Az elektronikus adatok rögzítése és az eljárási cselekmények dokumentálása

Bevezetés

A felkészülést és a végrehajtást követő utolsó, ám ugyanolyan fontos mozzanat a lefoglalt elektronikus adatok megfelelő rögzítése (csomagolása), illetve az eljárási cselekmény dokumentálása. A bizonyításhoz ugyanis nem elegendő a keresett adat megtalálása, azt megfelelően is kell kezelnünk ahhoz, hogy bizonyító erejét az eljárás végéig megtartsa. A bizonyító erő megtartása pedig az elektronikus adatok esetén sem jelent mást, mint annak igazolását, hogy a lefoglalt bizonyítási tárgy – jelen esetben az adat – a lefoglalást követően is megegyezik a lefoglaláskori állapotával, méghozzá az eljárás végéig bármikor.

Korábban többször is említettük, hogy a büntetőeljárási törvény az elektronikus adatok lefoglalásának több módját is nevesíti az adathordozó tartalma egy részének másolásától vagy áthelyezésétől, az adathordozó egész tartalmának másolásán át egészen az adathordozó vagy akár a teljes információs rendszer eredetiben történő lefoglalásáig. Nem árt megismételni azt sem, hogy ezeket a módszereket a törvény nem csupán nevesíti, hanem egyértelmű sorrendet is megjelöl az alkalmazható módszerek kapcsán (a legkisebb érdeksérelmet okozó másolástól a legnagyobb érdeksérelemmel járó fizikai lefoglalásig), minden módszer esetén megjelölve azt a törvényi többletfeltételt, amely annak alkalmazásához szükséges.

A rögzítés és dokumentálás kapcsán azonban ezek a módszerek végső soron mégiscsak két, egymástól markánsan különböző végkifejlethez vezethetnek; vagy csupán elektronikus adatot foglalunk le, vagy pedig valamilyen fizikai tárgyat, ami az elektronikus adatot tartalmazza (és bizonyító ereje is főleg ebből a tényből, nem pedig a fizikai tulajdonságaiból ered).

Nyilvánvaló, hogy a kibertérben és a valós térben létező dolgok kezelése teljesen más módszereket igényel, még ha büntetőeljárási értelemben mindkettő esetben ugyanúgy elektronikus adatok lefoglalásáról is beszélünk. Az alábbiakban ezért e kettő eset mentén választom szét a lefoglalást követően teendő intézkedéseket, kezdve a – kevesebb magyarázatot igénylő – fizikai eszközök lefoglalásával, majd bemutatva azt, hogy az „egyesek és nullák” lefoglalása miben tér el ettől.

https://doi.org/10.36250/01004_09

Elektronikus adatot tartalmazó fizikai eszközök lefoglalása

Eszközök lefoglalásáról beszélünk azon módszer esetén, amelyet a törvény „az azt tartalmazó információs rendszer vagy adathordozó lefoglalásával" fordulattal jelöl. Látható, hogy itt is rögtön két külön esetet kell elválasztanunk egymástól: az adathordozó, illetve az információs rendszer lefoglalása.

A kettő közül nyilván az adathordozó a szűkebb fogalom; ezek azok a műszaki eszközök, amelyek fő és egyetlen funkciója az adatok tárolása. A legkézenfekvőbb ilyen eszköz a merevlemez (függetlenül a fajtájától, hiszen lehet akár külső vagy belső, mágneses elven működő HDD vagy mozgó alkatrészek nélküli SSD), a pendrive és a különböző memóriakártyák, illetve az optikai adattárolók (CD- és DVD-lemezek, amelyek önmagukban ugyebár még csak elektronikus eszköznek sem tekinthetők). Említhetjük természetesen az olyan régebbi eszközöket is, mint a floppy lemezek vagy a kazetták, azonban egyre kevéssé valószínű, hogy ezekkel a jövőben találkozni fogunk a kutatások során.

Az adathordozók esetén újabb kettős felosztást érdemes figyelembe venni: az adathordozók nagyobb része megváltoztatható adatokat tartalmaz, ezért a lefoglalásuknál biztosítani kell, hogy a megváltoztatás lehetősége ki legyen zárva (vagy legalábbis észrevétlenül ki legyen zárva, ergo legyen nyomonkövethető). Ezzel szemben az adathordozók kisebb hányada – gyakorlatilag csupán az optikai lemezek egy része – olyan, ami az adatokat megváltoztathatatlan módon tárolja (hiszen egy CD-t vagy DVD-t legfeljebb tönkretenni lehet, az azon lévő adatokat megváltoztatni nem). Vegyük figyelembe, hogy léteznek újraírható lemezek is. Ezeket természetesen ugyanúgy megváltoztatható adathordozóként kell kezelni, mint egy merevlemezt. Éppen ezért a meg nem változtatható adathordozók csomagolásánál a sérülésmentes rögzítésre kell helyezni a hangsúlyt, és kevesebb figyelmet kell fordítani a „hitelesség" megőrzésére, mint a megváltoztatható adathordozók esetén.

Az információs rendszer fogalma alatt gyakorlatilag bármilyen elektronikus, számítástechnikai, digitális (sok hasonlóan csengő, azonban végső soron ugyanazt jelentő fogalmat sorolhatnánk még) eszközt értünk, amely más funkciói mellett elektronikus adatok tárolására is alkalmas (míg az adathordozóknak ugyebár az adatok tárolása az egyetlen funkciója). Ezek kimerítő felsorolása nem lehetséges, és sok esetben csak nézőpont kérdése, mit tekintünk a „rendszer" részének.

Tipikus információs rendszer egy személyi számítógép, amelynek része nem csupán a merevlemez, hanem a processzor, a videókártya, az alaplap, a tápegység

és minden más olyan alkatrész is, amely a számítógépházban van és a rendszer működéséhez szükséges. Nincs különösebb indokunk azonban a rendszer részének tekinteni a monitort, a billentyűzetet és az egeret, még ha ezek egyébként szükségesek is a számítógép használatához. Ugyanakkor egy laptop, egy tablet vagy egy mobiltelefon (amelyek szintén információs rendszerek, hiszen az adattároláson túl más funkciójuk is van) esetén a képernyő is a rendszer részének számít, mivel ezek értelemszerűen egységet képeznek. Mint említettem azonban, a kérdés (mi tekinthető az információs rendszer részének?) inkább filozófiai, hiszen ahogy a személyi számítógép esetén kicserélhető a monitor, ugyanúgy kicserélhető a benne lévő tápegység is, illetve végső soron akár egy telefon képernyőjét is el lehet választani, a gyakorlatban azonban a legtöbbször mégis könnyen belátható józan mérlegelés után, hogy mely részegységekre szükséges kiterjednie a lefoglalásnak, és melyekre nem.

Láthattuk, hogy az eszközök (adathordozók és információs rendszerek) lefoglalásához tartozik a legtöbb törvényi többletkövetelmény, hiszen ez jár a kényszerintézkedés alá vontra nézve legnagyobb hátránnyal (tekintve, hogy ténylegesen is elveszíti az eszköze feletti birtoklás jogát). Eszközt akkor foglalhatunk le, ha az elektronikus adat elkobozható, vagy vagyonelkobzás alá esik (például egy gyermekpornográf felvételeket tartalmazó CD-lemezt el kell kobozni, hiszen már a birtoklása is törvénybe ütközik), tárgyi bizonyítási eszközként jelentősége van (például az informatikai támadást az adott eszközzel követték el), vagy a bizonyítás érdekében az abban tárolt nagy mennyiségű vagy előre nem látható adatok átvizsgálására van szükség (mert mondjuk a helyszínen nem dönthető el, mit kell lemásolni, vagy ez aránytalanul hosszú ideig tartana vagy sok tárhelyet igényelne). Minden más esetben tehát az elektronikus adat másolással (vagy áthelyezéssel) foglalandó le, és ennek során is törekedni kell arra, hogy a kényszerintézkedés csak a feltétlenül szükséges körben és ideig érintse az adatokat [Be. 315. § (4) bekezdése].

