átmásolás lehetőség szerint utólag meg nem változtatható adathordozóra történhet – ami elképzelhetetlen nagyobb adatmennyiség esetében, így sokkal életszerűbb egy konténerfájl létrehozása az adathordozón, ezáltal biztosítva a meg nem változtatható jelleget. Az átmásolást megelőzően a lefoglalás helyszínén ellenőrizni kell, hogy a hatóság által az átmásoláshoz használt adathordozó adatokat nem tartalmaz, kivéve azt az esetet, amikor több konténerfájlt hozunk létre, és azokat egy adathordozón helyezzük el. A jogalkotó szándéka e szabály beiktatásával vélhetően a kisebb méretű elektronikus adatok lefoglalásának szabályozása volt, amely értelemszerűen történhet például egyszer írható optikai lemezre is.

A rendelet alapján az elektronikus adat lefoglalását másolat készítésével kell végrehajtani, ha

– a lefoglalt dolog érintett őrizetében hagyásának feltételei fennállnak, és
– a másolat készítését követően az adat eredeti helyen való további tárolása a büntetőeljárás érdekeit nem veszélyezteti.

A lefoglalás során a másolat egyezőségét biztosítandó hiteles másolat készül az adatállományról. A hitelességet a másolási folyamat lezárásaként számolt hashérték (ellenőrző összeg) garantálja. A hashérték egy matematikai algoritmusok segítségével számolt, kizárólag egy adott byte-szerkezetű adatállományra jellemző karakterlánc. Az adatállomány szerkezetének legkisebb változása is eltérő hashértéket eredményez, így az eredeti és a másolt állomány azonossága a hashértékek összevetésével bármely időpillanatban kétséget kizáróan igazolható.

A kriptográfiában leggyakrabban használt hashalgoritmusok az MD5, a SHA-1, -2, -3, a RIPEMD, illetve a Whirlpool-algoritmus. Minden egyes algoritmus más-más matematikai műveletekkel hozza létre a jellemző karakterhosszúságú hashértéket, amely ezt követően az adathalmaz „ujjnyomataként" is értékelhető. Mivel a kulcsképzés matematikai műveletekkel történik, a létrehozásához a másolás időigényén túl további időre van szükség. A hatékonyság-megbízhatóság-létrehozási idő tekintetében a tapasztalat azt mutatja, hogy az SHA-1 algoritmus használata a legcélszerűbb. Általánosságban elmondható, hogy minél bonyolultabb egy algoritmus, annál megbízhatóbb is – azaz nehezebb „feltörni" –, ugyanakkor annál időigényesebb is a létrehozása. Kétséget kizáróan alkalmazható egyszerre kettő (vagy több) – különböző matematikai algoritmuson alapuló – hashérték feltüntetése az adatösszesség mellett.

Az eredeti és a másolt állomány egyezőségének megállapításához mindkét állomány egyidejű jelenlétére van szükség, amely logikusan nem minden esetben biztosítható. A gyakorlat alapján így a helyszínen számított ellenőrző összeg a lefoglalásról készített jegyzőkönyvben van rögzítve, amely a másolt adatállomány tekintetében bármely pillanatban újraszámítható hashértékkel összevethető. Az adatok egyezősége az eljárás során így a fenti módszerrel biztosított, és bármikor igazolható.

Előfordulhat olyan eset is, amikor az eredeti adat – például egy hozzáférési naplóállomány – folyamatosan változik, vagy jellegére tekintettel – például felhőalapú szolgáltatásokban elérhető adatok – nem menthető le kétszer ugyanabban a formában. Ilyen esetben is a lefoglalásról készített jegyzőkönyvben rögzített hashérték biztosítja az adatállomány változatlanságát – gyakorlatilag tehát azt igazoljuk, hogy a vizsgált adatállomány megegyezik a lefoglalás pillanatában keletkezett adatállománnyal.

Fontos és mással nem pótolható eljárási lépés tehát a lefoglalásról készült jegyzőkönyvben a korábbiakban jelölt ellenőrző összeg szerepeltetése. Az eljárás későbbi szakaszában, akár az eredeti adathordozó vagy az eredeti adat megsemmisülése esetén is igazolható, hogy a bizonyítás során felhasznált adatállomány pontosan megegyezik a lefoglalt adatállománnyal.

