

Nemzeti
Közzszolgálati
Egyetem
Rendészettudományi
Kar

Kiberynyomozói kézikönyv

Szerkesztette
Nagy Zoltán András



LUDOVIKA
EGYETEMI KIADÓ

Kibernetizációs kézikönyv

Kibernyomozói kézikönyv

Szerkesztette
Nagy Zoltán András



LUDOVIKA
EGYETEMI KIADÓ

Budapest, 2022

A kutatás az Innovációs és Technológiai Minisztérium mint Támogató által a TUDFO/51757-1/2019-ITM iktatószámmon meghozott támogatói döntése alapján, az NKFIH-830-8/2019. számú Megállapodásban foglaltak szerint, a 2019. évi Térmaterületi Kiválósági Program céljainak elérése érdekében költségvetési támogatásból valósult meg.

Szerkesztette
Nagy Zoltán András

Szerzők
Gyaraki Réka (2. és 6. fejezet)
Halász Viktor (9. fejezet)
Herédi István (8. fejezet)
Kovács Zoltán (3. és 5. fejezet)
Máté István Zsolt (10. fejezet)
Nagy Tamás (7. fejezet)
Nagy Zoltán András (1. fejezet)
Simon Béla (4. fejezet)

Szakmai lektor
Muha Lajos

Kiadja a Nemzeti Közfoglalati Egyetem
Ludovika Egyetemi Kiadó
A kiadásért felel: Deli Gergely rektor

Székhely: 1083 Budapest, Ludovika tér 2.
Kapcsolat: kiadvanyok@uni-nke.hu

Felelős szerkesztő: Karácsony Fanni
Olvasószerkesztő: Bujdosó Hajnalka
Korrektor: Tomka Eszter
Tördelőszerkesztő: Stubnya Tibor

Nyomdai kivitelezés: Pátia Nyomda Zrt.
Felelős vezető: Orgován Katalin vezérigazgató

DOI: https://doi.org/10.36250/01004_00

ISBN 978-963-531-643-4 (nyomtatott)
ISBN 978-963-531-644-1 (elektronikus PDF) | ISBN 978-963-531-645-8 (ePub)

© A szerkesztő, 2022
© A szerzők, 2022
© A kiadó, 2022

Minden jog védve.

Tartalom

1. Az internet mint nemzetközi tér	9
1.1. Bevezetés	9
1.2. Bűncselekmények az interneten	12
1.3. Új problémák a jogban	21
2. Adatvédelmi ismeretek	27
2.1. Bevezetés	27
2.2. Az adat fogalma	28
2.3. Az adatvédelem fogalma	30
2.4. Az adatvédelem elvei	30
2.5. Az adatok fajtái	32
2.6. Az adatvédelem büntetőjogi háttere	35
2.6.1. A személyes adattal visszaélés bűncselekménye	35
2.7. A közérdekű adattal visszaélés	37
2.7.1. A nemzeti adatvagyon körébe tartozó állami nyilvántartás elleni bűncselekmény	38
2.7.2. Információs rendszer felhasználásával elkövetett csalás	38
2.7.3. Tiltott adatszerzés	40
2.7.4. Információs rendszer vagy adat megsértése	42
3. Az információbiztonság alapjai: a hálózatok	45
3.1. Bevezetés	45
3.2. Az információbiztonság alapjai	46
3.3. Az információbiztonság fogalma	48
3.4. Adatvédelem	53
3.5. Informatikai biztonság	53
3.6. Az elektronikus információs rendszer biztonsága	54
3.7. Kiberbiztonság	54
3.8. Információbiztonság az infokommunikációs rendszerekben	55
3.9. A szolgáltató és a felhasználó feladatai, felelőssége, valamint a kibernyomozó számára releváns információk forrásai	59
3.10. A felhőalapú rendszerek rövid összefoglalása	60
3.10.1. Szolgáltatási modellek (service models)	61
3.10.2. Telepítési modellek (deployment models)	62
3.11. A személyi biztonság a PC/SaaS felhőalapú rendszerekben	63
3.12. A fizikai biztonság a PC/SaaS felhőalapú rendszerekben	64
3.13. A dokumentumbiztonság a PC/SaaS felhőalapú rendszerekben	65
3.14. Az elhárítás a PC/SaaS felhőalapú rendszerekben	65

3.15. Az elektronikus információbiztonság–kiberbiztonság a PC/SaaS felhőalapú rendszerekben	66
3.16. Összefoglalás	67
4. Az infokommunikációs eszközök	69
4.1. Bevezetés	69
4.2. Elméleti alapok	71
4.2.1. Mi a digitális? Mi a bináris? Mi a hexadecimális?	71
4.3. Az adatok tárolása	74
4.4. A személyi számítógépek felépítése	74
4.4.1. A központi vezérlőegység – a processzor	75
4.4.2. Az alaplap	77
4.4.3. A RAM-memória	84
4.4.4. Tápegység	85
4.5. Adattárolás – háttértárak	86
4.5.1. Optikai adattárolók	87
4.5.2. Mágneses adattárolás	88
5. Infokommunikációs hálózatok – hírközlő hálózatok	93
5.1. Bevezetés	93
5.2. A kibernetikusok számára releváns hírközlő hálózatok	94
5.3. Fix (helyhez kötött) telefonhálózatok	96
5.3.1. Fix (helyhez kötött) telefonhálózatok felépítése	96
5.4. A kibernetikusok számára releváns adatok a fix (helyhez kötött) telefonhálózatokban	99
5.5. Telefonalközponti hálózatok	100
5.5.1. Telefonalközponti hálózatok felépítése	100
5.6. A kibernetikusok számára releváns adatok a telefonalközponti hálózatokban	102
5.7. Mobiltelefon-hálózatok	103
5.8. Mobiltelefon-hálózatok felépítése	104
5.8.1. A kibernetikusok számára releváns adatok a mobiltelefon-hálózatokban	117
5.9. Összefoglalás	119
6. Az infokommunikációs hálózatok – az IT-hálózatok	121
6.1. Bevezetés	121
6.2. IT-hálózatok	121
6.2.1. Jellemzők és előnyök	123
6.2.2. Célok	123
6.3. Az internet fogalma	123
6.4. A TCP/IP-protokoll (transmission control protocol/internet protocol)	124
6.4.1. Az IP- (internetprotokoll-) cím	125

6.5. A számítógép-hálózat előnyei és céljai	127
6.5.1. LAN (local area network)	128
6.5.2. Vezeték nélküli hálózatok (WLAN)	129
6.5.3. Személyi hálózatok (PAN)	129
6.5.4. A nagyvárosi hálózatok (MAN)	130
6.5.5. Nagy kiterjedésű hálózatok (WAN)	130
6.5.6. Egyenrangú hálózatok	130
6.5.7. Ügyfélkiszolgáló hálózat	131
6.6. A hálózat alkotóelemei	132
6.6.1. Üzenetek (messages)	133
6.6.2. Eszközök (devices)	133
6.6.3. Átviteli közegek (media)	133
6.6.4. Szolgáltatások (services)	133
6.7. Gyakran használt portok és protokollok	134
6.7.1. TCP és UDP	134
6.8. Hálózati eszközök	135
6.8.1. Modemek	135
6.8.2. Hubok	136
6.8.3. Hidak és kapcsolók	137
6.8.4. Forgalomirányítók és vezetékek nélküli hozzáférési pontok	138
6.8.5. Többfunkciós eszközök	139
6.8.6. Az IP-telefonok	140
6.8.7. Hardveres tűzfal	140
7. A kiberbűncselekmények nyomozása – elméleti alapok	141
7.1. Bevezetés	141
7.2. A kiberbűnözés és a kiberbűncselekmények	142
7.3. A kiberbűncselekmények felderítésének gyakorlati szempontjai	143
7.4. Az elektronikus adat nyomozásban betöltött szerepe	144
7.4.1. Önálló adatrögzítés	146
7.4.2. Adatkérés	147
7.4.3. Lefoglalás	148
7.5. A kutatás, motozás és lefoglalás szerepe a nyomozásban	148
7.6. A kutatás és lefoglalás előkészítése	151
8. Az elektronikus adatokat érintő eljárási cselekmények végrehajtása	155
8.1. Bevezetés	155
8.2. A helyszín szerepe a végrehajtásban	155
8.3. Az eszközök szerepe a végrehajtásban	156
8.4. Elektronikus adatok lefoglalása	158
8.4.1. Az elektronikus adat lefoglalásának módjai	159
8.4.2. Jogszabályban meghatározott más módon történő lefoglalás	165

8.4.3. A hatósági adatmentés készítése	166
8.4.4. Kikapcsolt eszköz	166
8.4.5. Bekapcsolt eszköz	168
9. Az elektronikus adatok rögzítése és az eljárási cselekmények dokumentálása	173
9.1. Bevezetés	173
9.2. Elektronikus adatot tartalmazó fizikai eszközök lefoglalása	174
9.3. Elektronikus adatok lefoglalása	179
9.3.1. A korábbi gyakorlat kialakulásának okai	180
9.3.2. A korábbi gyakorlat hátrányai – miért ne alkalmazzuk?	182
9.3.3. Az elektronikus adatok lefoglalásának dokumentálása	185
9.3.4. A lefoglalt elektronikus adatok tárolása a büntetőeljárás során	190
9.4. Összefoglalás	192
10. Az igazságügyi informatikai szakértő feladatai	195
10.1. Bevezetés	195
10.2. Az elektronikus adatok forrásai	196
10.3. Az elektronikus adatokból megismerhető információk típusai	197
10.4. A kibernetikai és szakértői munka kapcsolata	200
10.4.1. Készenlét	200
10.4.2. Folyamatindítás	202
10.4.3. Megszerzési folyamatok	203
10.5. Az elektronikus adatok vizsgálati modelljei	210
10.6. Statikus elemzés	210
10.6.1. Azonosítás	210
10.6.2. Élő rendszer elemzése	212
10.7. Szakértői vélemény és annak felhasználása	216
10.8. Felhasznált irodalom	217
10.8.1. Szakkönyvek, tanulmányok	217
10.8.2. Jogforrások	221
10.8.3. Internetes források	222

Az internet mint nemzetközi tér

Bevezetés

A számítógépes hálózatok kiépítésének lehetőségét a távíró, telefon, rádió és számítógép integrációja készítette elő. J. C. R. Licklider fogalmazta meg az *intergalaktikus hálózat* koncepcióját, amely hasonlít a mai világhálózathoz.

Az internetet is, mint annyi más tudományos felfedezést, így például a rakétatechnikát, a számítógépet, a mélytengeri búvárruhákat, az éjjellátó távcsöveket, a Global Position Systemet (GPS) vagy a mesterséges esőt, valamint további találmányokat, a katonai kutatás hívta életre.