A követendő sorrendet ugyanakkor az eszközök lefoglalásán belül is fel kell állítani; nyilvánvalóan kisebb érdeksérelemmel jár és így megelőzi (még ha a törvényszöveg éppen fordítva is említi) az adathordozó lefoglalása a teljes információs rendszer lefoglalását, és legtöbbször elégséges is. Az adatokat az adathordozó tartalmazza, így az egész rendszer lefoglalása csak abban az esetben indokolt, ha az adathordozó a rendszer többi alkatrészével megbonthatatlan egységet képez (a már említett értelemszerű kereteken belül, hiszen abszolút „szétszedhetetlen" rendszer nem létezik). Ezek tipikusan a már említett laptopok, tabletek és telefonok, azonban egy személyi számítógép esetén már indokolt

a helyszínen kiszerelni a merevlemezt, ugyanis ehhez csupán egy csavarhúzóra és 5 perc munkára van szükség, és a legtöbb esetben semmi szükség a számítógép többi alkatrészére. Ugyanakkor egy személyi számítógépet is indokolt lehet „bontatlanul" lefoglalni, ha abban több merevlemez található, és a helyszínen nem tudjuk eldönteni, hogy azok működése milyen módon függ össze (ebben az esetben ugyanis elképzelhető, hogy a szakértő nem lesz képes rekonstruálni az eredeti adatállapotot).

Az említett esetek és példák azért lényegesek, mert a dokumentálás során rögzítenünk kell a jegyzőkönyvben, hogy az adott módszer és terjedelem alkalmazásának mi volt az indoka (mely körülmény merítette ki a törvény által megkövetelt valamely többletkövetelményt). A lefoglalt dolog bizonyító ereje ugyanis két forrásból ered: egyrészről annak igazolásából, hogy a dolog már a lefoglaláskor is azokkal a tulajdonságokkal rendelkezett, amelyekkel bármikor később az eljárás során; másrészről pedig annak igazolásából, hogy ahhoz a nyomozó hatóság törvényesen jutott hozzá. Ugyanis bármennyire is vitathatatlan a bizonyító ereje egy tárgynak, bizonyítékként mégsem vehető figyelembe, ha lefoglalása nem volt törvényes. Mivel mindkét körülményt a jegyzőkönyv igazolja, ezért mindkét körülmény dokumentálására egyforma hangsúlyt kell fektetnünk.

A lefoglalásról szóló jegyzőkönyvben ezért (egyéb magyarázat nélkül) nem szerepelhet az alábbi mondat:

> „A kutatás során a lakáshoz tartozó helyiségben találtunk egy 25 × 40 × 60 cm méretű, fekete színű, Lenovo típusú személyi számítógépet, amit címkével lezártunk és átlátszó bűnjeltasakban eredetben lefoglaltunk (1-es tételszám, fényképfelvételen rögzítve)."

Ehelyett a jegyzőkönyvnek az alábbi kifejtést kell tartalmaznia:

> „A kutatás során a lakáshoz tartozó helyiségben találtunk egy 25 × 40 × 60 cm méretű, fekete színű, Lenovo típusú személyi számítógépet. A számítógépház oldalának eltávolítását követően megállapítottuk, hogy abban 4 db, egyenként 2 terabyte kapacitású merevlemez található (SN432123, SN432134, SN432432, SN432156 sorozatszámokkal). Tekintve, hogy a helyszínen nem volt megállapítható, hogy a merevlemezek logikai egységének megbontása esetén azok adattartalma helyreállítható-e, ezért a gépház összeszerelését követően azt címkével lezártuk, majd átlátszó bűnjeltasakban eredetben lefoglaltuk (1-es tételszám, fényképfelvételen rögzítve)."

Amennyiben a fenti példában csak egy merevlemez lett volna a számítógépben, azonban nem állt volna rendelkezésre hasonló méretű adathordozó a másoláshoz,

vagy az adattartalom nagysága miatt az aránytalanul hosszú ideig tartott volna, úgy mindez a *merevlemez* lefoglalását alapozta volna meg, és a számítógép egészének lefoglalása ebben az esetben nem lett volna megalapozott. Ugyanezen példában viszont, ha az eljárás eddigi adatai alapján megállapítható, hogy az elkövető ezt a számítógépet használja bűncselekmények rendszeres elkövetéséhez – és így az a bűncselekmény eszközeként elkobozható –, úgy megalapozott lett volna a teljes számítógép lefoglalása, függetlenül az abban lévő merevlemezek számától vagy a másolás várható idejétől.

Akár adathordozót, akár információs rendszert foglalunk le, a *jegyzőkönyvnek tartalmaznia kell* az alábbi adatokat is:

- a lefoglalt eszköz (bűnjel) megjelölését;
- a bűnjel mennyiségét, adathordozó esetén kapacitását;
- a bűnjel állapotát, sérüléseit, esetleges hiányosságait (ha már a helyszínen megállapítható, hogy működésképtelen, ennek tényét);
- a bűnjel különös ismertetőjeleit (ha vannak);
- a bűnjel egyedi azonosításra alkalmas jellemzőit, elsősorban sorozatszámát (a merevlemezeken, laptopokon, tableteken általában található sorozatszám, a pendrive-okon és memóriakártyákon esetlegesen, mobiltelefonok esetén az IMEI-számot és a SIM-kártya számát rögzítsük, optikai lemezeken pedig általában nincs sorozatszám, így itt a különös ismertetőjelekre – mint például felirat – kell hagyatkoznunk);
- a bűnjel tárolására vagy csomagolására használt eszközt és a bűnjellel együtt csomagolt tartozékokat (például töltőkábel);
- illetve a már kifejtettek szerint a lefoglalás módszerére és terjedelmére okot adó körülményeket, illetve magát a módszert is.

Emellett értelemszerűen a jegyzőkönyvben fel kell tüntetni azon egyéb adatokat is, amelyeket minden egyéb eljárási cselekménynél (a lefoglalás idejét, helyét és körülményeit, a jelen lévő személyeket, a bűnjel tételszámát és a felvételek készítésének tényét, illetve a bűnjel megőrzésének leendő módját és helyét).

Látható, hogy bár az eszköz lefoglalása jelenti a legnagyobb érdeksérelmet a kényszerintézkedés alá vont számára, a nyomozó hatóság szempontjából a helyszínen mégis ez a legegyszerűbb módszer, hiszen nem kell „bajlódni" az elektronikus adatok lefoglalásánál felmerülő – a következő részben kifejtendő – további teendőkkel, az eszközt elég csupán „becsomagolni egy bűnjelzacskóba és elhozni". Mindazonáltal amit nyerünk a réven, elveszítjük a vámon,

ugyanis az így lefoglalt eszközökről később mindenképpen hiteles mentést kell készítenünk, ha az azon lévő adatokat elemezni szeretnénk.