Amennyiben az adatot időközben törlik, illetve módosítják, kerül, az eljárási módszer hitelességét akkor is biztosítja a jegyzőkönyvben már rögzített érték, amely különös jelentőséget az elektronikus adat áthelyezéssel történő lefoglalása esetében, valamint az elektronikus adat ideiglenes vagy végleges hozzáférhetetlenné tételére irányuló eljárásokban nyer.

Az egyes másolatkészítési eljárások (az adatmentés típusai) a következők:

– teljes bitazonos másolat (vagy tükörmásolat),
– forenzikus másolat,
– egyszerű másolat.

A bitazonos másolat esetében – nevéből adódóan – a forrás adattartalom minden bitje leképeződik a céladathordozón. Amennyiben egy adathordozó teljes adattartalma egy másik adathordozóra képeződik le, és a másik adathordozón „megmaradt" hely kizárólag nullával van feltöltve, akkor tükörmásolatról beszélünk.

A forenzikus másolat esetében hitelesített szoftver felhasználásával készül bitazonos másolat az adattartalomról – legtöbbször egy konténerfájlba, amely tömöríthető, így kevesebb helyet igényel, mint az eredeti adatösszesség. Egy adathordozóra több forenzikus másolat is kerülhet.

Az egyszerű másolat esetében nem hitelesített úgynevezett „backup" szoftverrel vagy az operációs rendszer beépített másolóalgoritmusával történik az adattartalom leképezése egy másik adathordozóra. Bár az adat változatlansága ebben az esetben nem biztosított, előfordulhat olyan helyzet, amikor az adatok lefoglalásának az egyszerű másolás az egyetlen módszere – például távoli szerverszolgáltatáson elhelyezett elektronikus adatok, amelyek csupán hálózati meghajtóból érhetők el a vizsgált eszközön.

Az elektronikus adatok mentésére hitelesített fizikai írásvédő eszköz közbeiktatásával kerülhet sor. Egy adathordozó számítógéphez történő csatlakoztatásakor az eszközre telepített operációs rendszer azt „felcsatolja", hogy a későbbiekben azon írási, illetve olvasási műveleteket végezhessen a felhasználó. A felcsatolás folyamata azonban adatírással jár, azaz a merevlemez eredeti tartalma megváltozik, hacsak nem kerül az eszközök közé egy fizikai írásvédő eszköz

közbeiktatásra. Az írásvédő megakadályozza, hogy az operációs rendszer adatokat továbbítson a forrás adathordozóra, így annak tartalma változatlan marad.

A hitelesített másolat létrehozásához az írásvédő eszközön túl hitelesített szoftvereket kell alkalmazni, amelyek az adatok beolvasását, fájlba írását, illetve a hitelesítő összeg kiszámítását is elvégzik. Ilyen szoftver lehet többek között az AccessData FTK Imager nevű, ingyenesen hozzáférhető alkalmazás. Az alkalmazás a nyomozó hatóságok tagjainak regisztrációt követően ingyenesen hozzáférhető a https://accessdata.com/product-download weboldalon.

Lefoglalás az elektronikus adat áthelyezésével

Az áthelyezés mint számítástechnikai művelet leegyszerűsítve egy másolási, illetve egy törlési folyamatból tevődik össze. Az áthelyezéssel érintett állomány először a célhelyre kerül átmásolásra, majd a forrás helyén törlésre. Az ilyen módon átmozgatott adat eredeti tárolási helyén a továbbiakban nem lesz fellelhető.

A végrehajtási rendelet alapján az elektronikus adat lefoglalását áthelyezéssel kell végrehajtani, ha az adat eredeti helyen történő további tárolása a büntetőeljárás érdekeit veszélyezteti.

Mivel jellegét tekintve egy másolási folyamatról beszélünk, az eljárási rend az elektronikus adat másolással történő lefoglalásával megegyezik. Az egyetlen különbséget itt az jelenti, hogy az eredeti adatállomány a továbbiakban nem lesz elérhető, csupán a másolat. Ahhoz azonban, hogy az eredeti adatösszesség ne legyen elérhető a forráseszközön, nem elegendő csupán egyszerű törlési műveletet végezni, hanem az elektronikus adatok által lefoglalt szektorokat nullával kell feltölteni – ez az úgynevezett *wipe-folyamat.*

A hitelességet ebben az esetben kizárólag a jegyzőkönyvben szereplő – és a lefoglalt adatállomány tekintetében számított – ellenőrző összeg biztosítja. Amennyiben az eljárás során meg kell bizonyosodni arról, hogy a vizsgált adatállomány a lefoglalt adatokkal megegyezik, akkor az újraszámolt ellenőrző összeget kell összevetni a jegyzőkönyvben szereplő értékkel. Ebben az esetben célszerű nem csupán egyfajta hashalgoritmussal dolgozni, hiszen egyszerre több alkalmazása növeli a megbízhatóságot.