Történetünk a II. világháború előtti évekre nyúlik vissza; a német ipari technológia szinte minden téren évtizedekkel megelőzte a világ technológiai tudását, a légi járművek, tengeralattjárók, harckocsik, a V–1 robotrepülőgépek és a V–2 rakéták jelezték a német haditechnikai fölényt. Közel kerültek az atombomba előállításához, készen voltak a helyből felszálló repülőgép és a 30–40 kilométerre távolhordó ágyúk tervei, és folytak más irányú fejlesztések is. K. Zuse megalkotta az első programvezérelt számítógépet. (Adalékként a német technikai fejlettséghez megemlíthjük, hogy az 1936-os berlini olimpia megnyitójáról a német televízió színes adásban közvetített. Az USA-ban több mint másfél, a COCOM-lista miatt [is] Magyarországon közel három évtizeddel később kezdődött a színes televíziózás korszaka.)

Érthető, hogy a háborúban a szövetségesek német vagy Németországban dolgozó, dolgozni kényszerített tudóst, szakembert igyekeztek maguknak megszerezni mindenáron, magas fizetéssel, zsarolással, emberrablással és más módon politikai céljaik szerint. Csak az Egyesült Államokba 1800 tisztet, tudóst, hírszerzőt, más specialistát vittek át, ahol új életet kezdhettek.¹ Pregnáns példa Wernher von Braun esete, aki kollégáival a V–2 rakéta gyakorlati megalkotói között volt. Az egykori SS-tiszt az USA-ban a Holdra szállást célul kitűző Apolló-program egyik vezetője, sőt a NASA (*National Aeronautics and Space Administration* – Nemzeti Repülési és Űrhajózási Hivatal) igazgatója volt 1960–1970 között.²

¹ Erich Lichtblau: *The Nazis Next Door: How America Became a Safe Haven for Hitler's Men*. Boston – New York, Houghton Mifflin Harcourt, 2014. 2.

² Bob Ward: *From Nazis to NASA: The Life of Wernher Von Braun*. London, Sutton, 2006. 75–85.

A szovjet Szputnyik-programban együtt dolgozott Konsztantyin Ciolkovszkij és Herman Oberth, aki Von Braun ellenlábasa volt a náci időkben, a V-2 rakéta egyik elméleti kidolgozója.³

A Szputnyik fellövésének második próbája sikeres volt 1957 októberében. Ez a siker azt is üzent a világnak, hogy a Szovjetunió interkontinentális ballisztikus rakéta segítségével gyakorlatilag bárhová bármilyen eszközt eljuttathatott, ami az USA-ban aggodalmat keltett. Válaszként 1958 januárjában létrehozták a NASA-t.

A DARPA (*Defense Advanced Research Projects Agency*, Fejlett Védelmi Kutatási Projektek Ügynöksége), az Egyesült Államok Védelmi Minisztériumának kutatásokért felelős részlege létrehozta az ARPANET-et, egy föld alatti telefonhálózatot, amely a nemzetbiztonsági szempontból fontos intézményeket, később egyetemeket kötötte össze.

1969. szeptember 2-án indult el az ARPANET. 1973-ban a hálózat részévé vált Európa, először a University College of Londont és egy norvég radarállomást kötöttek be.

1982-ben létrejött az EUNET, az első európai internetszolgáltatás Nagy-Britanniában, Hollandiában, Dániában, Svédországban, majd másutt is. Az akkori szocialista országokat természetesen kihagyták az EUNET-ből.

1985–1986-ban az ARPA-Internetet MILNET-re (*military network*) és Internetre (*internet working system*) osztották.

1991-ben a Nemzeti Kutatási Alapítvány (USA) engedélyt adott az internet kereskedelmi célú hasznosítására.

Az internet technikai értelemben „hálózatok hálózata”. A hálózat többretegű. A keresőmotorok által indexált felület a surface web, amely csupán a „jéghegy csúcsa”. Ahhoz, hogy a surface web egy meghatározott tartományát elérhessük, ismernünk kell annak domainnevét. A tartománynevek felépítése hierarchikus, az elemek alá vannak rendelve egy másik elemnek.

Például az rtk.uni-nke.hu tartománynév példáján mutatva:

- .hu – a legmagasabb szintű tartománynév,
- .uni-nke – a második szintű tartománynév (főállomás neve),
- .rtk (alállomás neve).

A legmagasabb szintű tartománynevek (*top level domain* – TLD) tipikusan nemzetközi jelzések:

³ Horvai Ferenc: Ötven éve a világűrben. *Meteor*, 37. (2007), 10. 12.

- a .com (commercial) kereskedelmi tevékenységként;
- a .biz (business) az előbbinél szűkebb körben az üzleti tevékenységként hirdeti magát;
- az .org (organization) különböző szervezetekre;
- a .gov (government) kormányzati szervekre;
- az .edu (education) oktatási tevékenységre, egységekre utal (például egyetemi oldalak jelölése);
- az .info (information), tájékoztatási, informálódási lehetőséget kínál;
- a .net (network) hálózati, operátori tevékenységként hirdeti magát.

Léteznek szponzorált, legmagasabb szintű tartománynevek, így

- a .travel kiterjesztés, amely esetén utazási irodákról, utazási ajánlatokról vagy
- a .museum kiterjesztés esetén múzeumokról, kiállítótermekről nyerhetünk információkat;
- a .jobs kiterjesztés a munkát keresőknek, munkát kínálóknak ad lehetőséget.

Legmagasabb szintű tartománynevek lehetnek országkódok is, ideértve az Európai Unióra történő utalást is, például .hu, .de, .at, .uk vagy az .eu.

A fenntartott legmagasabb szintű tartománynevek:

- a .test elnevezés valamilyen új webes megoldással kísérletező oldalra utal, vagy például
- az .example oldalak webdesigner tevékenységet ígérnek.

A *deep weben* jelszóval, azonosítóval érhetők el a vállalati, intézményi adatbázisok, az e-mail és a közösségi média fiókjainak tartalma és más adatbázisok.

A *dark web* az úgynevezett *Onion Router* rejtett szolgáltatási protokollt használja. A „Tor” szerverek – a *The Onion Router* rövidítése – saját klienssel válnak megismerhetővé. A felhasználók névtelenek maradnak a protokoll által biztosított speciális titkosításoknak köszönhetően.⁴

A dark web ma még „szürke zóna”, megtalálhatók a szólás- és véleményszabadságért küzdők által közzétett tartalmak és a bűnözők „piaca” is.

⁴ Cath Senker: *Cybercrime and the Darknet*. London, Arcturus Publishing Ltd., 2017. 117–140, Lance Henderson: *Tor and the Dark Art of Anonymity*. Amazon Media EU, 2016. 13–98, Jamie Bartlett: *The Dark Net*. London, Windmill Books, 2015. 13–303.

A weboldalak (felső szintű) tartományneve a dark weben mindig .onion.

A bűnözők anonimitásukat – többek között – proxy szervereken keresztül történő aktivitásukkal igyekeznek leplezni.

A ma ismert proxyszerver-típusok:

- anonim public proxy szerver igénybevételével is elrejtőzködhetnek a felhasználók. E szerverek „mögé” rendkívül egyszerűen el lehet bújni. Az anonim public proxynál egy „fokkal” biztonságosabb az úgynevezett
- distorting proxy szerver. Ez a fajta proxy szándékosan hamis IP-t szolgáltat, azaz a proxy szerver helyét is elrejt. A „legbiztonságosabb” mégis a
- high anonymity proxy. Ezek kifelé nem is proxynak mutatják magukat, úgy jelennek meg, mint ha maga a felhasználó hívná a célzott szervert, legfeljebb a TC/IP-szám vagy hamis (nem egyezik meg a földrajzi-matematikai képlettel kiosztott országra), vagy nem létezik.

Jelenleg nehézséget jelent, ha a felhasználó egy publikus router „mögül” lép az internetre, mivel a router nem oszt ki IP-számokat az arra kapcsolódó egyes felhasználók számára. Ebben az esetben maradnak a hagyományos nyomozati megoldások, a felhasználó által hagyott internetes lábnyomok vizsgálata, továbbá a helyszíni webkamerák felvételei, tanúk kikérdezése stb.

Ha valamilyen azonosító szükséges a wifihálózathoz, akkor némileg egyszerűbb a helyzet, de számolhatunk azzal, hogy olyan e-mail-címmel azonosítja magát, amely e-mail-cím olyan ország szerveréről működik, amely ország jellemzően nem partner a nemzetközi nyomozásokban.

A terroristacsoportok⁵ saját biztonságuk miatt, valamint a terrorelhárítók működésének megnehezítése céljából úgynevezett „mozgó IP-címet” (moving IP) használnak, amely a szerverek lokalizálását és azok gyors légi vagy szárazföldi beavatkozással történő likvidálását próbálja ellehetetleníteni.

Bűncselekmények az interneten

A számítógépes hálózatokon elkövethető bűncselekményeket kriminológiai közelítéssel két fő csoportba sorolhatjuk:

⁵ Jeremiah Joliff: *Islamic extremism and cybercrime*. Leipzig, Amazon, 2017; Michael Mealer: *Internet Radicalization: Actual Threat or Phantom Menace*. US Government, Department of Defense, Naval Postgraduate School, Monterey, 2012. 7–63.

- A tartalomközlésben megvalósuló bűncselekmények jellemzően olyan tradicionális deliktumok, amelyek java részben verbálisan, de írásban is elkövethetők.
- Olyan támadások, amelyek célzott szerverekben kárt okoznak. A károk keletkezhetnek a szerverek működésének leállásától kezdve a pénzügyi viszonyok sértésén át a zsarolás miatt fizetett anyagi károkig.

1. A tartalomszolgáltatók weboldalain, a közösségi oldalakon, továbbá a felhasználók saját weboldalain, blogokban, fórumrovatokban, közösségi, torrent-, valamint egyéb fájlcsereoldalakon vagy másutt megjelentetett szöveges, képi közléseit, csatolt audio- vagy videófájljait a világ bármely pontján, bárki láthatja, elolvashatja. A közlések címzettje bármely földrészen bárki lehet, akár egyetlen személy, közösség, avagy bárki ismeretlen.

A 2000-as évektől a felhasználók tartalomfogyasztóból tartalom-előállítókká váltak; az egyéni felhasználók *tartalomközléssel is elkövethetnek* bűncselekményeket. Különösen *tiltott a gyermekpornográf, pedofil felvételek terjesztése, megosztása*.