Márpedig az elektronikus adatokat (akár eszközzel, akár anélkül) általában azért foglaljuk le, hogy azokat később elemezzük. Az adat lefoglalása önmagában ugyanis nem sokat lendít egy nyomozáson, ha nincs mellette egy elemző jelentés vagy szakértői vélemény az ügy szempontjából lényeges körülmények megállapításáról. Az elektronikus adat ebből a szempontból egyáltalán nem olyan, mint egy ellopott tárgy vagy egy elkövetéshez használt szerszám, amelynél már önmagában az a tény is bizonyító erővel bír, hogy a gyanúsítottól foglaltuk le azt.

Éppen ezért a lefoglalt adatokat elemeznünk kell, ehhez azonban nem használhatjuk az eredeti eszközt, hiszen ebben az esetben később semmilyen módon nem tudnánk bizonyítani – a nem újraírható optikai lemezek kivételével –, hogy az elemzés során nem változtattuk meg annak tartalmát. És bár természetesen fel sem merülhet, hogy az eljárás során bármely nyomozó is szándékosan adatokat törölne vagy helyezne el egy lefoglalt eszközön, azonban ezt nem elég egyszerűen tudnunk, hanem bizonyítani kell tudnunk.

Hogy ezt bizonyítani lehessen, a lefoglalás során az eszközt úgy kell csomagolni, hogy a csomag látható megsértése nélkül ahhoz ne legyen lehetőség hozzáférni (erre tökéletesen alkalmasak a rendőrségen használt különböző méretű, öntapadó szájjal rendelkező, átlátszó bűnjelzacskók, amelyeket lezárásukat követően már csak felvágni lehet). A lefoglalt merevlemezeken, laptopokon, telefonokon stb. túl ilyen zsákban kell elhelyezni a lefoglalt személyi számítógépet is, hiszen ha csak a gépház megbontását akadályoznánk meg az erre szolgáló címkével történő leragasztással, attól még a gépházban lévő merevlemezen lévő adatok ugyanúgy észrevétlenül megváltoztathatók lennének, ha valaki perifériákat csatlakoztatna a számítógéphez. Ettől függetlenül a címke felragasztása is indokolt, hiszen ennek megléte bizonyítja, hogy a gépházat nem nyitották fel, és így a benne lévő egyéb (sokszor nagy értékű) alkatrészeket sem cserélhette ki vagy tehette tönkre senki a nyomozó hatóság tagjai közül, azok biztosan a lefoglaláskori állapotnak felelnek meg.

A helyszínen így csomagolt eszköz ezt követően igazságügyi informatikai szakértőhöz (vagy a hiteles másolat elkészítéséhez megfelelő eszközökkel és szakértelemmel bíró rendőri egységhez) kerül, ahol szintén dokumentált módon bontják fel a csomagolást és készítik el – egy rendőrségi adathordozóra – a mentést, amely adattartalma ezután már szabadon vizsgálható az elemzések során. Az elkészült másolat nem lesz bűnjel, az továbbra is az eredetileg

lefoglalt eszköz marad, ami ezt követően visszakerül a bűnjelkamrába vagy – ha már nincs rá szükség – a tulajdonosához.

Mindebből látszik az is, hogy az eszköz lefoglalása esetén annak csomagolása és bűnjelként történő kezelése gyakorlatilag épp ugyanúgy történik, mintha bármilyen más fizikai tárgyat foglalnánk le, annak ellenére is, hogy egyébként nem az eszköz fizikai tulajdonságai, hanem az azon lévő adattartalomnak van jelentősége. Ez utóbbi momentum csupán abban a mozzanatban nyer elismerést, hogy az eszközről később hiteles másolatot készítünk, de egyébként a fennmaradó időben az eszköz éppúgy a bűnjelkamrában pihen, mint bármely más fizikai tárgy, és a lefoglalási jegyzőkönyvben és a bűnjeljegyzéken is a fizikai tulajdonságaira helyezzük a hangsúlyt, nem pedig az azon tárolt adatokra (hiszen ezek jellegével ekkor még nem is lehetünk tisztában).

Éppen ezért az adathordozók és egyéb információs rendszerek csomagolásánál a bűnjelkezelésről szóló rendelet általános – minden egyéb lefoglalt bűnjel csomagolására irányadó – szabályait kell betartani, azaz az eszközt olyan csomagban kell elhelyezni, amely a bűnjelet a károsodástól megóvja, a csomagot pedig úgy kell lezárni, hogy az a csomagolóanyag vagy a zár sérülése nélkül ne legyen felnyitható. A csomagolás burkolatán (illetőleg bűnjelcímkén) fel kell jegyezni a csomag tartalmát, illetve a bűnjel megnevezését, az ügyszámot, a lefoglalás helyét és idejét, az eljáró nyomozó szerv megnevezését, továbbá − ha ismert − a terhelt nevét.

Az eddigieket összegezve tehát elmondhatjuk, hogy amennyiben az elektronikus adatot az adathordozóval vagy az információs rendszerrel együtt foglaljuk le, úgy a dokumentálás, rögzítés, csomagolás és bűnjelkezelés szabályai csak néhány ponton térnek el a bármely más fizikai tárgy lefoglalása során követendő alapvető szabályoktól. A legfontosabb különbséget a lefoglalás módját megalapozó tények jegyzőkönyvben való rögzítésének fontossága, illetve azon körülmény jelenti, hogy a bizonyító erő „kinyerése" érdekében ezeket a bűnjeleket a lefoglalást követően legtöbbször alá kell még vetni egy szakértői adatmásolásnak is.

Elektronikus adatok lefoglalása

Az elektronikus adatok lefoglalásának másik jól elkülöníthető esetköre, ha az adatot önmagában, az adathordozó nélkül foglaljuk le (akár részleges vagy teljes másolással, akár áthelyezéssel). Fontos kiemelni, hogy természetesen ebben

az esetben is használunk adathordozót a lefoglaláshoz (másképp nehezen lenne elképzelhető az adatok „hordozása"), azonban ilyenkor ezt a rendőrség biztosítja. Ennek az elsőre jelentéktelennek tűnő különbségnek az eredményeképpen azonban teljesen máshova kerül a hangsúly a rögzítés, a dokumentálás és a későbbi bűnjelkezelés során is. Ennek oka, hogy a fókusz már a rögzítés kezdetétől az adatra kerül, és az adathordozó szerepe gyakorlatilag teljesen mellékes lesz mindvégig az eljárás során (lehetővé téve akár annak kicserélését is).

Az új büntetőeljárási törvény megalkotásával, illetve a bűnjelkezelésről szóló rendelet ezzel párhuzamos módosításával az elektronikus adatok lefoglalásának és kezelésének szabályozása alkalmassá vált arra, hogy ezeket az eljárási cselekményeket végre valóban a digitális kor támasztotta követelményeknek megfelelő módon hajtsuk végre, szem előtt tartva a kényelem, a hatékonyság és az értelemszerűség szabályait.

Mindazonáltal fontos kiemelni, hogy amennyire alkalmas környezetet teremtett az új szabályozás az elektronikus adatok lefoglalására, annyira alkalmatlan volt ez a környezet a korábbi szabályozás idején, és az ehhez idomuló, hosszú évtizedek alatt kialakuló, ma már felesleges terheket okozó régi gyakorlat sajnos sok helyen még tetten érhető a rendőrségi munkában. Ez részben érthető, hiszen a jogszabályi változásokat természetszerűleg mindig bizonyos késéssel követi a gyakorlat tényleges változása, és míg a jogszabályokat a jogalkotónak, addig a gyakorlatot a joggyakorlóknak – jelen esetben a nyomozóknak – kell alakítania.