Az áthelyezés során az eljárónak különös figyelemmel kell lennie arra, hogy az adatok törlése mások jogát, illetve jogos érdekét a törvényben meghatározott mértéket meghalódóan ne sértse vagy veszélyeztesse. A büntetőjog alapelveinek tekintetében az arányosság elve itt is előtérbe kerül.

Lefoglalás az elektronikus adatot tartalmazó információs rendszer vagy adathordozó teljes tartalmáról történő másolat készítésével

Az elektronikus adat lefoglalásának teljesebb módja az adatot tartalmazó adathordozó teljes tartalmáról történő másolat készítése, mivel ilyen esetben nemcsak az elektronikus adat hozzáférhető, hanem további járulékos információk is, amelyeket a fájlrendszer további – akár üres területei – tartalmaznak. Fontos azonban, hogy a már említetteknek megfelelően teljes másolat csak akkor készíthető, ha azt jogszabály lehetővé teszi.

A 11/2003. (V.8.) IM-BM-PM együttes rendelet alapján az elektronikus adat lefoglalását az azt tartalmazó adathordozó vagy információs rendszer teljes tartalmáról történő másolat készítésével kell végrehajtani, ha a bizonyítás szempontjából az adatot tartalmazó információs rendszer vagy adathordozó teljes tartalmának jelentősége van, ideértve azt is, ha a bizonyítás érdekében az információs rendszerben tárolt, előre nem meghatározható vagy jelentős mennyiségű adat átvizsgálására van szükség.

A másolat elkészítésének folyamata megegyezik a másolással történő lefoglalás esetében említettekkel, azonban itt nem egyszerű vagy forenzikus másolat készül, hanem teljes bitazonos másolat (vagy más néven tükörmásolat).

A lefoglalás végrehajtásának ezen módja biztosítja, hogy az adathordozón lefoglaltként meg nem jelölt – azaz üresnek látszó – szektorokból a hatóság, illetve a szakértő az eljárás során adatokat állítson vissza – amelyre a Be. is lehetőséget teremt. A módszerrel korábban törölt, de még felül nem írt állományok, illetve részállományok állíthatók vissza és tehetők vizsgálat tárgyává.

A teljes információs rendszer vagy adathordozó adattartalmának másolása időigényes folyamat, amelyet az eszközök közötti átviteli sebesség korlátoz. Nagyobb kapacitású rendszerek esetében az eljárás több órát is igénybe vehet, ebben az esetben pedig az ellenőrző összeg számítása is jóval lassabb.

Az elektronikus adat lefoglalása az azt tartalmazó információs rendszer vagy adathordozó lefoglalásával

A legegyszerűbb és a gyakorlatban is legtöbbször alkalmazott lefoglalási módszer – amely mindezen tulajdonságai ellenére egyben az egyik leginkább szakszerű – nagy valószínűséggel az elektronikus adatot tartalmazó adathordozó fizikai egészében történő lefoglalása.

A kényszerintézkedés gyorsasága sokszor kulcsfontosságú az eljárás sikerének biztosítása érdekében. Ez a gyorsaság azonban nem mehet a szakszerűség és a törvényesség rovására. Amennyiben a megfelelő informatikai szakismeretekkel, illetve jártassággal rendelkező személy az eljárási cselekményen nincs jelen, úgy nemcsak a legkézenfekvőbb módszer az adathordozó vagy az információs rendszer lefoglalása, hanem szakszerűség szempontjából is ez a legkevésbé megkérdőjelezhető. A jogszerűség talaján maradva azonban ez a lefoglalási mód is kizárólag abban az esetben alkalmazható, ha a Be. ezt lehetővé teszi.

A lefoglalás végrehajtásának módozatait tekintve közös, hogy a 11/2003. (V.8.) IM-BM-PM együttes rendelet rendelkezései alapján a bűnjelet olyan módon kell megjelölni, hogy az azon rögzített adatok meg legyenek jelölve, méghozzá úgy, hogy az adathordozó tartalma azonosítható legyen.