A tradicionálisan tiltott tartalmak között találjuk a felhasználókat pénzügyi kiadásokra ösztönző, megtevesztő csalásra vagy piramisjátékokra felhívó közléseket. Néhány ismertté vált megtevesztés:

- *Nigériai levelek*, amelyek ismertek 419-es csalásként is (utalva a nigériai büntető törvénykönyvben a 419. §-ban található csalásra), vagy spanyol lottóként, holland lottóként. Ezen esetekben kilátásba helyezett örökség (megnyílt egy nagy örökség, például egy diktátor vagyona), valamint nem is játszott szerencsejátékban, „kiválasztott, szerencsés” IP-cím miatt nyemremény eléréséhez (ügyvédi díjként, pénzügyi költségként stb.) anyagi hozzájárulást kérnek a csalók.
- Ismert eset az is, hogy a *közösségi oldalakon történő ismerkedést követően* az ismerkedést kezdeményező személy meg kívánja látogatni az általa kiválasztott személyt, majd az utazáskor „felmerült” problémára (ellopták a bőröndjét, pénztárcáját, repülőjegyét stb.) hivatkozva pénzt kér átutalással a meglátogatni kívánt személytől. Természetesen a meghívást kezdeményező személy megtevesztő célzattal, anyagi haszonszerzés végett teszi mindezt. Az utazást meg sem kezdte.

Filmek, zeneszámok, könyvek, kották, albumok és más *szerek művei illegálisan fel- és letölthetők* torrentoldalakon, surface weben jellemzően warezoldalakon

pénzért, illetve ingyenesen. Különösen a torrenttechnológia kitalálása óta vált ez tömegessé. Napjaink jelensége a *streaming*, – élő vagy rögzített médiataralom – az interneten keresztül elérhetővé válhat. A közvetítés lehet a rádió- vagy TV-állomás egész napos műsora vagy egy-egy esemény közvetítése, például sportmérkőzés, díjkiosztó ünnepség. A streamelés is lehet jogszerű, ha a rádió- vagy TV-társaság maga sugározza az adását, vagy engedéllyel veszi át a streaminghálózat a műsorát, de lehet jogellenes is, ha például egy fizetős csatorna műsorát vagy egy-egy ott sugárzott eseményt közvetítenek. Jogellenes streamelés esetén nagyon gyakran (másutt tiltott) reklámokat is találunk a program betöltésekor vagy a közvetítés megszakításakor. Az illegális streamingplatformokon vírusok is terjeszthetők.

A torrentezés, az illegális streamelés szerzői jogsértésnek minősül.⁶

A számítástechnika fejlődése tette lehetővé a *3D-s nyomtatás* technológiáját, amely alkalmas bármely, a fizikai térben létező tárgy reprodukálására. A technológiának óriási előnyei vannak: termékek prototípusainak olcsó gyártásától a manuálisan megmunkálhatatlan, létrehozhatatlan, vagy miniatűr (milliméter nagyságú) tárgyak előállításán, a helyszínen történő szervizelés lehetőségén át a gyógyászatban használatos protézisek abszolút pontos elkészítéséig sok minden megoldható. Ugyanakkor e körben az iparjogvédelem körébe tartozó védett tárgyak vagy fegyverek is előállíthatókká váltak. A jogvédett tárgyak „nyomtatásához” szükséges fájlok illegális elérésének tiltása még várat magára.⁷ Reális a félelem, hogy a 3D-s fájlok elérhetősége az interneten ugyanúgy ellenőrizhetetlenné válik, mint jelenleg a digitalizált filmek, zenék le- és feltöltése.

Tartalomközlő, egyben támadó ténykedés a megfélemlítő, megalázó (cyberbullying), a társadalmi csoportot célba vevő (cybermobbing) tartalmak közlése, amely zaklatásnak minősül. A törvény főszabályként a Btk. 222. §-ban⁸ meghatározott *zaklatás* tényállása alapján rendeli büntetni az ilyen cselekményeket. Szintén elérhetők az interneten *becsületsértő, nyíltan rasszista, holokausztagadó* – horribile dictu náci propaganda – közlések is.

⁶ 2012. évi C. törvény a Büntető törvénykönyvről (Btk.) 385. §. Szerzői vagy szerzői jogok megsértése.

⁷ Szabó Csaba: *A 3D nyomtatási technológiával előállított tűzfegyverek biztonságpolitikai kihívásainak vizsgálata a fegyverrendészet aspektusából I–II. Nemzetbiztonsági Szemle*, 5. (2017), 4. 91–124.

⁸ Btk. 222. §. Zaklatás.

A pénzügyi viszonyok tisztaságát, az adórendszert sérti a *pénzmosás*, amelynek megvalósításához, elleplezéséhez tág teret teremt az internet, így például:

- a bűnszervezet (terroristaszervezet) által létrehozott, működtetett névtelen, azonosíthatatlan alapítványok bűncselekményből származó pénzekkel történő „támogatása”, azaz befizetés, ami az alapítványszámlán már legális összegként jelenik meg;
- a bűnszervezet (terroristaszervezet) által létrehozott és működtetett illegális szerencsejátékokban (gambling) való részvétel, ahol a „játékos” mindig csak veszít, jóllehet csak befizet, így a gamblingsszervezet számláján ez már legális összeg;
- szabad munkavállalási oldalakon (freelancer oldalak) történő fizetéssel, ahol akár a munkaadó, akár a munkavállaló ugyanaz a személy is lehet, mivel több oldalon elegendő e-mail-címmel regisztrálnia magát a felhasználónak vagy a bűnszervezet egyik, illetve másik tagjának;
- az online játékokban, ahol nem érvényesülnek piaci árak, szabadon vásárolhatók valós vagy virtuális valutában a játékhöz szükséges vagyontárgyak, vagy a játékokban maradásért „élet”;
- offshore számlák nyitása, azokon pénzek elhelyezése, azokról átutalások kezdeményezése;
- virtuális valutában történő adásvételek, azok átváltása valós valutára stb.

A pénzmosás büntetendő magatartás a Btk. 2012. évi C. törvény a Büntető törvénykönyvről 399. §. Pénzmosás alapján.

Az internet „életben tartója” az e-kereskedelem, színtere az üzleti (*business to business* – B2B), az üzlet és a fogyasztó közötti (*business to consumer* – B2C; *consumer to business* – C2B), valamint a fogyasztók közötti kereskedelemnek (*consumer to consumer* – C2C).⁹

Ez utóbbi üzleti kapcsolatban a felhasználók különböző aukciós, secondhand oldalakon, elektronikus hirdetőtáblákon (*electronic bulletin boards* – más elnevezéssel üzenőfalakon vagy fórumokon), az Airbnb-n és egyéb oldalakon kínálják új vagy használt cikkeiket, szállásaikat, szolgáltatásaikat, vagy kereshetik ezeket.

⁹ Eszes István: *Digitális gazdaság. Az e-kereskedelem marketinges szemmel*. Budapest, Nemzeti Tankönyvkiadó, 2012. 61–126.

E körben különböző visszaélések valósulhatnak meg, ezek egy része bűncselekmény, más része polgári jogi felelősséget vet fel:

- a vevő fizetett, de az eladó nem küldte az árut, vagy
- gyengébb minőségű árut küldött;
- bűncselekményből származó (csempészett, hamis) árut kínált vagy küldött az eladó;
- a szállást bérbe vevő a bérbe adott szálláson kárt okozott, onnan
- valamilyen dolgot eltulajdonított, majd a bérbe vevő rágalmozás miatt feljelentést tehet stb.

Az alábbi bűncselekmények valószínűsíthetők: csalás, rossz minőségű termék forgalomba hozatala, fogyasztók megtévesztése, versenytárs utánzása, rongálás, vagy akár rágalmozás.¹⁰

Létező jelenség a bűnözők egymás között folytatott üzletelése (nevezhetjük Cr2Cr vagy *criminals to criminals* kapcsolatnak) a – fentebb említett – dark weben.

2. A tartalomközlések mellett a technika fejlődésével a társadalomra való veszélyesség korábban nem ismert formáival kerültünk szembe. Feltűnnek a valamennyiünk biztonságát közvetlenül vagy közvetve veszélyeztető visszaélések.

A *hacker* a számítástechnikai rendszerbe történt jogellenes belépését („elektronikus betörés”) követően távoli országok szervereinek működését malware-ekkel, adat- vagy programmanipulációval akadályozhatja, kárt okozhat, titkot sért-het, webtartalmat írhat felül.

Hackingtámadással különösen fenyegetetté válnak az Internet of Things hálózatok, mivel minden, az internethez csatlakoztatott eszközt veszélyeztet egy hackertámadás. Minél több eszköz kapcsolódik a hálózathoz, annál inkább kitett nemcsak az eszköz, hanem az egész hálózat egy ilyen támadásnak. A hálózatba történő jogosulatlan belépéssel károk idézhetők elő, a termelési-logisztikai folyamatok megbénításától az okosotthonokban a riasztó kikapcsolásán, a tüzesetek előidézésén át az önvezető járművek baleseteinek okozásáig (fékrendszer, sebesség manipulálásával).

Napjainkban már tipikus, hogy a felhasználók wifihálózaton keresztül kapcsolódnak az internethez. A szolgáltatás publikus hálózaton (köztereken, középületekben stb.) szabadon, publikus-zárt hálózaton (például szállodában,

¹⁰ Btk. 373. §, 415. §, 417. §, 419. §, 371. §, 226. §.

vendéglátóhelyeken stb.) jelszóval, míg magánhálózaton felhasználónév/jelszó megadásával vehető igénybe. A hacking sajátos megvalósulása a *wardriving*, amikor is az elkövető jogellenesen használja a más által előfizetett (publikus-zárt, illetve magán) és használt wifi-hálózatot.

Hackingtámadás célja lehet az úgynevezett *defacing* is, ami a weboldal eredeti tartalmának jogellenes felülírását jelenti. Tipikusan valamilyen protest támadás eszköze a defacing. Az elkövetők valamilyen politikai, gazdasági vagy más követelés megjelenítését, dezinformáció közlését, konkurencia lejáratását stb. jeleníthetik meg. A defacing is tiltott.¹¹

A *malware-támadás* offline módon, a számítógéphez közvetlenül hozzáférve sem kizárt.

Ennek felderítése könnyebb feladatnak látszik, hiszen az elkövető közvetlenül használja a célzott számítógépet, és ennek lehet tanúja, vagy kamera is rögzítheti ezt a ténykedést. Távolról nem célzottan, számítógépeket (szervereket) is veszélyeztethet malware-támadás. A különböző malware-eket warezekben, egyéb alkalmazásokban, fertőzött bannerekben, csomagolt fájlokban és másutt helyezik el, és azokat a felhasználók telepítik eszközeikre.