Épp ezért a szabályok kifejtése előtt mindenképpen indokolt néhány szóban kitérni arra, hogy milyen körülmények között és hogyan alakult régebben az adatlefoglalások gyakorlata. Egyrészről azért fontos ez, hogy jobban megérthető legyen, melyek azok a hátrányok, amelyek az új szemléletmóddal kiküszöbölhetők, másrészről pedig azért, mert a frissen végzett hallgatók előreláthatóan néhány évig még találkozni fognak a régi gyakorlat nyomaival, amelyeket fel kell tudniuk ismerni ahhoz, hogy legyen elég magabiztosságuk változtatni rajta.

Rögzítsük azt is, hogy az adathordozóról szóló fejtegetéseinkben a rendőrség saját adathordozóját értjük, nem pedig az eljárás alá vont személy eszközét.

A korábbi gyakorlat kialakulásának okai

A korábbi büntetőeljárási törvényünk hatályba lépése idején – az ezredforduló előtt – az elektronikus adatok nyomozásbeli szerepe elhanyagolható volt,

gyakorlatilag nem létezett. Ennek okán természetesen maga a törvény sem tartalmazott az elektronikus adatokra vonatkozó külön rendelkezéseket.

Az évezred elején felgyorsult információtechnológiai forradalmat követően azonban hirtelen lényegesen megnőtt az elektronikus adatok jelentősége a mindennapi életben, és szükségszerűen a nyomozások során is egyre többször merült fel az ilyen adatok bizonyítékként való rögzítésének szükségessége. A kezdeti időkben ez még nem jelentett gondot, hiszen értelemszerűnek tűnt, hogy ha adatot kell lefoglalni, akkor ehhez mindenképpen szükséges az azt tartalmazó eszköz lefoglalása is. A világ digitalizációjával párhuzamosan azonban egyre többször fordultak elő olyan esetek, amikor egy-egy fájl rögzítése céljából kellett lefoglalni egy egész számítógépet, emellett pedig általánosan elterjedtek azok a technikai eszközök is, amelyek lefoglalása az emberek többségének komoly kellemetlenséget okoz (gondoljunk csak a mobiltelefonunkra). Egyre többször vált szembetűnővé tehát a kényszerintézkedés célja és az okozott hátrány közötti aránytalanság, ami magával hozta azt a természetes igényt, hogy a büntetőeljárás során lehetőség legyen csak az adat lefoglalására is.

Mivel a büntetőeljárási törvény rendelkezései kizárólag a fizikai, „kézzel fogható" bizonyítékok kezelésére adtak iránymutatást, a jogalkotó 2014-ben – érzékelve az egyre növekvő igényt – az adat fogalmát is bevezette a törvény rendelkezései közé. A törvény alapvető, fizikai bizonyítékokra szabott struktúrája azonban alapvetően nem változott, és bár az adat fogalmát valóban „behajították" a büntetőeljárásba, az a törvény belső logikájában továbbra is értelmezhetetlen volt.

Ez nemcsak dogmatikai következetlenségekhez, hanem szükségszerűen a már említett félszeg gyakorlat kialakulásához (továbbéléséhez) is vezetett. Egyértelmű volt ugyanis, hogy ha az eljárás alá vont adathordozóját nem foglalja le a rendőrség, akkor az adatok rögzítéséhez saját adathordozót kell biztosítania (mi mást), arra viszont nem adott iránymutatást a törvény, hogy miben térjen el az ilyen adathordozók kezelése azokétól, amelyeket eddig az eljárás elszenvedői foglaltak le.

A nyomozók ezért – hogy a munkájukat a törvény és az ahhoz kapcsolódó rendeletek keretei között tudják értelmezni – arra kényszerültek, hogy a lefoglalt elektronikus adatoknak valamilyen fizikai, kézzel fogható formát adjanak, és ezért az eljárási cselekmények fókuszába az adat helyett a rendőrségi adathordozót helyezték. Azt ugyanis be lehet csomagolni, oda lehet adni a bűnjelkezelőnek, be lehet tenni a bűnjelkamrába, csatolni lehet az aktához, és minden egyéb olyan dolgot is meg lehet vele csinálni, amit egyébként a törvény szerint

a bűnjelekkel meg kell csinálni (míg az elektronikus adatokkal gyakorlatilag nem lehetett mit kezdeni a korábbi jogszabályi környezetben). A gyakorlatban ez azt jelentette, hogy a jegyzőkönyvben az eljáró nyomozók feltüntették, amint valamilyen releváns adatot átmásoltak a rendőrség tulajdonában lévő merevlemezre (pendrive-ra stb.), majd ezen eszköz tulajdonságainak (típus, kapacitás, sorozatszám) leírása mellett lefoglalták magát az *eszközt.*

És bár ez a fajta dokumentálás teljesen megalapozott, amennyiben az adatokat a kényszerintézkedés alá vont tulajdonában lévő adathordozóval együtt foglaljuk le – hiszen ekkor valóban egy fizikai tárgy kerül a rendőrség birtokába, amely egyébiránt olyan tulajdonságokkal rendelkezik (olyan adatokat tartalmaz) amelyek a bizonyítás során jelentőséggel bírnak –, nyilvánvalóvá válik a gyakorlat értelmetlensége akkor, amikor ténylegesen is csupán adatokat foglalunk le, és ehhez az adathordozót a rendőrség biztosítja. Ekkor ugyanis a „lefoglalt bűnjel" egy olyan tárgy lesz, amelynek alapvetően semmi köze sem a cselekményhez, sem pedig a kényszerintézkedés alá vont személyhez (akitől ugye elméletileg lefoglaljuk), hanem csupán hordozóeszközként szolgál a valóban jelentőséggel bíró bizonyíték – az elektronikus adat – tárolásához.

És bár az új – a digitális kor igényeinek megfelelő – szabályozás most már lehetőséget biztosít arra, hogy az elektronikus adatokat valóban a természetüknek megfelelően kezeljük, a valamivel több mint két évtized alatt berögzült gyakorlat az új norma szellemét még nem teljesen vette át, és az elektronikus adat sokszor továbbra is az adathordozóval megbonthatatlan egységként kerül lefoglalásra, az adat helyett pedig az eszköz kerül bűnjelezésre.

A korábbi gyakorlat hátrányai – miért ne alkalmazzuk?

Tágabb nézőpontból szemlélve az adat és az adathordozó ösztönös, azonban a jelen szabályozás mellett már minden szempontból felesleges összekötésével mindenekelőtt nem használjuk ki a digitális tér jelentette nyilvánvaló – és különösebb magyarázatra nem szoruló – előnyöket. Az emberiség pont azért rendezkedett be az utóbbi évtizedekben az adatok digitalizálására, hogy az információkat ne „kézben kelljen átcipelni" egyik helyről a másikra. Ezzel szemben, ha a lefoglalt adatot egy meghatározott, bűnjelként kezelt adathordozó elválaszthatatlan részévé tesszük, azzal *éppen* hogy az adat digitális jellegét szüntetjük meg és redukáljuk a kezelhetőségét egy fizikai tárgy szintjére (hiszen ekkor – az eljárás logikája szerint – már nem lehet többé elszakítani az adathordozótól).

A filozófiai aggályok mellett azonban a büntetőeljárásban konkrét, kézzelfogható hátrányai is vannak annak, ha nem csupán magát az adatot, hanem az azt tartalmazó saját adathordozót is bűnjelként kezeljük. Ennek akkor van jelentősége, ha az elektronikus adatot másolás útján, a saját adathordozója felhasználásával foglalja le a rendőrség.