A jogszabályhely „korszerűtlen" megfogalmazása az adatok és a programok megjelölése tekintetében szembetűnő, hiszen a technika jelenlegi állása szerint egyetlen adathordozón több ezer program és több milliárd sornyi adat is szerepelhet, amelyek pontos megjelölése nyilvánvalóan lehetetlen feladat lenne. Az egyértelmű azonosítás végett a hatóságnak ehelyett érdemes megjelölni a mentett állomány elnevezését és kiterjesztését, annak méretét és a számított ellenőrző összeget.

Jogszabályban meghatározott más módon történő lefoglalás

A Be. lehetővé teszi, hogy rendelkezéseitől eltérően ne a felsorolt módozatok valamelyikén foglalják le az elektronikus adatot, hanem bármely jogszabály által megjelölt egyéb módon.

A legkézenfekvőbb példa erre éppen a Be. egyik szintén új szabályozási formája, amely szerint a fizetésre használt elektronikus adat lefoglalását úgy is végre lehet hajtani, hogy az elektronikus adattal olyan műveletet végeznek, amely az érintettnek az elektronikus adat által kifejezett vagyoni érték feletti rendelkezési lehetőségét megakadályozza. A 11/2003. (V.8.) IM-BM-PM együttes rendelet szabályozza továbbá azt is, hogy e művelet elvégzése végrehajtható olyan művelettel is, amely alapján a fizetésre használt elektronikus adat értékét a bűnjelkezelő e célból rendszeresített számláján írják jóvá.

A hatósági adatmentés készítése

A helyszínen adatmentés készítése akkor indokolt, amikor az adatok beszerzése nem tűr halasztást, vagy olyan destruktív, illetve titkosító algoritmus található az elektronikus adatokat tartalmazó eszközön, amely egy későbbi időpontban lehetetlenné teszi az adatok kinyerését.

Az elektronikus adatok lefoglalása ebben az esetben a legtöbbször másolat készítésével történik, akár forenzikus másolatról, akár teljes, bitazonos másolatról beszélünk. A Be. lehetőséget teremt az áthelyezéssel történő lefoglalásra is, ez azonban akkor lehet releváns, ha fizetésre használt elektronikus adatokat foglal le a hatóság, vagy ha például az elektronikus adatok birtoklása jogszabályba ütközik, ám nem a fizikai rendszer tulajdonosa tárolja az adatokat az információs rendszeren. A legegyszerűbb példa erre egy szerverszolgáltató, amelytől akár virtuális, akár dedikált szervert bérelt az érintett, és azokon olyan tartalmakat tárolt, amelyek birtoklása jogszabályba ütközik. Ha azonban a bérelt információs rendszer felhasználásával bűncselekményt követtek el, úgy a Be. lehetőséget teremt a teljes információs rendszer lefoglalására is tekintet nélkül arra, hogy az elkövető nem a rendszer tulajdonosa.

Az adatmentés két formája különíthető el attól függően, hogy az eszköz bekapcsolt vagy kikapcsolt állapotban van-e.

Kikapcsolt eszköz

Az eszköz kikapcsolt állapotában érdemes egy nagyon egyszerű elvet követni: maradjon is kikapcsolva. A bekapcsolás minden esetben adattartalom-módosulással jár, amely a későbbi szakértői vizsgálat során is kimutatható lesz, így csak rendkívül indokolt esetben szabad az ilyen eszközt bekapcsolni.

Fontos meggyőződni arról, hogy az eszköz valóban kikapcsolt állapotban van, vagy csak úgy tűnik. A gyártók körében energiatakarékossági szempontok miatt népszerű lett az úgynevezett „hibrid alvás" üzemmód alkalmazása. Ebben az üzemmódban úgy tűnik, hogy az eszköz ki van kapcsolva, a képernyőn nem jelenik meg tartalom, a visszajelző LED-ek nem világítanak, azonban az eszköz mégis üzemkész, azonnal „ébreszthető" állapotban van. Ilyen esetben akár egy gombnyomásra vagy fedélnyitásra is aktiválódik a gyorsindítási folyamat, amelynek következtében már bekapcsolt állapotú rendszerrel kell dolgozni.

A „hibrid alvás” üzemmódban lévő eszközök ilyen állapotának felderítése azért is fontos, mert sok eszköz ebben az állapotában csatlakozik az internetre a már ismert vagy szabadon hozzáférhető hotspotokon keresztül, így utasításokat is képes fogadni, helyadatokat oszt meg, valamint azzal távoli interakciók végezhetők.