Amennyiben a malware-támadás a számítástechnikai rendszer működését jogellenesen akadályozza, úgy az elkövető cselekménye büntetendő.¹²

A *zsarolóvírusok* (WannaCry, Petya, NotPetya, Jaff, CryptoLocker stb.) alkalmazása napjaink legveszélyesebb visszaélése, amely irányulhat a vállalati (ideértve a kisvállalati) szféra ellen és a védekezéssel keveset törődő, felkészületlen felhasználók ellen is. A zsarolás, bár többféle módon történik, célja minden esetben jogosulatlan anyagi ellenszolgáltatás.

A zsarolóvírust a felhasználó – figyelmetlensége, gondatlansága révén – maga tölti le és telepíti eszközére, majd a vírus lehetetlenné teszi a felhasználó számára a fájlljai, könyvtárai elérését azáltal, hogy titkosítja őket. Azok feloldásáért cserébe – tipikusan – valamilyen kriptovalutát követel a zsaroló. A kifizetés követően vagy megérkezik a feloldó kód (*patch* stb.), vagy a zsaroló nem küld, esetleg hamis kódot küld, és folytatódik a zsarolás. A *police malware* lényege, hogy hatóságok nevében küldött levelek zsarolják a felhasználót egy efféle indokolással: „a felhasználó tiltott tartalmat töltött le, vagy szélsőséges csoportokkal tartott kapcsolatot, és ha fizet, akkor nem indul büntetőeljárás”.

¹¹ Btk. 423. § (2) bekezdés b) pont.

¹² Btk. 423. § (1) bekezdés.

Zsarolás végrehajtható terheléses támadással történő fenyegetéssel is, amikor az elkövetők megüzenik, hogy terheléses támadást fognak végrehajtani a szerver ellen, ha nem fizet a szerveret üzemeltető. Ez a cselekmény különösen azon esetekben veszélyes, amikor a szervernek 0–24 órában kell működnie, így különösen a kritikus infrastruktúrák vagy a szerencsejáték-oldalak vannak veszélyben.

A zsarolás, mivel relatív állandósággal jelen van a büntető törvénykönyvekben, a magyar Btk. szerint is büntetendő.¹³

A hálózatot irányító személy *botnet* (a robot network rövidítése) vírusokkal több tíz- (vagy akár száz-) ezer számítógép felett szerezheti meg az uralmat, és ezekkel a zombigépekkel terheléses támadásokat (DoS, DDoS) hajthat végre célzott szerver, szerverek ellen. Botnet létrejöttéhez szükséges valamilyen malware, amely a számítógép, mobiltelefon hálózathoz történő csatlakozásakor kapcsolódik a támadó szerverhez; a botnet gazdája így szerzi meg az uralmat több ezer – mit sem sejtő – felhasználó számítógépe felett. Ilyen malware (úgynevezett *exploit kit*) letölthető valamely weboldalról vagy e-mailhez csatolt fájlból, illetve egy másik programban elrejtett trójai vírusként.

A DoS (*denial of service*) támadás célja szolgáltatásmegtagadás: ebben az esetben egy számítógépet (vagy számítógépeket) használnak TCP- és UDP-csomagokkal. A DDoS (*distributed denial of service*) támadás az, amikor több rendszerről egy rendszert céloznak meg az elkövetők terheléses támadással. A célzott hálózatot több helyről származó csomagokkal bombázzák.

A bűncselekmény alapesetben az információs rendszer vagy adat megsértése.¹⁴ Ha jelentős számú információs rendszert érint, akkor a bűncselekmény minősített esete állapítandó meg,¹⁵ ha közérdekű üzem ellen intézik a terheléses támadást, akkor az még súlyosabban minősül.¹⁶

Terheléses támadás fenyegető kilátásba helyezésével zsarolás is elkövethető. A botnettel spamek is terjeszthetők.

A malware-ek másoknak történő *bitcoinbányászatra* is beállíthatják eszközeinket.

A *kémszoftverek* adatainkat, jelszavainkat, napi ténykedésünket, rutinjainkat rögzíthetik.

¹³ Btk. 367. §.

¹⁴ Btk. 423. § (1) bekezdés.

¹⁵ Btk. 423. § (2) bekezdés.

¹⁶ Btk. 423. § (3) bekezdés.

Az *adathalász* technikák rendkívül szofisztikáltak, ahogy az úgynevezett *social engineering* legkülönbözőbb imposztori formái is színesítik az adathalászat változatosságát. Tipikusak az egy kiválasztott célcsoporttal szembeni adathalász-támadások (*spear phishing* – szigonyozás), a felső vezetőket célba vevő támadás (*executive whaling* – bálnavadászat), a hamis címről függelmi viszonyt színlelő úgynevezett BEC, valamint adathalász e-mailek.

Az internet lehetőségeit a szervezett bűnözés is kihasználja kábítószeres, fegyveres, pornográf és pedofil tartalmak¹⁷ pénzért történő elérésétől a hamis okiratok készítésén át a bérnyilkos bérlésén, a botnetek pénzért történő átadásán át a pénzmosásig. A pénzügyi tranzakciók kriptovalutában zajlanak, ami biztosítja a vásárló és az eladó névtelenségét.¹⁸

A dark weben a bűnözők áru vagy szolgáltatás értékesítőjeként, illetve megrendelőként egyaránt megjelenhetnek.

Az elektronikus kommunikáció jogszerű, vagy annak nem nevezhető *lehallgatására* pedig szinte minden államban rendelkezésre áll a csúcstechnológia.

A bűnözés elterjedtségének okai a *felkészületlen, felelőtlen felhasználók* is, akiknek ismerete sokszor alulmarad az elkövetők tudásához képest. A felhasználók könnyelmű közlései (a vagyoni helyzetükről, tartózkodási helyükről, gyűjtőszennvedélyükről, hobbijukról, szexis szelfik) a bűnözők számára hívószók lehetnek.

A felhasználók naivságát használják ki a *clickjacking-támadók*. Különlegesnek szánt videó- és más tartalom elérhetőségét kínálják, ám az odakattintott meglepetés éri, mivel a felkínált tartalom nem elérhető, azt törölték stb. Találunk

¹⁷ Mezei Kitti – Dornfeld László: Az online gyermekpornográfia elleni küzdelem aktuális kérdései. *Infokommunikáció és Jog*, 14. (2017), 68. 32–37; Mezei Kitti: A szervezett bűnözés az interneten. In Mezei Kitti (szerk.): *A bűnügyi tudományok és az informatika*. Budapest – Pécs, Pécsi Tudományegyetem Állam- és Jogtudományi Kar – MTA Társadalomtudományi Kutatóközpont, 2019a. 125–147; Gyarakai Réka: A kiberbűncselekmények megjelenése és helyzete napjainkban. In Mezei Kitti (szerk.): *A bűnügyi tudományok és az informatika*. Budapest – Pécs, Pécsi Tudományegyetem Állam- és Jogtudományi Kar – MTA Társadalomtudományi Kutatóközpont, 2019a. 83–101.

¹⁸ Gazdag Tibor – Kovács Zoltán: *Felhő alapú új pénzügyi tranzakciós lehetőségek és azok veszélyei*. *Nemzetbiztonsági Szemle*, 2. (2014), 2. 36–57; Halász Viktor: *Kriptovaluták a bűnüldözésben – új kihívások és lehetséges válaszok*. Diplomamunka. NKE NETK, 2018; Simon Béla: A kriptovaluták és a kapcsolódó rendészeti kihívások. In Mezei Kitti (szerk.): *A bűnügyi tudományok és az informatika*. Budapest – Pécs. PTE ÁJK – MTA Társadalomtudományi Kutatóközpont, 2019. 169–186; Miskolczi Barna – Szathmáry Zoltán: *Büntetőjogi kérdések az információ korában*. Budapest, HVG–ORAC, 2018. 146–165. Mezei Kitti: *A kriptovaluták büntető anyagi és eljárásjogi kihívásai*. *Pro Futuro*, 9. (2019b), 1. 79–98.

példát a romantikus csalásokra is, amikor érzelmi kapcsolatkeresés céljával férfo-
köznek a másik személy bizalmába, majd valamilyen ürüggyel (pl. utazáshoz,
gyógykezeléshez) pénzt kérnek.

Az interneten a *kommunikáció* is leplezhető (például végpontok közötti
titkosítással), szöveges, audio- vagy videóchat formájában, számítógépen,
mobileszközön. A *titkos üzenet küldésének* kedvelt formája az úgynevezett
halott e-mail-fiók, ahová a felhasználók belépnek, majd kilépnek anélkül, hogy
az e-mail-fiókot egyetlen adat is elhagyta volna. Ebben az esetben a be- és kilépő
felhasználók a Piszkozat mappában hagyott üzenetekkel kommunikálnak.

A bűnözők is hasznát veszik a világ városait, tájait online mutató webka-
meráknak, vagy a Google Earth (például online) szolgáltatásoknak, amely által
a kiválasztott célpont beazonosítható.

A modern technológia lehetőséget kínál a *bűnüldözés* számára is.¹⁹ Az elkö-
vetők tartózkodási helyének megállapításához például a mobiltelefon helymeg-
határozási szolgáltatása (LoCation Service) révén, vagy mobiltelefon GPS-adatai
alapján. A bankkártyás fizetés helyét, idejét, összegét az ATM-ek, POS-ek,
az imprinterek rögzítik. A gépkocsiban a GPS, a beépített nyomkövető tájékoztat
a gépkocsi földrajzi helyzetéről. A közösségi hálók az elkövető kapcsolati hálóját,
aktuális tartózkodási helyét, esetleg vagyoni helyzetét is mutatják.

A számítógépek TC/IP-szám alapján általában lokalizálhatók, feltéve, ha
a felhasználó nem VPN (virtuális magánhálózat) vagy egyéb proxy szervert,
publikus, publikus-zárt wifihálózat routerét használja, bár ez utóbbi esetben
legalább a router helye meghatározható. Publikus-zárt hálózat használója, ha
személyére adat utal (például szállodai szobaszáma), akkor nyomonkövethető,
ám ha személyére nem utal semmi (például vendéglátóhelyen), akkor az elkövető
nehezebben azonosítható.

Meg kell említenünk azt is, hogy az elkövetők egy része megjelenik az inter-
neten vagy akciója előtt, vagy azt követően mintegy dicsekvésként. Mindenkép-
pen fontos az internet monitorozása, és hogy az extrém tartalmakra, a szélsőséges
elveket, gondolatokat kifejező tartalmakra, azok készítőire figyelmet fordítsunk.
Ezek a közlések ugyanúgy és ugyanott megjelenhetnek, ahol más közlések is
az interneten. Érdemes mesterséges intelligenciát alkalmazni a felderítés ered-
ményessége érdekében.