Ha a lefoglalás a kényszerintézkedés alá vont tulajdonában álló adathordozóra mint fizikai tárgyra is kiterjed, úgy a bűnjelkezelés gyakorlatilag semmilyen módon nem tér el attól, mint amikor bármilyen más tárgyat foglalunk le.

A legjelentősebb ilyen hátrány, hogy az így kezelt – a rendőrség tulajdonában lévő, rendszeres felhasználásra szánt – adathordozó mindaddig kiesik a mindennapi munkából, amíg a lefoglalt adat tárolása szükségtelenné nem válik. Az adat tárolása pedig gyakorlatilag csak egy esetben válhat szükségtelenné: ha megszüntetjük az adat lefoglalását.

Az adat lefoglalásának megszüntetése azonban nem jelenti egyben azt, hogy a bűnjelként bevételezett saját adathordozó automatikusan újra felhasználhatóvá válik más eljárások során. A lefoglaláskor ugyanis csak olyan adathordozó vehető igénybe, amely semmilyen más adatot nem tartalmaz [11/2003. (V. 8.) IM-BM-PM együttes rendelet 67/A. § (2) bekezdése]. Ahhoz pedig, hogy a korábban már használt adathordozó ne tartalmazzon adatot, a lefoglalás megszüntetésén túl a lefoglalt adatok megsemmisítésére is szükség van, ami a büntetőeljárás során csak időigényes folyamat után végezhető el. A lefoglalás megszüntetése esetén a határozat jogerőre emelkedését követően a nyomozó hatóságnak értesítenie kell a jogosultat, akinek ezt követően 30 napja van a dolog átvételére, ennek letelte után pedig a nyomozó hatóságnak újabb 30 nap áll rendelkezésére a bűnjel értékesítése vagy megsemmisítése felől dönteni. Megsemmisítésre akkor kerülhet sor, ha a lefoglalt dolog értéktelen, és a lefoglalás megszüntetését követően arra senki sem tart igényt. A megsemmisítés azonban bizottság jelenlétében kell hogy történjen, amelynek tagja a bűnjelkezelő, az ügyész, valamint a nyomozó hatóság egy képviselője (vagy a bíróság képviselője, ha a megsemmisítést a bíróság rendelte el). A megsemmisítésre bármely alkalmas módon sor kerülhet, ami által a bűnjel használhatatlanná válik (a fizikai bűnjeleket legtöbbször elégetik, az elektronikus adatok azonban nyilvánvalóan az adathordozóról való törléssel semmisítendők meg). Az említett bizottság azonban – célszerűségi okokból – évente csak egy-két alkalommal kerül összehívásra, és egyszerre semmisíti meg az addig felgyűlt bűnjeleket. Egyszerű tárgyak esetén ennek nincs jelentősége, hiszen a bűnjelkamrában történő falnak támasztásuk nem jár

különösebb többletköltséggel, a saját adathordozók viszont erre az időre kiesnek a munkából, és helyettük folyamatosan újakat kell beszerezni.

Szükséges megjegyezni továbbá, hogy az említett folyamat hónapokat vehet igénybe akkor is, ha az adatok lefoglalásának megszüntetéséről még a nyomozati szakban határozunk (mert megszüntettük az eljárást, vagy egyszerűen csak kiderül, hogy a bizonyítás szempontjából a lefoglalt adat mégsem bír jelentőséggel). Ha viszont a nyomozás eredményeképpen az ügyészség vádat is emel, akkor a nyomozás végével természetesen a bizonyítékként szolgáló adatokat is át kell adnunk az ügyészség részére, amelyek lefoglalásának megszüntetéséről csak az ítélethozatal után lehet határozni. Egy büntetőeljárás során ez további hosszú hónapokat – vagy akár éveket is – jelenthet, amelynek folyamán a rendőrség bűnjelként bevételezett és az ügyészségnek átadott adathordozója nem lesz újra felhasználható.

Az adathordozók bűnjelként történő kezelése esetén a technikai eszközöknek a szükségesnél több ideig tartó „újra fel nem használhatósága" azonban csupán a probléma egyik oldalát jelenti. Talán még ennél is nagyobb hátrány, hogy az így kezelt eszközök kapacitásának csupán töredékét használják fel, ugyanis a lefoglalások során jellemzően nem éppen akkora – sőt, általában még megközelítőleg sem akkora – adatmennyiséget rögzítenek, mint amekkora az adott eszköz teljes kapacitása. A gyakorlatban könnyen előfordulhat, hogy egy 1 TB kapacitású merevlemezre csupán 100 GB adatot másolunk, így amíg ezt a merevlemezt bűnjelként kezeljük, úgy a kapacitásának 90%-át semmire sem használjuk.

Könnyen belátható, hogy amennyiben a rendőrség rendelkezésére álló adathordozókat nem külön-külön létező, egyes lefoglalt adatokhoz kötött bűnjelekként kezeljük, hanem úgy tekintünk rájuk, mint az adott szervezeti egység rendelkezésére álló digitális kapacitás összességére, úgy a szervezet által felhasználható tárhely rögtön a többszörösére növekszik anélkül, hogy akár egyetlen új eszközt is beszereztünk volna. Mivel pedig az új szabályozás nemcsak lehetővé tette a másolással lefoglalt elektronikus adatok kezelését, hanem egyben egyértelműen meg is jelölte a másolást mint elsődlegesen alkalmazandó lefoglalási módot (a korábbi büntetőeljárási törvényben ez a sorrend még nem volt egyértelműen lefektetve), így a jövőben a korábbinál nagyobb arányban lesz szüksége a nyomozó hatóságnak a saját adathordozóira a lefoglalásoknál, ezért a megfelelő és hatékony gyakorlat kialakítása és követése különösen fontos.

Az elektronikus adatok lefoglalásának dokumentálása

Elektronikus adatok lefoglalása esetén a jegyzőkönyvben fel kell tüntetni az átmásoláshoz használt adathordozó típusát, gyártási számát, illetve a rajta tárolt adat jellegét és tartalmát. Ha az átmásolás utólag megváltoztatható adathordozóra történik, biztosítani kell az adatok változatlanságát, vagy azt, hogy a megváltoztatás nyomonkövethető legyen [11/2003. (V. 8.) IM-BM-PM együttes rendelet (3) bekezdés]. Az elektronikus adatok lefoglalásának dokumentálásával kapcsolatban a rendelet mindössze ennyi iránymutatást ad.

Az adathordozó típusának és gyártási számának jegyzőkönyvben való rögzítése értelemszerű, azonban ez inkább a belső adminisztrációt és nyomon követést támogatja (magyarul, hogy a lefoglalt adatot a helyszíni intézkedést követően mely adathordozón kell keresnünk), a bizonyítást nem segíti. Nyilvánvaló ugyanis, hogy attól, hogy rögzítettük az adathordozó tulajdonságait, a rajta lévő adatok még bármikor megváltoztathatók. Önmagában az adathordozó tulajdonságainak rögzítése csak abban az esetben segítené a bizonyítást, ha meg nem változtatható adathordozót használnánk, azonban ez a helyszíneken ritkán fordul elő (nyilvánvalóan praktikusabb és egyszerűbb egy pendrive vagy külső merevlemez igénybevétele, még ha ezek megváltoztatható adathordozók is, mint a lefoglalt adatok CD- vagy DVD-lemezekre történő írása, tekintve ezek korlátozott kapacitását és egy külön íróeszköz szükségességét).