Az alvásüzemmód ellenőrzéséhez érdemes az egeret mozgatni (vagy a touchpadot megérinteni), illetve ha ezt a funkciót letiltották, akkor a SHIFT billentyűt megnyomni. Kerülendő az ENTER, ESC, DEL, WIN stb. funkciógombok használata, mivel azok az éppen futó szoftverek működését befolyásolhatják.

Az ilyen eszközöket lehetőleg ebben az állapotukban kell lefoglalni egy árnyékoló tasakban történő elhelyezéssel, és azt mielőbb át kell adni a szakértőnek, hogy az érdemi vizsgálatot megkezdhesse, hiszen az akkumulátor kapacitása véges, és ebben az állapotban, ugyan csak minimális fogyasztása van a hardvernek, előbb-utóbb lemeríti az akkumulátort.

A sötét – nem reagáló – képernyő önmagában nem jelenti azt, hogy az eszköz ki van kapcsolva, hiszen elképzelhető, hogy csupán a képernyő csatlakozását, áramellátását kell ellenőrizni.

A teljesen kikapcsolt eszköz lefoglalása a dokumentálással kezdődik, amelynek a későbbiekben fontos szerepe lehet. Az eszközt eredeti környezetében is érdemes lefotózni, hiszen akár az egyes csatlakozási pontok elhelyezkedésének is szerepe lehet a későbbi vizsgálat során. Magáról az eszközről is külön felvételeket kell készíteni, hiszen ezek szükségesek az esetlegesen már létező sérülések, hiányok dokumentálásához is.

Az eszközt áramtalanítani kell a hálózati csatlakozó kihúzásával, majd az egyes csatlakozópontokat is fel kell szabadítani. Akár a jegyzőkönyvön kívül is, de érdemes az egyes csatlakozók helyzetét, csatolási pontját is dokumentálni, hiszen annak a szakértői vizsgálat keretében jelentősége lehet. Amennyiben a fényképfelvételeken ezek láthatók, úgy a szöveges dokumentáció mellőzhető.

Az eszköz lefoglalása a csomagolással folytatódik, amelynek során ügyelni kell arra, hogy a csomag hitelesen legyen lezárva. Amennyiben az eszközt például méretéből adódóan nem lehet csomagolni, abban az esetben házának megnyitási pontjait kell – roncsolásmentesen – lezárni egy arra alkalmas címkével. A be nem csomagolt eszközök szállításánál különös tekintettel kell lenni a potenciális sérülések megelőzésére, lehetőség szerint buborékfóliát vagy egyéb védőeszközt kell alkalmazni.

Bekapcsolt eszköz

Ha az eszköz bekapcsolt állapotban van, és azon valamilyen operációs rendszer fut, mérlegelni kell, hogy rendelkezünk-e elég szakismerettel a rendszer „élő" állapotában történő vizsgálatához, illetve egyáltalán szükség van-e erre.

Amennyiben az azonnali adatelemzéstől nem várható eredmény, vagy az időben elhalasztható, és a Be. 315. § (5) bekezdése lehetőséget teremt rá, úgy érdemes az információs rendszer egészének lefoglalása mellett dönteni, hiszen így az eljárás nem húzódik el indokolatlanul, és az adattartalom sem változik meg jelentősen.

A bekapcsolt eszköz vizsgálata, illetve azzal bármilyen művelet végzése nagyban függ attól, hogy otthoni vagy vállalati környezetben található-e a rendszer. Vállalati környezetben egy eszköz szerverszerepet is betölthet, illetve önálló munkaállomása is lehet egy virtuális környezetnek. Előbbi esetben annak vizsgálata és áramtalanítása is különleges szakértelmet igényel, hiszen tekintettel kell lenni a hálózati környezetben betöltött szerepére is; utóbbi esetben pedig elképzelhető, hogy a gépen semmilyen releváns elektronikus adat nem található, csak egy kliensprogram, amely egy távoli VPS-szerverhez kapcsolódik.

Az első lépés, ha bekapcsolt állapotú eszköz található a helyszínen, hogy senki ne kerüljön annak közvetlen közelébe az eljáró hatóság vizsgálatra kijelölt tagján túl. Akár egyetlen gombnyomás is elindíthat olyan folyamatokat, amelyekkel az eszköz adattartalma megváltozik. Ha a kijelzőn látható valamilyen tartalom, akkor arról is, illetve az egész eszközről és környezetéről is érdemes fényképfelvételeket készíteni, ezáltal az adattartalom későbbi vizsgálatakor is képet kaphat az ezeket elemző személy arról, milyen tevékenységet végeztek utoljára az eszközön.