Az interneten a *felhasználó azonosíthatóságát* segítik az azonos érdeklődési
oldalakon az azonos nickname-ek, a közlések közös tartalmi elemei (szavak,

¹⁹ Simon Béla: *A bűnüldözés előtt álló digitális kihívások*. *Magyar Rendészet*, 17. (2017), 5. 83–104.

szófordulatok, a mondatok hosszúsága stb.), vagy azok alaki jellemzői (írásjelek, smiley-k és más jegyek) segítenek az azonosításban.

Ahogy valós térben a grafológia segítheti a nyomozást, úgy az interneten a felhasználók közléseiből is lehetséges a gyanúsított kör behatárolására, a konkrét személyre vonatkozó személyiségi jegyek megismerése.²⁰

A gyanúsított megismerésére vagy a gyanúsított kör szűkítésére segítséget jelent a közlések elemzése; a fogalmazás precizítása, szavak ismételt használata, írásjelek, emojik, más jelzések beszúrása stb. Az esetlegesen leírt szakkifejezések utalnak a szakmájára, hobbjára. A közlésekből kiderülhet az, hogy mennyire hajlamos szélsőséges véleményekre, azokba mennyire lovalja bele magát, extrovertált vagy introvertált személyiségről van-e szó. A közösségi oldalakon az egyes csoport(ok)hoz csatlakozása, valamint más jellemzők is tükrözik személyiségét vagy éppen érintettségét az adott ügyben. Jellemzően a web2 nyilvánosságát használják fel közléseik közzétételére.

Legalább ennyire fontos a gyanúsítottak, gyanúsított körnek a közösségi oldalakon (még) fellelhető kapcsolatrendszere, amelyből baráti, családi és vagyoni viszonyai megismerhetők.

Rendőrségi eljárás hírére a közösségi oldalakon fellelhető ismerősök általában megszüntetik az ismeretséget.

Új problémák a jogban

Digitális környezetben a hagyományos jogi fogalmak, intézmények, szabályok alkalmazhatósága aggályokat vetett fel.

A valós térben elkövetett bűncselekmények nyomai, bizonyítékai közvetlenül érzékelhetők, láthatók a személyi sérülés nyomai, a megrongált vagyontárgyak, vagy éppen hiányoznak ezen dolgok, mert ellopták, elrabolták azokat stb. Azaz mind a bűncselekmény elkövetési tárgyai, mind a bűncselekményre utaló bizonyítékok közvetlenül érzékelhetők.

Ezzel szemben az elektronikus adatok csak más technikai eszköz alkalmazása révén tehetők láthatóvá, nyerneek értelmet.

Valós térben a sértett általában közvetlenül és azonnal érzékeli az ellene indított támadást, mert például testi sérülést szenvedett, a dolgát megrongálták,

²⁰ Ürmösné Simon Gabriella: *Miben segítik a nyelvi ujjnyomok a nyomozást? Magyar Rendészet*, 19. (2019), 1. 65–75.

ellopták. Virtuális térben a sértett korántsem biztos, hogy érzékeli a támadást. A fájlok, könyvtárak, helyükön vannak, ám a fájlok, könyvtárak tartalmát az elkövetők ellopták (le-, illetve kimásolták). Majd e szöveges, fénykép-, audio-, videótartalmakat (például manipulálva vagy anélkül zsarolási, illetőleg lejáratási célzattal) felhasználják a sértettel szemben. Megjeleníthetik közösségi oldalakon vagy másutt az interneten, ami a sértett számára kedvezőtlen, kínos következményekkel járhat.

A felhasználó azt látja, hogy számítógépe működik, minden funkcióját ellátja, tud böngészni, e-mailt írni, rádiót hallgatni stb. De nem kizárt, hogy a felhasználó számítógépe már zombigép, része egy robot networknek, egy másik személy (a botnet gazdagép felhasználója) átvette az uralmat a sértett számítógépe felett, számítógépe, mobiltelefonja már másnak bányászik bitcoint vagy más virtuális valutát. Az átlag felhasználó legfeljebb azt érzékeli, hogy számítógépe lassabb, nehezebben tölti be a kívánt weboldalt, meg-megszakad az internetes rádió, televízió adása stb., valószínűleg nem is gyanakszik arra, hogy a számítógépe egy terheléses támadásban vesz részt, és éppen egy célzott szerver működésképtelenné tételében használják mint eszközt.

Valós térben az elkövető és a sértett sok esetben *face to face* áll szemben egymással, akár személyleírás is van a támadóról, vagy a sértett a bűncselekmény célzata, motívuma (mint a tényállások esetleges alanyi elemei), személyi, üzleti vagy más kapcsolatai alapján tudja, sejtí, behatárolhatja a támadó kilétét, ami a nyomozásban fontos szempont, segítség.

Virtuális térben az elkövető az esetek nagy részében ismeretlen marad. A személyiséglopás, a jogtalan vagyoni haszonszerzési cél, egy szerver működésképtelenné tétele nem mutat az elkövetők irányába. Természetesen, ha a támadó ismertté szeretné tenni magát, vagy az elkövetés körülményei miatt ismert lesz (például defacing), akkor az elkövető(k) meghatározható(k).

Továbbmenve a valós és a virtuális térben elkövetett bűncselekmények közötti különbség vizsgálatában: a különbség komoly jogi dilemmát is okozhat. A valós térben elkövetett bűncselekmény elkövetési helye általában (*locus delicti*) adott, ami alapján a joghatóság, a hatásköri és az illetékességi szabályok kijelölik az eljáró hatóságokat. A hálózati tevékenységnek több helyen lehet hatása, nemcsak azon a helyen, ahol a felhasználó használta eszközeit, hanem ott is, ahol aktivitásának eredménye megjelenik. A bűncselekmény tényállási elemei sokszor különböző földrajzi helyeken lokalizálhatók.

A joghatóság problémája jól jelzi a büntetőjogi jogharmonizáció vagy akár europaizálódásának²¹ elmaradását, szemben az évszázadok óta a társadalom együttélését, fejlődését biztosító tulajdon-, birtok-, házassági, öröklési, kereskedelmi stb. viszonyokat rendező, precízen kimunkált, utat mutató római joggal.

Ha a számítógépek (szerverek), hálózatok fizikailag elérhetők Magyarországon vagy a zászló-elv szerinti magyar felségterületen, akkor a bizonyítékok megszerzése általában jogilag nem, legfeljebb technikailag okoz nehézséget.

Ha a számítógép (szerver) nem Magyarországon működik, akkor nemzetközi bűnügyi jogsegély igénybevétele a lehetőség.

A nemzetközi bűnügyi jogsegélyről szóló 1996. évi XXXVIII. törvény helyett az Európai Unióba tartozó állam esetében a 2012. évi CLXXX. törvényt kell alkalmazni. A 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezmény (Egyezmény) bűnügyi jogsegély hiányában is megnyitja az egyezményben részes országok számára az együttműködést.

E szerint „a Szerződő Fél megkeresheti a másik Felet, hogy a területén található számítástechnikai rendszer útján tárolt adatokat átvizsgálja vagy azokhoz más hasonló módon férjen hozzá, foglalja le vagy más hasonló módon szerezzé meg, illetőleg adja át”.²²

Izgalmasabb kérdés egy másik állam területén működő számítógépből, számítástechnikai hálózathoz történő bizonyítékszerzés lehetősége. Az Egyezmény szerint bármely ország más szerződő állam beleegyezése nélkül:

- a publikusan elérhető (*open source*) adatokhoz hozzáférhet;
- a másik Szerződő Fél területén tárolt számítástechnikai adathoz hozzáférhet, vagy a területén levő számítástechnikai rendszer útján azt megszerezheti, amennyiben a Fél beszerzi az adat számítástechnikai rendszer útján történő átadására jogszabályban feljogosított személy önkéntes és jogszerű hozzájárulását.

Az első esetben a bármely ország felhasználója által szabadon elérhető adatállomány elérése megengedett, másik esetben az adatállományhoz a feljogosított vagy illetékes személy önkéntes és legális hozzájárulásával szerezhet meg adatokat.

²¹ Nagy Ferenc: Az európai büntetőjog fejlődési irányairól és jogállami alapjairól. *Acta Universitatis Szegediensis Acta, Juridica Et Politica, Tomus LXI.*, (2002). Szeged. 308.

²² Számítástechnikai Bűnözésről szóló Egyezmény 31. pont.

Minden más esetben a kölcsönös jogsegély keretében közreműködnek az adatok összegyűjtésében.²³

A felhőszolgáltatás mint idegen tárhelyek igénybevételeének ötlete már az 1960-as évektől felmerült. Ez esetben a jogi kihívás a tárolt inkriminált adatállomány, különösen előállítója adatainak elérhetősége. Nem lokalizálható, hogy mely országban vannak az inkriminált adatot tároló szerverek, mivel az adatok elérésük biztonsága miatt folyamatosan áramolnak. Kérdés, hogy a tárolás éppen aktuális helyén milyen szabályok hívhatók fel (GDPR, az Adatvédelmi Pajzs vagy más szabályok alkalmazhatók?). Egy megoldás marad: a felhőszolgáltatóhoz fordulni, ahol a választ vagy a kérést teljesíthetik vagy elutasíthatják. A megkeresés sikere függ a felhőszolgáltatást alapító cég bejegyzése helyének jogszabályaitól, jellemzően az USA jogi szabályozásától (például a véleménynyilvánítási szabadság megítélésétől). A felhőszolgáltatók a legsúlyosabb bűncselekmények esetében hajlandók megosztani információikat.

Ugyanakkor, ha a szolgáltató nem adja ki a kért adatokat, gyakorlatilag a „koronabizonyítékokat” tagadják el a hatóságok előtt. A politikai és nagyvállalati érdekek – jelen pillanatban – nehezítik a nemzetközivé vált bűnözés közös üldözését. A jövő a politikai akarat és a nagyvállalati érdekek metszéspontjában dől el.

A joghatóság kérdésében nyilvánvaló problémát jelent, hogy egy kiberbűncselekmény több államot érint (ahol a törvényi tényállás egy-egy eleme megvalósul, egyik országban lenyomják a billentyűt, egy másik országban keletkezik a kár, egy harmadik országbeli elkövető hajtja végre a bűncselekményt, több országban utaztatják, bújtatják a pénzt, közben több országon keresztül zajlik az internetes kapcsolat; és sorolhatnánk azokat az okokat, amelyek a kiberbűncselekmények joghatóságának megállapítását nehezítik).

Ugyanakkor – *horribile dictu* – az is előfordul, hogy bármely okból egyetlen ország sem hajlandó (tud) nyomozást indítani.