Az adat jellegének és tartalmának leírása szintén nem segíti a bizonyítást, a gyakorlatban ugyanis lehetetlen pontosan rekonstruálható módon rögzíteni a jegyzőkönyvben, hogy egy képfájl mit ábrázol, vagy egy mappa mit tartalmaz. Ez csak úgy lenne lehetséges, ha rögzítenénk a jegyzőkönyvben a fájlt alkotó nullák és egyesek pontos sorozatát, azonban ez nyilvánvalóan értelmetlen.

Az elektronikus adatok lefoglalása esetén az adathordozó pontos leírása vagy az adatcsomag méretének megjelölése tehát semmilyen módon nem igazolja azt, hogy a lefoglalt adatot a nyomozó hatóság később nem változtatta meg. A rendelet megfogalmazása szerint azonban, ha az átmásolás utólag megváltoztatható adathordozóra történik (ami a tipikus eset), biztosítani kell az adatok változatlanságát vagy a változtatás nyomonkövethetőségét. Az adatok változatlanságának bizonyítása kevéssé képzelhető el megváltoztatható adathordozók esetén, legfeljebb csak akkor, ha azokat bűnjelként csomagoljuk és kezeljük az eljárás végéig (azonban az elektronikus adatok lefoglalásával pont ezt szeretnénk elkerülni). Ugyanakkor a megváltoztatás nyomonkövethetősége szerencsére nagyon egyszerűen biztosítható, méghozzá a már említett hashkulcs kiszámolásával és rögzítésével.

Az előző fejezetben már többször említett hashkulcs egyszerű és tökéletes módja annak, hogy az adatok változatlanságát bizonyítsuk. A hashkulcsot azonban nem úgy kell elképzelnünk, mint valamiféle pecsétet, ami az adatra helyezve megakadályozza annak megváltoztatását.

A hashkulcs lényege abban áll, hogy bármilyen adatösszesség (legyen az kép, videó, szöveges fájl, vagy akár egy merevlemez egész tartalma minden mappával és almappával együtt) végső soron nem más, mint egyesek és nullák meghatározott – rendkívül hosszú – sorozata. A hashkulcs számítása során nem teszünk mást, minthogy ezt a beláthatatlan hosszúságú sorozatot egy matematikai függvénnyel néhány tucat hosszúságú karaktersorrá redukáljuk, amely így már könynyedén rögzíthető a jegyzőkönyvön.

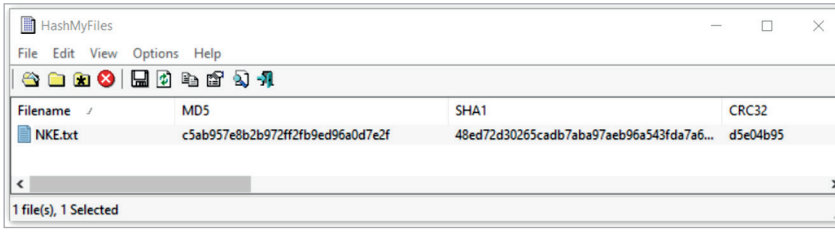
A karaktersor hosszúsága előre meghatározott, az nem függ az adatok jellegétől vagy méretétől; a függvény minden esetben addig „dolgozik", míg a megfelelő mértékig le nem egyszerűsíti az eredeti adattartalmat. Az így kapott karaktersor – a hashkulcs – természetesen nem fejthető vissza, a folyamat csak egyirányú, így egyedül a hashkulcs ismeretéből nem mondható meg, hogy mi volt az eredeti adat. Abban azonban biztosak lehetünk, hogy minden különböző adattartalomnak egyedi a hashkulcsa, mint ahogy két különböző embernek sem lehet egyforma ujjnyomata. És éppúgy, ahogy egy ujjnyomat sem alkalmas arra, hogy abból önmagában „visszafejtsünk" egy teljes embert, arra azonban alkalmas, hogy később össze tudjuk hasonlítani bármely személy ujjnyomatával, és megállapítsuk, hogy az övével éppen egyezik-e.

Ha egy egyszerű matematikai példával szeretnénk a hashkulcs működését szemléltetni, el kell képzelnünk, hogy van egy több ezer tagból álló számsorozatunk. Ha minden számot le szeretnénk másolni, rengeteg munkára és papírra lenne szükségünk, azonban ha összeadjuk a számokat, kapunk egy végeredményt, amely már egyszerűen rögzíthető. Természetesen a végeredményből nem fogjuk tudni megmondani, hogy az eredeti sorozat milyen számokat tartalmazott, viszont az nyilvánvaló, hogy ha bármelyiket is megváltoztatnánk, akkor a végeredmény is megváltozna. Éppen ezért, ha később valaki átad nekünk egy lemásolt számsorozatot, amiről azt állítja, hogy az megegyezik az eredetivel, elég az abban lévő számokat újra összeadnunk ahhoz, hogy ezt ellenőrizzük. Ha a végeredmény megegyezik, tudhatjuk, hogy a két számsorozat is megegyezik. Bár a matematikában minden további nélkül előfordulhat, hogy két különböző számsorozatnak ugyanaz legyen az összege. A hashfüggvények azonban jóval bonyolultabb műveleteket alkalmaznak, amelyek gyakorlatilag kizárják, hogy két különböző adattartalomnak megegyezzen a hashkulcsa.

A büntetőeljárás során épp ez történik; a helyszínen lemásoljuk az adatokat, majd kiszámoljuk és a jegyzőkönyvön rögzítjük a lemásolt adatok hashkulcsát. Ha később az eljárás során a gyanúsított vagy bárki más kétségbe vonja, hogy a rendőrség adathordozóján lévő adatok megegyeznének a helyszínen lefoglalt adatokkal, úgy a nyomozóknak nincs más dolga, mint kiszámolni a tárolt adatok hashkulcsát. Ha ez a hashkulcs megegyezik azzal, amit a helyszínen a jegyzőkönyvben rögzítettek, akkor a tárolt adatok is tökéletesen megegyeznek azzal, amit a helyszínen lemásoltak, és kizárható, hogy azokat bárki is módosította volna.

Látható tehát, hogy elektronikus adatok esetén a változatlanságot kizárólag a hashkulcs feltüntetése bizonyítja, a hashkulcs feltüntetése azonban tökéletesen bizonyítja minden további egyéb technikai adat rögzítése nélkül is (nyilvánvalóan ettől függetlenül a törvény által előírt előbb említett, illetve a lefoglalásoknál egyébként szokásos további általános körülményeket – dátum, hely, mód, érintett személy – ugyanúgy rögzíteni kell.)

A hashkulcsot a bitazonos és forenzikus másolatok elkészítésére szolgáló fizikai eszközök, valamint célszoftverek automatikusan rögzítik, azonban a hashkulcs speciális szakértői eszközök nélkül is bárki által kiszámolható. Éppen ezért amennyiben a helyszínen ezek nem állnak rendelkezésre, és egyszerű másolással (tehát az operációs rendszer másolás funkcióját használva) foglaljuk le az adatokat, úgy a hashkulcsot nekünk kell kiszámolnunk. Ehhez számtalan ingyen használható szoftvert találhatunk, amelyek közül egyszerűen és biztonságosan használható például a HashMyFiles nevű alkalmazás. Ez telepítést nem igényel, és indítást követően elég csupán kiválasztanunk a kérdéses fájlt, a program pedig feltünteti annak különböző hashazonosítóit.