Az eszköz vizsgálatát annak bekapcsolt állapotában is érdemes a lehető legkevésbé invazív technikák alkalmazásával végrehajtani. Alapvetően minden rendszert érintő vizsgálati folyamat invazív, hiszen az éppen futó rendszerállományok tekintetében írási műveletet végez, ezért korlátozni kell az alkalmazott technikákat, illetve azok végrehajtási idejét is.

Ebben az esetben először ellenőrizni kell, hogy fut-e bármilyen destruktív folyamat az eszközön. Ennek azonosítása nem minden esetben magától értetődő. Ha a kijelzőn a *wiping, deleting* (törlés), *formatting* (formattálás) kifejezések jelennek meg, akkor nyilvánvalóan éppen adatvesztés történik. A legjobb döntés a destruktív folyamat felismerését követően az eszköz áramtalanítása – csatlakozójának aljzatból történő eltávolítása, vagy ha eltávolítható akkumulátorral

rendelkezik, annak eltávolítása. Természetesen minden ilyen lépést – akárcsak a felismert folyamatokat – dokumentálni kell.

A destruktív folyamatok jelenlétének vizsgálatát követően azt kell ellenőrizni, hogy az eszköz csatlakozik-e valamilyen hálózatra. A csatlakozás történhet vezetéken keresztül vagy vezeték nélküli kapcsolattal is. A hálózatra kapcsolt eszközök esetében fennáll annak veszélye, hogy adattartalma távoli eléréssel vagy időzített folyamat indításával módosulhat. Ebben az esetben tehát meg kell szakítani a hálózati kapcsolatot a hálózati kábel lecsatlakoztatásával vagy a vezeték nélküli adapter kihúzásával, illetve belső adapter esetén annak letiltásával. A hálózati kapcsolat egyik jele a főképernyőn megjelenő hálózat-, illetve wifiikon. A legtöbb operációs rendszerben az ikonra kattintva van mód ki-, illetve bekapcsolni a használt hálózati eszközt.

A hálózati kapcsolat megszüntetése esetében is körültekintően kell eljárni, hiszen elképzelhető, hogy a kapcsolat megszakadása esetén az eszköz kijelentkezteti a felhasználót, vagy kikapcsol. Szintén elképzelhető, hogy az adott eszközön fizikailag nem találhatók meg a releváns adatok, a hálózaton keresztül azonban egy hálózati meghajtón vagy felhőszolgáltatáson keresztül elérhetők lehetnek. Hálózati csatlakozás esetén tehát minden esetben mérlegelni kell, hogy eljárástaktikai szempontból bekapcsolva maradhat-e a hálózat elérése az eszköz átvizsgálásáig.

Amennyiben az ügy jellege megkívánja, a bekapcsolt állapotú eszköz hálózati adatforgalma is megfigyelhető és rögzíthető speciálisan erre a célra kialakított szoftverek segítségével – például a Wireshark nevű, ingyenesen hozzáférhető szoftver alkalmazásával. A hálózati forgalmi adatok a kapcsolódásokat, kapcsolódási kéréseket, a beérkező és kimenő hálózati csomagokat egyaránt tartalmazzák, aminek a későbbi szakértői vizsgálat során kiemelkedő jelentősége lehet.

Külön kiemelendő a felhőszolgáltatások kérdése. A felhőben tárolt adatok távoli szerveren elérhető elektronikus adatok, amelyek sok esetben fizikálisan nem tárolódnak le a helyi eszközön, azonban egy felcsatolt hálózati mappából azok hozzáférhetők. Hálózati kapcsolat nélkül a felhőben tárolt elektronikus adatok lementése nem lehetséges, azokat a szolgáltató megkeresése útján lehet beszerezni.

Amennyiben a hatóság észleli, hogy a számítógépre hálózati meghajtókat csatoltak fel, azonban jelenleg azok tartalma nem jeleníthető meg, úgy a Be. 312. § (1) bekezdése alapján az elektronikus adat birtokosát vagy kezelőjét fel kell szólítani, hogy a keresett dolog hollétét fedje fel, illetve az elektronikus

adatot tegye hozzáférhetővé. Amennyiben a felszólított ennek eleget tesz, úgy az elektronikus adatok másolással lefoglalhatók.