A probléma megoldása lehetőségének felvillantásához vissza kell nyúlni egy 1926-os esethez, amely a nemzetközi jogi gondolkodásban paradigmaváltást hozott. Az úgynevezett Lotus-ügyben az Állandó Nemzetközi Bíróság kimondta, hogy nincs a nemzetközi jognak olyan szabálya, amely a lobogó államának kizárólagos joghatóságát állapítaná meg, azaz a területi hatályt kiterjesztő lobogó-elv (*flag principle*) is megtérhet.

²³ Számítástechnikai Bűnözésről szóló Egyezmény 33–34. pont.

A bíróság szerint a nem tevés csak igen kivételes esetben lehet szokásjog-keletkeztető (ügynevezett negatív) gyakorlat.²⁴

A kiberbűncselekmények nyomozásához alapvetőnek kell(ene) tekintenünk az Eurojust (az Európai Unió Büntető Igazságügyi Együttműködési Ügynöksége) 2003-as Éves Jelentését.²⁵ Mivel a számítógépes környezetben nemritkán a bűncselekmények megvalósulásának csupán egyetlen eleme detektálható, értelmezhető a nemzeti hatóságok számára, ezért az eljáró hatóságoknak a joghatóság megállapításához figyelembe kell(ene) venniük:

- azt a helyet, ahol a bűncselekmény legnagyobb részét elkövették;
- azt a helyet, ahol a kár vagy veszteség jelentős része keletkezett;
- a gyanúsított vagy vádlott tartózkodási helyét; valamint
- más joghatóságok számára történő átadásának vagy kiadatásának lehetőségeit;
- a gyanúsított vagy vádlott állampolgárságát vagy lakóhelyét;
- a gyanúsított vagy vádlott jelentős érdekeit;
- a sértettek és tanúk jelentős érdekeit;
- a bizonyítékok elfogadhatóságát vagy
- az esetlegesen előforduló késedelmeket.

A felsoroltak egyben sorrendet teremtenek, tehát a versengés – elméletileg – kizárt, mert bármely fent említett körülmény – figyelembe véve azok sorrendjét – megalapozhatja a joghatóságot.

Az európai ügyészek szervezetének iránymutatásában megfogalmazottakat érdemes volna átültetni a magyar jogba.

A kiberbűnözés elleni harcban nemzetközi és hazai szervezetek is részt vesznek, gyakorlati és tudományos iránymutatásokkal. 2004-ben kezdte meg működését az ENISA (*The European Union Agency for Cybersecurity*), amely praktikus tanácsokkal és megoldásokkal szolgál az EU-tagállamok köz- és magánszektorbeli szereplőinek a hálózat- és információbiztonság területén. Az ENISA kiberbiztonsági gyakorlatokat szervez, segíti a tagállamokat kiberbiztonsági stratégiájuk kidolgozásában. A hálózatbiztonságért felelős nemzetközi és nemzeti szervezetek közötti együttműködés megteremtése is céljai közt szerepel.

²⁴ Dérné Hopoczky Janka: *Univerzális joghatóság pro és kontra. Jogi tanulmányok*, 14. (2010), 2. 339–354.

²⁵ Online: <http://eurojust.europa.eu/doclibrary/corporate/eurojust%20Annual%20Reports/Annual%20Report%202003/Annual-Report-2003-EN.pdf>, 62–64.

1999-ben alapították az Europol-t, majd azon belül 2013-ban a *European Cyber Crime Centre*-t (EC3). Az EC3 által évről évre kiadott IOCTA (*Internet Organised Crime Threat Assessment*) Jelentés ajánlásokat fogalmaz meg a bűnüldöző szervezeteknek, törvényhozóknak annak érdekében, hogy hatékony és összehangolt módon reagálhassanak a számítógépes bűnözésre. A Jelentések az interneten szabadon elérhetők, visszamenőleg is.

A Készenléti Rendőrség Nemzeti Nyomozó Irodánál (KR NNI) a nemzetközi bűnügyi együttműködéssel járó feladatok, jellemzően az információcsere és a közös nyomozások feladatai összpontosulnak. Az NNI együttműködése folyamatos a rendőrséggel, a Nemzeti Adó- és Vámhivatallal, az Országos Katasztrófavédelmi Főigazgatósággal és a titkosszolgálatokkal is.

Adatvédelmi ismeretek

Bevezetés

A 21. századra eljutottunk a 4. ipari forradalom korszakába, amelyben egyre inkább megtapasztalhatjuk, hogy a számítógépre, az informatikai eszközökre minden területen szükségünk van, úgy az oktatásban, a gazdaságban, a kommunikációban, mint a pénzügyi életben. A bűnözés is áttevődött a fizikai térből a kibertérbe, mivel felismerték azt, hogy a felhasználók szívesen osztanak meg információkat, adatokat magukról, aminek következtében egyre több és egyre kevésbé észlelhető bűncselekményt lehet elkövetni.

A felhasználók által megadott adatok – személyes adatok, érzékeny adatok, különleges adatok stb. – védelme nemcsak magának a felhasználónak az érdeke, hanem az egyre szigorodó adatvédelmi és kiberbiztonsággal foglalkozó jogszabályoknak, nemzeti és nemzetközi szervezeteknek is, betartását, betartatását az államok, szervezetek követik figyelemmel és felügyelik is. A folyamatos kontrollnak köszönhetően a biztonságtudatosság, az adataink védelme mindinkább előtérbe került, és komolyabb szankciókkal, egyes esetekben komolyabb pénzbírsággal sújtották a cégeket, szervezeteket.

A kibercselekmények és a kibertámadások egyik célja épp az adatok (akár a személyes adatok, a közérdekű adatok, egészségügyi adatok stb.) megszerzése, felhasználása, azok egyrészt anyagi, másrészt öncélú, akár bosszúból történő ellopása.

Az adatok életünk minden területén körbevesznek minket: az egészségügyben, a bűnüldözésben, a közlekedésben, az értékelőrendszerek működésében, a reklám- és marketingértékesítés területén.

Az egyre terjedő informatikai eszközök és a rajtuk futó alkalmazások használata során számos adat (fényképek, helyadatok, egészségügyi adatok, biometrikus adatok stb.) keletkezik, amelyeket annak használója generál, és amelyeket a különböző kényelmi szolgáltatások (applikációk) révén nyilvánossá tehet, vagy épp amelyekhez a hozzájárulását adja. Ezen kényelmi szolgáltatások legteljesebb mértékű kihasználásáért a szolgáltató vagy az „áruház” nem kér pénzt, csak hozzáférést az adatokhoz, fényképekhez. Ilyenkor a felhasználók hátradólnak, és az ingyenesnek vélt szolgáltatást igyekeznek a legteljesebb mértékben kihasználni, és meggondolatlanul és elolvasás nélkül fogadják el az adatvédelmi beállításokat. Pedig nincs semmi sem ingyen. A szolgáltatóknak, a cégeknek az adatainkkal fizetünk.

A következőkben az adat fogalmával, a fent is leírt adatfajtákkal, azok védelmével, törvényi és büntetőjogi hátterével fogunk foglalkozni.

Magyarországon több törvény is tartalmazza az adatokkal és az adatvédelemmel kapcsolatos szabályokat. A kiberbűncselekmények szempontjából kiemelt a 2018. évi XXXVIII. törvény az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvénynek az Európai Unió adatvédelmi reformjával összefüggő módosításáról, valamint más kapcsolódó törvények módosításáról, a 2009. évi CLV. törvény a minősített adatok védelméről, a 2013. évi L. törvény az állami és önkormányzati szervek információbiztonságáról.

Az adat fogalma

Az adat fogalmát a 2013. évi L. törvény (Ibtv.)²⁶ értelmező rendelkezése tartalmazza. Ennek alapján az adat az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas.

A számítástechnikában az adat fogalmára kétféle meghatározás létezik. Az egyik esetben az adat a számítógépes állományok meghatározott része (minden, ami nem program); vagy pedig mindaz, amivel a számítógépek működésük során foglalkoznak (ki- és bemeneti, tárolt, feldolgozott, továbbított, megsemmisített adat).²⁷

Az adatot mint fogalmat sokszor tévesen azonosítják vagy szinonimaként használják az információ fogalmával.

Az információ meghatározására többféle – tartalmában egymást átfedő – fogalmat használnak:

Az informatikai biztonság kézikönyve alapján:

„bizonyos tényekről, tárgyokról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságot csökkent vagy szünteti meg”.²⁸

²⁶ 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

²⁷ Muha Lajos: Fogalmak és definíciók. In Muha Lajos (szerk.): *Az informatikai biztonság kézikönyve*. Budapest, Verlag Dashöfer Szakkiadó, 2004.

²⁸ Vö. Muha (2004) i. m.

A Rendészettudományi szaklexikon szerint:

„valamely személyre, ügyre vagy dologra vonatkozó olyan tájékoztatás, felvilágosítás, értesülés, hír, amely a címzettet választásra, döntésre, meghatározott cselekvésre, magatartásra, gondolkodásra készteti. Információ: értesülés, hír, üzenet, tájékoztatás, amely egyben az informatika alapfogalma.”²⁹

Az Ibtv. akként fogalmaz, hogy

„információ: bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti.”

Az adatvédelem során a két legfontosabb jogszabályról mindenképpen szót ejtünk a fejezetben, a minősített adatokkal kapcsolatos szabályozást ugyanakkor a büntetőjogi alfejezetben csak említjük, hiszen arról részletesen fognak tanulni a bűnügyi szolgálati ismeretek és az adat- és titokvédelmi tantárgyak keretei között.

Az Európai Parlament és a Tanács (EU) 2016/679. rendelete, a GDPR (*General Data Protection Regulation*) (a továbbiakban: Rendelet) az európai általános adatvédelmi rendelet, amely 2018. május 25-étől lépett életbe, és amelynek következtében az Infotv. is több módosításon ment keresztül annak érdekében, hogy a személyes adatok védelme a legteljesebb mértékben érvényre jusson.

A Rendelet célja:

„A természetes személyek személyes adataik kezelésével összefüggő védelméhez kapcsolódó elvek és szabályok a természetes személyek állampolgárságától és lakóhelyétől függetlenül tiszteletben tartják e természetes személyek alapvető jogait és szabadságait, különösen, ami a személyes adataik védelméhez való jogukat illeti. Ez hozzájárul a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség, valamint a gazdasági unió megteremtéséhez, a gazdasági és társadalmi fejlődéshez, a belső piacon belüli gazdaságok erősödéséhez és konvergenciájához, valamint a természetes személyek jólétéhez.”³⁰

²⁹ Boda József (főszerk.): *Rendészettudományi szaklexikon*. Budapest, Ludovika Egyetemi Kiadó, 2019.

³⁰ Európai Parlament és a Tanács (EU) 2016/679. rendelete. Bevezető, 2. pont.