31. ábra: Az NKE.txt nevű, „Nemzeti Közszolgálati Egyetem" tartalmú szöveges fájl különböző hashkulcsai

Forrás: a szerző szerkesztése

A példában az NKE.txt elnevezésű, „Nemzeti Közszolgálati Egyetem” tartalmú szöveges fájl különböző hashkulcsai láthatók. Amennyiben a szövegben bármit változtatnánk, úgy a hashkulcsok is megváltoznának, azonban egy „Nemzeti Közszolgálati Egyetem” tartalmú „txt” fájl hashkulcsai minden esetben a képen látható értékek lesznek, függetlenül attól, hogy ki, mikor és milyen számítógépen hozta létre a fájlt, vagy később milyen másik eszközre másolta azt. Szintén nem változik meg a hashkulcs a fájl átnevezésével, hiszen – hasonlóan a létrehozás idejéhez, helyéhez és a létrehozó személyéhez – a fájlnév is csupán metaadat, és nem tekinthető a fájl adattartalmának.

Több fájl lefoglalása esetén (tekintve, hogy az egyszerűségre törekszünk) érdemes a fájlokból konténerfájlt létrehozni, és csak annak a hashkulcsát rögzíteni. Amennyiben nem rendelkezünk speciális szoftverrel, úgy az operációs rendszer tömörítés funkcióját is használhatjuk erre, amely – függetlenül a tömörített adatok számától és fajtájától – egy fájlba tömöríti a lefoglalandó adatokat.

A hashkulcs megfelelő rögzítése esetén jószerivel teljességgel lényegtelen, hogy a nyomozó hatóság milyen adathordozót használt az eljárási cselekmény során, mint ahogy az is lényegtelen, hogy később az eljárás során hol és mennyi ideig tárolta az adatokat, amennyiben később bármikor újra be tudja mutatni a hashkulcs változatlanságát. A leírtak alapján jól látható a különbség a lefoglalás dokumentálásának helytelen és helyes módja között.

Nem szerepelhet a jegyzőkönyvben az alábbi szöveg:

> „A helyszínen végzett ellenőrzés során a gyanúsított számítógépén 20 db fényképfelvételt azonosítottunk, amelyet egy hatóságunk tulajdonában lévő, Kingston 32 GB típusú, SA231435 sorozatszámú pendrive-ra foglaltunk le.”

Ehelyett a jegyzőkönyvnek a következőket kell tartalmaznia:

> „A helyszínen végzett ellenőrzés során a gyanúsított számítógépén 20 db, a sértettet ábrázoló fényképfelvételt azonosítottunk, amelyeket »kepek.zip« nevű, 897 kb méretű fájlba történő tömörítést követően másolással lefoglaltunk. A lefoglalt adatállomány MD5 hash-azonosítója Ea891660c76f2a7178b2d191f9f082b4. Az adatokat Kingston 32 GB típusú, SA231435 sorozatszámú pendrive-ra másoltuk.”

Az első esetben a lefoglalás fókuszában az eszköz áll, amelyből ezt követően kénytelenek leszünk bűnjelet csinálni, a dokumentáció alapján pedig egyrészről nem egyértelmű a lefoglalás módja, másrészről pedig a későbbiek során nem igazolható az adatok egyezősége (legfeljebb az, hogy a bűnjelkamrába helyezett

pendrive-hoz senki nem fért hozzá, azonban épp azért foglaltuk le az adatokat, hogy azokat később elemezzük, nem pedig azért, hogy a bűnjelkamrában érintetlenül őrizzük).

A helyes dokumentáció ezzel szemben megjelöli a lefoglalás módját (másolás), a lefoglalt adatcsomag egyértelmű azonosítására és a változatlanság igazolására szolgáló hashkulcsot (emellett a későbbi adminisztráció és kezelés megkönnyítése miatt annak nevét és méretét, valamint leíró jelleggel tartalmát), a lefoglaláshoz használt eszköz technikai adatait pedig megjelöli ugyan, de nem köti össze közvetlenül a lefoglalás aktusával.

A lefoglalás mellett a dokumentálás ezen elveinek később a bűnjeljegyzék készítése során is érvényesülnie kell:

Bűnjeljegyzék

A Büntető Törvénykönyvről szóló 2012. évi C. törvény 339. § (1) bekezdésébe ütköző és aszerint minősülő garázdaság vétségének gyanúja miatt **ismeretlen tettes** ellen indított bűnügyben lefoglalt tárgyakról.

A bűnjelek

Sorsz.	Mennyiség	Megnevezés / leírás	Tulajdonos	Megjegyzés
1.	1 db	Kingston 32 GB SA231435 pendrive	KR NNI	20 db fényképfelvétellel
2.	1 db	20 db fényképfelvételt tartalmazó adatállomány (MD5 HASH: Ea891660c76f2a7178 b2d191f9f082b4)	Kovács Béla gyanúsított	Kingston 32 GB SA231435 pendrive-on tárolva

32. ábra: Bűnjeljegyzék
Forrás: a szerző

A követendő gyakorlat szerint a bűnjel tárgyát jelölő részben csak az elektronikus adat szerepel, és csupán megjegyzésként kell feltüntetni annak fizikai hordozó*ját* (míg a helytelen gyakorlat épp az ellenkező irányba mutat). Értelemszerűen a bűnjel tulajdonosa ebben az esetben már a kényszerintézkedéssel érintett személy, nem pedig a hatóság, ami kiküszöböli a korábban jellemző öszvér megoldásokat (saját magunktól történő „lefoglalás" és annak megszüntetése).

Összefoglalva a fentieket tehát, adat lefoglalása esetén a jegyzőkönyvnek a következőket kell tartalmaznia:

- a lefoglalás mely módozatát alkalmaztuk (másolás, áthelyezés vagy teljes másolat készítése);
- a másolást milyen módon hajtottuk végre (bitazonos másolat, forenzikus másolat vagy egyszerű másolás);
- amennyiben a bekapcsolt állapotú eszközön bármilyen interakciót végeztünk, ennek tényét;
- időpontját és eredményét (például a bekapcsolt számítógépen megtekintettük a nyitva lévő böngészőablakokat, és átnéztük az éppen futó programok listáját);
- az alkalmazott írásvédő vagy hardvereszköz pontos megnevezését, verziószámát (ha használtunk ilyet);
- a másolás végrehajtására alkalmazott szoftver elnevezését, verziószámát (ha használtunk ilyet);
- a használt rendőrségi adathordozó azonosításra alkalmas megjelölését (típusát és gyártási számát);
- a tárolt adat jellegét (képfájl, videófájl, szöveges fájlok stb.) és tartalmát (általános leíró jelleggel, például a gyanúsított és a sértett közötti chatbeszélgetés);
- a létrehozott konténerfájl vagy adatösszesség elnevezését, kiterjesztését, méretét és hashkulcsát (a használt – egy vagy akár több – hashalgoritmus megjelölésével);
- az adatmentés kezdő és befejező időpontját.

A lefoglalt elektronikus adatok tárolása a büntetőeljárás során

A fent említett 11/2003. (V. 8.) IM-BM-PM együttes rendelet 2. §-a szerint a lefoglaláskor az adatok csak üres adathordozóra másolhatók. Nincs viszont semmilyen arra vonatkozó előírás, miszerint az adatok később is csak ilyen adathordozón lennének tárolhatók. Sőt, ennek épp ellenkezőjét mondja ki a rendelet, amely szerint a lefoglalt elektronikus adatot adathordozón vagy a hatóság rendelkezése alatt álló tárhelyen kell őrizni (ugyanezen rendelet 7. §-a). Márpedig egy tárhely esetén legalábbis feltételezhető – a tárhelyek alapvető funkciójából adódóan –, hogy már tartalmaz más adatokat is.