Érdekes jogkérdés, hogy amennyiben a felhőszolgáltatás bejelentkezési adatai elérhetők a számítógépen, de az adatokhoz csak egy bejelentkezési műveletet követően lehetséges hozzáférni, úgy az eljárással érintett személy együttműködésének hiányában azokhoz a hatóság tagja hozzáférhet-e? Nyilvánvalóan a bűnüldözési érdek megkívánja, azonban sem a Be., sem a Nyer. nem rendelkezik arról, mi a teendő ebben az esetben. A jogeset természetesen nemcsak felhőszolgáltatással képzelhető el, hanem egy a kutatás során észlelt, olyan számítógéppel, amelyen egy elektronikus szolgáltatás – például e-mail-fiók – bejelentkezési felülete jelenik meg. A felületen a felhasználói név és a jelszó mezőket is kitöltötte a felhasználó, vagy azokat automatikus kitöltési szolgáltatásba mentette, de még nem jelentkezett be. A hatóság tagja vajon ebben az esetben bejelentkezhet-e a fiókba tartalmának átvizsgálása, és az elektronikus adatok lefoglalása végett?

Az egyszerűbb – és egyben gyakoribb – esetet, a felhőszolgáltatás esetét alapul véve: a kutatás pillanatában a hatóság előtt nem ismert, hogy a hálózati meghajtó egy a helyszínen elérhető távoli eszközhöz vagy egy földrajzilag is elkülönülő távoli eszközhöz csatlakozik-e, így a lefoglalás maradéktalan végrehajtásához annak tartalmát is ellenőrizni kell. Az adatok hivatalos úton történő beszerzéséről a szolgáltató megkeresése vagy jogsegélykérelem kibocsátása útján kell a későbbiekben gondoskodni.

A destruktív folyamatok vizsgálata, valamint a hálózatra csatlakozás ellenőrzését követően érdemes időt szentelni az éppen futó alkalmazások, illetve szolgáltatások ellenőrzésére is. Az alkalmazások és szolgáltatások között különös figyelmet kell fordítani azokra, amelyek egyértelműen a rendszer titkosítására vagy egyéb védelmi mechanizmusaira utalnak. Előfordulhat, hogy a rendszer bekapcsolt állapotában annak adattartalma hozzáférhető, azonban kikapcsolást követően az adatokat tartalmazó tikosított konténer is „lezár", így azok nem lesznek olvashatók. Amennyiben ilyen folyamat fut az eszközön, akkor mindenképpen gondoskodni kell annak helyszíni, bekapcsolt állapotában történő adatmentéséről.

Az eszköz memóriája rendkívül értékes információkat tartalmazhat – ilyenek lehetnek a fájl- vagy tevékenységelőzmények, jelszavak, bejelentkezési adatok stb. A helyszíni adatmentés során ezért érdemes az eszköz memóriájáról is mentést készíteni, amennyiben az ügy jellege ezt megkívánja.

Az eszközön végzett bármely műveletet dokumentálni kell, hiszen ezek annak adattartalmában változást hoznak létre. Tilos az eszközzel olyan interakció vég-

zése, amelynek hatása nem ismert, vagy ahhoz olyan különleges szakértelem szükséges, amellyel a hatóság tagja nem rendelkezik!

Az eljáró hatóság tagjai abban a szerencsés helyzetben vannak, hogy minden kérdésre megtudhatják a választ. A helyszínen ugyanis jellemzően jelen van az eszközök használója is, az eljárással érintett személy. Minden esetben célszerű nyilatkoztatni az eszköz felhasználóját a már felvázolt kérdések tekintetében. A kérdésekre adott válaszokat természetesen az eszközön lehet ellenőrizni. Ügyelni kell azonban arra, hogy a hatóság kijelölt tagján kívül senki, így az egyébként arra jogosult felhasználó sem érhet az információs rendszerekhez. Szóban kell nyilatkoztatni a helyszínen jelen lévő személyt, majd az elhangzottak mérlegelésével kell eljárni.

Amennyiben a rendszer ellenőrzése megtörtént, az eljárás vezetőjének döntése alapján sor kerülhet az elektronikus adatok lefoglalására helyszíni adatmentéssel is, valamint amennyiben a Be. lehetőséget teremt rá, a teljes információs rendszer vagy adathordozó lefoglalásával is.