Az Infotv. 1. §-ában kötelezettségként határozza meg, hogy „a természetes személyek magánszféráját az adatkezelők tiszteletben tartásák, valamint a közügyek átláthatósága a közérdekű és a közérdekből nyilvános adatok megismeréséhez és terjesztéséhez fűződő jog érvényesítésével megvalósuljon”.

Az adatvédelem fogalma

Az adatvédelem (*data protection*) a személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége.³¹

A kibercbncselekmények sokszor az informatikai rendszerek ellen irányulnak, az azokban tárolt adatok elleni támadásokban nyilvánulnak meg, amelyeket a szaknyelv *incidensnek* nevez. Az adatvédelmi incidens fogalmát az Infotv. szabályozza. Ennek alapján az az adatbiztonság olyan sérelme, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisülését, elvesztését, módosulását, jogosulatlan továbbítását vagy nyilvánosságra hozatalát, vagy az azokhoz való jogosulatlan hozzáférést eredményezi.³²

Az adatvédelem elvei

A GDPR 2. §-ában a következő alapelveket nevezi meg:

- célhoz kötöttség,
- jogszerűség, tisztességes eljárás, átláthatóság,
- adattakarékosság,
- pontosság,
- helyesbítéshez való jog,
- korlátozott tárolhatóság,
- integritás és bizalmas jelleg,
- elszámoltathatóság.

A *célhoz kötöttség* elve az Infotv.-ben található, és alkotmányossági alapelv is, amely alapján a személyes adat kizárólag meghatározott célból, a jog gyakorlása

³¹ Nemzeti Adatvédelmi és Információszabadság Hatóság: *Adatvédelmi Értelmező Szótár* (é. n.).

³² Infotv. 3. § 26. pont.

és kötelezettség teljesítése érdekében kezelhető. Az adatvédelmi munkacsoport 2013. április 2-ai állásfoglalása szerint a személyes adatok kezelése csak meghatározott, egyértelmű és törvényes célból történhet, illetve az adatok további kezelése nem végezhető e célokkal összeférhetetlen módon.

Az elv kimondja tehát, hogy személyes adatok csak abban az esetben kezelhetők, ha az adatkezelés célját *egyéb eszközzel észszerű módon nem lehetséges elérni*, vagyis a cél elérése érdekében ténylegesen szükség van az adatok kezelésére. Az adatkezelőnek haladéktalanul törölni kell az érintett személyes adatait, amennyiben az adatkezelés célja megszűnt, vagy az adatok további kezelése már nem szükséges az adatkezelés céljának megvalósulásához (ennek ágazatban való gyakorlati megvalósulása kérdéses). Az adatkezelés során csak a cél megvalósulásához szükséges mennyiségben és mértékben kezelhetők az adatok.

A személyes adatok gyűjtése, eredeti céljától eltérő, egyéb célból történő kezelése csak akkor megengedett, amennyiben *az adatkezelés összeegyeztethető az adatkezelés eredeti céljaival*, amelyekre a személyes adatokat eredetileg gyűjtötték. Ebben az esetben nincs szükség attól a jogalaptól eltérő, külön jogalapra, mint amely lehetővé tette a személyes adatok gyűjtését. Ez az elv megvalósul, ha ugyanannak az ellátott személynek a segítségben kitűzött célját próbáljuk elérni, s ehhez más-más formában, de folyamatosan használjuk a személyes adatait.

A *jogszerűség* követelménye értelmében annak érdekében, hogy a személyes adatok kezelése jogszerű legyen, annak az érintett hozzájárulásán kell alapulnia, vagy valamely egyéb jogszerű, jogszabály által megállapított – akár e rendeletben, akár más, az e rendeletben említettek szerinti uniós vagy tagállami jogban foglalt – alappal kell rendelkeznie, ideértve az adatkezelőre vonatkozó jogi kötelezettségeknek való megfelelés szükségességét, az érintett által kötött esetleges szerződés teljesítését, illetve az érintett által kért, a szerződéskötést megelőzően megteendő lépéseket.

A jogszerűség elve mellett az *átláthatóság elve* szerint a természetes személyek számára átláthatónak kell lennie annak, hogy a rájuk vonatkozó személyes adataikat hogyan gyűjtik, használják fel, hogyan tekintenek bele, vagy milyen egyéb módon kezelik, valamint annak, hogy a személyes adatokat milyen mértékben kezelik, vagy fogják kezelni. Az átláthatóság elve megköveteli, hogy a személyes adatok kezelésével összefüggő tájékoztatás, illetve kommunikáció könnyen hozzáférhető és közérthető legyen, valamint az átláthatóság követelménye, hogy annak világosnak és egyszerű nyelvezettel fogalmazottnak kell lennie.

Ez az elv vonatkozik különösen az érintetteknek az adatkezelő kilétéről és az adatkezelés céljáról való tájékoztatására, valamint az azt célzó további

tájékoztatásra, hogy biztosított legyen az érintett személyes adatainak *tisztességes és átlátható* kezelése, továbbá arra a tájékoztatásra, hogy az érintetteknek jogukban áll megerősítést és tájékoztatást kapni a róluk kezelt adatokról.

Az *adattakarékosság* elve szerint a kezelt adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell hogy legyenek, és a kezelt adatok körét és a kezelés mértékét pedig a célhoz szükséges minimumra kell korlátozni.

A *pontosság* követelménye szerint a személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük; minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék.

A *helyesbítéshez való jog*. Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat. Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését.

Az *integritás és a bizalmasság* elve azt jelenti, hogy a személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága. A személyes adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve. A személyes adatokat úgy kell kezelni, hogy azoknak a megfelelő szintű biztonsága és bizalmas kezelése során megakadályozzák a személyes adatokhoz és a személyes adatok kezeléséhez használt eszközökhöz való jogosulatlan hozzáférést, illetve azok jogosulatlan felhasználását.

Az *elszámoltathatóság* elvének követelménye szerint az adatkezelő alakítsa ki azokat a belső szabályokat, folyamatokat, mechanizmusokat, amelyek a rendeltből fakadó kötelezettségek teljesítéséhez szükségesek, másrészt képes legyen a megfelelés bemutatására.

Az adatok fajtái

Amikor adatokról beszélünk, a jobb megértés miatt célszerű megnevezni, hogy milyen típusú adatra gondolunk, hiszen az önmagában tág fogalom.

Az Európai Unió Adatvédelmi Rendelet alapján személyes adatnak nevezzük minden olyan információt, amely valamely *azonosított vagy azonosítható élő személlyel* kapcsolatos. Mindazon információk, amelyek összegyűjtése

egy bizonyos személy azonosításához vezethet, ugyancsak személyes adatnak minősülnek.³³

A *személyes adat* fogalmát az Infotv. csak egy mondattal határozza meg: az érintettre vonatkozó bármely információ.³⁴

A személyes adat fogalmának használatakor szükséges megemlíteni azokat az eseteket, amikor bár maga a személy nincs pontosan megnevezve, mégis a róla gyűjtött adatokból személyére következtetni lehet, hasonlóan a *Ki vagyok én?* elnevezésű társasjátékhoz.

Az azonosításra alkalmatlanná tett, titkosított vagy *álnevesített* személyes adatok, amelyek felhasználhatók egy személy újraazonosítására, személyes adatnak minősülnek, és az általános adatvédelmi rendelet hatálya alá tartoznak.

Az olyan személyes adatok, amelyeket olyan módon *anonimizáltak*, amelynek következtében az érintett nem, vagy többé nem azonosítható, nem tekinthetők többé személyes adatnak. Az adatok valódi anonimizálásához az anonimizálásnak visszafordíthatatlannak kell lennie.

Az általános adatvédelmi rendelet a személyes adatokat *az adatok kezelése során használt technológiától függetlenül* védi – a jogszabály „technológiasemleges”, és egyaránt vonatkozik az automatizált és manuális kezelésre, feltéve, hogy az adatokat kritériumok szerint rendszerezik (például betűrendben). Nem számít az sem, hogy az adatokat milyen módon tárolják: IT-rendszerben, videokamerás megfigyelőrendszerben vagy papíron; ezen esetek mindegyikére vonatkoznak az általános adatvédelmi rendelet személyes adatok védelmére vonatkozó követelményei.

Személyes adatoknak minősülnek:

- vezetéknév, családnév,
- lakcím,
- e-mail-cím, amely például annak használójára visszavezethető,
- személyazonosító igazolvány száma,
- helymeghatározásra vonatkozó adatok (GPS-adatok, közösségi oldalakon a tartózkodási hely megjelölése, a különböző alkalmazásokból gyűjtött helyadatok stb.),
- IP-cím,
- süti-azonosító (cookie),
- a telefon hirdetési azonosítója,

³³ GDPR ide vonatkozó számos rendelkezése.

³⁴ Infotv. Értelmező rendelkezések 3. § 2. pontja.

- a személy egyedi azonosítását lehetővé tevő, kórház vagy orvos által tárolt adatok.
- *A különleges adat* a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.
- *A genetikai adat* egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az adott természetes személyből vett biológiai minta elemzéséből ered.
- *Biometrikus adat* az, ami egy természetes személy fizikai, fiziológiai vagy viselkedési jellemzőire vonatkozó olyan, sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, mint például az arckép vagy a daktiloszkópiai adat.
- *Az egészségügyi adat* egy természetes személy testi vagy szellemi egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról.
- *Bűnügyi személyes adatnak* minősül a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat.

Az Európai Adatvédelmi Rendelet alapján a fent felsorolt típusokon kívül *különleges adatnak* minősül még:

- faji vagy etnikai hovatartozásra, a politikai véleményre, a vallási vagy világnézeti meggyőződésre utaló személyes adatok;
- szakszervezeti tagság;
- a nemi életre vagy a nemi irányultságra vonatkozó személyes adatok.

A személyes adat mellett sokszor lehet hallani a különböző adatigénylések kapcsán a közérdekű adat fogalmát. Közérdekű adatnak minősül az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó, vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat.

Az utolsóként meghatározott adatfajta a közérdekből nyilvános adat, ami a közérdekű adat fogalma alá nem tartozó minden olyan adatot jelenti, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli.

Az adatvédelem büntetőjogi háttere

Ahogy felületesen is, de érintettük, az Infotv., illetve az Európai Adatvédelmi Rendelet szabályainak megszegése esetén az azt sértő vállalkozások, szervezetek, weboldal-üzemeltetők ellen a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) bírságot szabhat ki. Ugyanakkor a pénzbírság nem mindig elegendő és lehetséges az adatok nem megfelelő felhasználásával, esetleg az azokkal való jogellenes visszaéléssel szemben. Lássuk a legfontosabb tényállásokat és azok vázlatos elemzését!