Az elektronikus adatok lefoglalására vonatkozó törvényi és rendeleti szabályok nem tartalmaznak ennél részletesebb leírást arra vonatkozóan, hogy a tárhelynek milyen követelményeknek kell megfelelnie, így tárhelynek bármely rendőrségi tulajdonban lévő adathordozó tekinthető, amelyet a nyomozó hatóság ilyenként hasznosít.

Éppen ezért semmi akadálya nincs annak, hogy a lefoglalt adatokat a lefoglaláskor használt adathordozóról – akár más eljárásokban lefoglalt adatokkal együtt – később egy másik adathordozóra másoljuk, kihasználva annak teljes kapacitását, és kiküszöböljük ezzel az adathordozók kevéssé optimális felhasználásából adódó hátrányokat. Ezzel egy időben természetesen az eredeti adathordozóról törölhetők az adatok, így az újból felhasználható egy újabb lefoglalásnál.

A fentiek szerint minden rendelkezésre álló adathordozó két kategória valamelyikébe sorolható: a lefoglaláshoz használt adathordozók, illetve a tárhelyek. A lefoglaláshoz használt adathordozókon az adatok csak a kényszerintézkedéstől a tárhelyig történő átmásolásig kerülnek tárolásra, majd ezt követően azok rögtön újból felhasználhatók. A tárhelyekre ezzel szemben folyamatosan másolhatók az adatok, kihasználva az adathordozó teljes kapacitását.

Az egyik adathordozóról a másikra történő átmásolás nem tesz szükségessé semmilyen újabb interakciót a bűnjelkezelővel. A bűnjelezés lényege, hogy a lefoglalt dolog – ami ebben az esetben maga az adat, nem pedig az adathordozó – a nyomozó hatóságnál nyilvántartásba kerüljön (a bűnjelkezelő „nyilvántartási tételszámot adjon" neki). A nyilvántartási szám viszont az adatra vonatkozik, és annak integritása akkor is megmarad, ha azt később más adathordozóra másoljuk.

Természetesen a nyomonkövethetőség érdekében szükséges, hogy ezt valamilyen formában az aktában is rögzítsük, ehhez azonban egyáltalán nem szükséges új bűnjeljegyzék készítése, elegendő erről egy feljegyzést csatolni az ügyhöz (éppenséggel törvényes lenne az a megoldás is, ha eleve a bűnjeljegyzékre is csak azt vezetnénk fel, hogy a „rendőrség rendelkezésére álló tárhelyen" kerül őrzésre az adat, könnyen belátható azonban, hogy ez a tág megfogalmazás a gyakorlatban egészen biztosan a kelleténél többször vezetne az adatok „elkavarodásához", így az adminisztrációnak legalább az említett szintje mindenképpen indokolt).

Itt is hangsúlyozandó, hogy a feljegyzés – vagy bármilyen egyéb dokumentáció – célja nem a bizonyító erő megtartása, hanem kizárólag a saját magunk számára szolgáló követhetőség biztosítása (hogy tisztában legyünk

vele, melyik adat éppen melyik adathordozón van). A bizonyító erő garantálása egyedül a hashkulccsal történik, és a hashkulcs erre önmagában alkalmas is.

Fontos megjegyezni, hogy az adatoknak a nyomozó felügyelete alatt álló tárhelyen történő tárolása csak abban az esetben lehetséges, ha a bűnjelezést követően a bűnjelkezelő a lefoglalt dolgot – ennek a ténynek a bűnjeljegyzéken való feltüntetése mellett – „visszaadja" a végrehajtó állomány tagjának további megőrzésre, hiszen a rendelet szabályai szerint a bűnjeleket (akkor is, ha elektronikus adatokról van szó) alapvetően a bűnjelkezelőnek kell őriznie a bűnjelkamrában. Adatok bűnjelezése esetén azonban – tekintve, hogy a lefoglalást követően értelemszerűen szinte mindig szükséges azok elemzése – ez előbbi tekinthető a tipikus eljárásnak, és a rendelet szabályai erre lehetőséget is biztosítanak (mint említettem azonban, ezt a tényt fel kell tüntetni a bűnjeljegyzéken).

A nyomozás végeztével világossá válik, hogy mely adatok lefoglalását kell megszüntetni, és mely – bizonyítékként felhasználható – adatokat kell átadni az ügyészségnek. Ekkor szintén döntést lehet hozni arról, hogy – figyelembe véve az adatok méretét – milyen adathordozóra célszerű azokat átmásolni (esetleg CD- vagy DVD-lemezre végleg kiírni), és az aktához csatolni. Ekkor szintén nem lesz jelentősége annak, hogy az átadott adathordozó nem egyezik meg azzal, ami az eredeti lefoglalási jegyzőkönyvben szerepel, hiszen az adatok átmásolása dokumentált, és azok változatlanságát az ügyész is bármikor ellenőrizheti a hashkulcs kiszámolásával és összehasonlításával.

Idővel várhatóan kiépülnek az egyes rendőri szerveknél a lefoglalt adatok központi tárolására szolgáló, a bűnjelkezelő felügyelete alatt álló egységes tárhelyek (úgynevezett elektronikus bűnjelkamrák), valamint várható, hogy az ügyészségeken és bíróságokon is létrehoznak ugyanilyen célú szervereket. Ekkor lehetséges lesz a lefoglalt adatokat a helyszíni intézkedést követően rögtön ezekre a tárhelyekre másolni, illetve az ügyészségnek történő átadáskor egyszerűen csak az ügyészi szerverre átmásolni, azonban a szükséges infrastruktúra kiépítéséig is indokolt a rendelkezésre álló jogszabályi lehetőségeket hatékonyan kihasználni.

Összefoglalás

Látható, hogy az elektronikus adatokat tartalmazó fizikai eszköz lefoglalása, valamint az elektronikus adatok közvetlen lefoglalása merőben más

eljárásrendet és későbbi kezelést von maga után, noha végső soron mindkét esetben elektronikus adatok lefoglalását hajtjuk végre. A két módszer közül az éppen megfelelőt az ügy jellemzőinek és a helyszíni körülményeknek a gondos mérlegelése útján kell kiválasztanunk. Ennek során azonban, valamint ezt követően is figyelemmel kell lennünk a két módszer közötti különbségekre (amelyeket összegezve a 4.táblázat tartalmaz), illetve az ezekből adódó eltérő feladatokra.

4. táblázat: Az adathordozó lefoglalása és az adat másolása vagy áthelyezése

	Adathordozó lefoglalása	**Adat másolása vagy áthelyezése**
Mi válik bűnjellé?	Az adathordozó	Az adat
Mivel bizonyítjuk a változatlanságot?	Az adathordozó tulajdonságainak dokumentálásával és megfelelő csomagolással	A hashkulcs helyszínen történő kiszámolásával és dokumentálásával
Kinek a tulajdona az adathordozó?	Az eljárás alá vont tulajdona	A rendőrség tulajdona
Kicserélhető-e az adathordozó?	Nem cserélhető ki, hiszen az adathordozó maga a bűnjel.	Kicserélhető, hiszen az adat tartalma ugyanaz marad.
Felhasználható-e újra az adathordozó?	Természetesen nem, a lefoglalást követően a bűnjelkamrában kell őriznünk.	Az adatok dokumentált áthelyezését követően újra felhasználható.

Forrás: a szerző szerkesztése