A személyes adattal visszaélés bűncselekménye

„Aki a személyes adatok védelméről vagy kezeléséről szóló törvényi vagy az Európai Unió kötelező jogi aktusában meghatározott rendelkezések megszegésével haszonszerzési célból vagy jelentős érdeksérelmet okozva

- a) jogosulatlanul vagy a céltól eltérően személyes adatot kezel, vagy
- b) az adatok biztonságát szolgáló intézkedést elmulasztja [...].”³⁵

³⁵ Btk. 219. §.

Az elkövetési (tevékenységi) tárgy a személyes adat, valamint a különleges adat.

A bűncselekmény sértettje az a természetes személy, akire az adatok vonatkoznak.

Az elkövetési (tevékenységi) magatartásai:

Adatkezelés, vagyis az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége (például gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, lekérdezése stb.) A büntetőjogi szabályozásnál ugyanazok az elvek érvényesülnek, amelyeket már fentebb is ismertettünk. Személyes adatot kezelni csak meghatározott célból, jog gyakorlása, illetve kötelezettség teljesítése érdekében lehet, míg a különleges adat esetén (fogalmát lásd fentebb) szükséges, hogy annak kezeléséhez az érintett hozzájáruljon. Fontos megjegyezni, hogy írásbeli hozzájárulás nélkül a faji eredetre, a nemzetiséghez való tartozásra, politikai véleményre, pártállásra, szexuális beállítottságra, vallásos vagy egyéb világnézeti meggyőződésre, érdekképviselési tagságra vonatkozó személyes adat kezelése akkor lehetséges, ha az törvényben kihirdetett nemzetközi szerződés végrehajtásához szükséges, vagy ha azt az Alaptörvényben biztosított alapvető jog érvényesítése, bűncselekmény megelőzése, üldözése érdekében vagy nemzetbiztonsági, illetve honvédelmi érdekből törvény elrendeli.

A bűncselekmény tettese (aktív alanya) bárki lehet, aki személyes adatot kezel, feldolgoz, akinek törvényben írt kötelessége a személyes adatok biztonságáról történő gondoskodás. Ennek során köteles megtenni azokat a technikai és szervezési lépéseket, intézkedéseket, figyelemmel lennie azokra a szabályokra, amelyeket az Információs és önrendelkezési jogról szóló törvényben, valamint az adat- és titokvédelmi törvényben rögzítettek, így különösen az adat tárolására, hozzáférésére, megosztására, nyilvánosságra hozására, törlésére, úgyszintén az adat megváltoztatására, véletlen megsemmisülésére vagy sérülésére, a hozzáférhetetlenné tétele megakadályozására.

Az adatról az érintett kérelmére az adatkezelő köteles tájékoztatást adni. A kérelem vonatkozik a kezelt adatokra, a megbízott adatfeldolgozó által feldolgozott adatokra, azok forrására, az adatkezelés céljára, jogalapjára, időtartamára, az adatfeldolgozó nevére, címére, az adatkezeléssel összefüggő tevékenységre, az adattovábbítás jogalapjára és címzettjére.

Egyes esetekben az adatkezelő törvényi felhatalmazás alapján megtagadhatja a tájékoztatást. Ilyen eset az állam külső vagy belső biztonságának megőrzése, bűnüldözési, bűnfelderítési és bűnmegelőzési célból.

Az adatkezelő 30 napon belül köteles tájékoztatást adni közérthetően az adatkezelés megtagadásáról, különben bűncselekményt követ el.

A közérdekű adattal visszaélés

„Aki a közérdekű adatok nyilvánosságáról szóló törvényi rendelkezések megszegésével

- a) közérdekű adatot az adatigénylő elől eltitkol, vagy azt követően, hogy a bíróság jogerősen a közérdekű adat közlésére kötelezte, tájékoztatási kötelezettségének nem tesz eleget,
- b) közérdekű adatot hozzáférhetetlenné tesz vagy meghamisít, illetve
- c) hamis vagy hamisított közérdekű adatot hozzáférhetővé vagy közzé tesz [...]”³⁶

A bűncselekmény elkövetési (tevékenységi) tárgya: közérdekű adat. Fogalmát lásd fentebb.

A bűncselekmény elkövetési (tevékenységi) magatartásai:

A közérdekű adat eltitkolása az adatigénylő elől jogerős bírósági kötelezés előtt vagy azt követően.

Az állami vagy helyi önkormányzati feladatot vagy közfeladatot ellátó szervnek vagy személynek lehetővé kell tennie, hogy a szervezetre vonatkozó vagy az általuk kezelt adatot bárki megismerhesse, kivéve, ha az a minősített adat védelméről szóló törvényben meghatározottak szerint minősített adat. Kivételt képeznek még a megismerési kötelezettség alól a személyes adatoknál leírt esetek és a pénzügyi vagy devizapolitikai érdekek, a külügyi kapcsolatok, a nemzetközi szervezetekre vonatkozó kapcsolatok, a szellemi tulajdonhoz fűződő jog védelmének körébe eső adatok.

A c) pontban említett hozzáférhetetlenné tétel a közérdekű adat elrejtését és megsemmisítését jelenti.

³⁶ Btk. 220. §.

A nemzeti adatvagyon körébe tartozó állami nyilvántartás elleni bűncselekmény

„(1) Aki a nemzeti adatvagyon körébe tartozó állami nyilvántartásban kezelt adatot az adatkezelő részére hozzáférhetetlenné teszi, ha más bűncselekmény nem valósul meg, büntetett miatt három évig terjedő szabadságvesztéssel büntetendő.”³⁷

A bűncselekmény elkövetési (tevékenységi) tárgya: a nemzeti adatvagyon védelméről szóló 2010. évi CLVII. törvény 1. § (1) bekezdése szerint a nemzeti adatvagyon a „közfeladatot ellátó szervek által kezelt közérdekű adatok, személyes adatok és közérdekből nyilvános adatok összessége”.

A bűncselekmény elkövetési (tevékenységi) magatartása: a nemzeti adatvagyon körébe tartozó adat hozzáférhetetlenné tétele, amennyiben azt az adatkezelője számára teszi hozzáférhetetlenné.

Ugyanakkor – mivel ez egy szubszidiárius tényállás, így – annak elkövetése csak akkor valósul meg, ha az elkövetési magatartás nem valósít meg másik bűncselekményt. Azaz, amennyiben az elkövetése kifejezetten a kiberterrorizmus vagy kiberhadviselés jellegével történik meg, úgy abban az esetben az annál súlyosabban minősülő deliktum miatt indul eljárás.

Információs rendszer felhasználásával elkövetett csalás

A bűncselekmény szabályozásának történetére érdemes egy pillantást vetni. Azt az ellentmondást, hogy a hagyományos csalás esetében csak természetes személy megtévesztése tényállásszerű, ugyanakkor számítógépes környezetben a számítógép (egy számítástechnikai rendszer) működésébe történik csalárd célú beavatkozás, amit természetes személy legfeljebb utólag kontrollálhat, nehezen tudta feloldani a törvényhozás, ez problémát jelentett a jogalkalmazás számára is. Bár már az 1994. évi XVII. törvényben megszületett a számítógépes csalás tényállása, egyben szabályozva a csalás és a vírus kárt okozó bűncselekményét, ezt követően az 1996. évi LII. törvényben, majd az 1999. évi

³⁷ Btk. 267. §.

CXX. törvényben, ezt követően a 2001. évi CXXI. törvényben módosították,³⁸ végül 2012-ben született meg ez a dispozíció.

A szabályozás nehézsége például szolgálhat a jövőre vonatkozóan is, hiszen az új technológiák, az új visszaélések a jövőben is vethetnek fel problémákat a jogalkotás, illetve a jogalkalmazás szintjén. Erre fel is kell készülnünk.

A hatályos rendelkezés alapján „(1) Aki jogtalan haszonszerzés végett információs rendszerbe adatot bevisz, az abban kezelt adatot megváltoztatja, törli, vagy hozzáférhetetlenné teszi, illetve egyéb művelet végzésével az információs rendszer működését befolyásolja, és ezzel kárt okoz [...]”³⁹

A bűncselekmény elkövetési (tevékenységi) tárgya egyrészt az információs rendszer/maga a számítógépes adat, program, másrészt a hamis, a hamisított, illetve jogosulatlanul megszerzett elektronikus készpénz-helyettesítő fizetési eszköz.

A bűncselekmény elkövetési (tevékenységi) magatartásai: a törvényi tényállás elnevezésében jogtalan haszonszerzés végett a számítástechnikai rendszerbe elektronikus adat bevétele, az abban kezelt adat megváltoztatása, törlése vagy hozzáférhetetlenné tétele. A tényállás ezen része a haszonszerzés végett végrehajtott, célzatos cselekményeket (amelyek csak egyenes szándékkal valósíthatók meg) foglalja magában. A haszonszerzésre való törekvés. Az elektronikus adat bevétele történhet úgynevezett offline módban vagy akár online módban is. Más (valódi) személy kártyájának jogtalan felhasználását, azzal történő fizetést nevezik Card-not-present (CNP) csalásnak.

A deliktumnál hiányoznak a klasszikus értelemben vett tényállási elemek, azaz a tévedésbe ejtés vagy a tévedésben tartás, így sokszor a csalás tényállását – amennyiben azt például internetes hirdetési oldal segítségével követik el – sok esetben összetévesztik az elektronikus információs rendszer felhasználásával elkövetett csalással.

A sértett kárának bekövetkezését az információs rendszer jogtalan befolyásolása okozza. Azaz amennyiben valaki az információs rendszerbe bármilyen valótlan vagy a jogosultsága kereteit túllépve adatot bevisz, bármilyen adathordozóról (például CD, DVD, pendrive, külső tároló) feltölt, a már bevitt adat tartalmát megváltoztatja műszaki úton, a törléssel a rendszerben tárolt adatot megsemmisíti, úgy, hogy azt visszaállítani már nem lehet.

³⁸ Nagy Zoltán András: A számítástechnikai rendszer és adatok elleni új bűncselekmények. *Belügyi Szemle*, 40. (2002), 11–12. 27–41.

³⁹ Btk. 375. §.

A hozzáférhetetlenné tétel esetében akár ideiglenesen, akár véglegesen a jogosult gátolva van az adat elérhetőségében.

A jogosulatlanul többszörözés szintén bűncselekménynek számít.

A hamis, hamisított vagy jogosulatlanul megszerzett elektronikus készpénz-helyettesítő fizetési eszköz felhasználásával vagy az ilyen eszközzel történő fizetés elfogadásával történő károkozás, vagyis a készpénz-helyettesítő fizetési eszköz hamisítása.

„Készpénz-helyettesítő fizetési eszköz a hitelintézetekről szóló törvényben meghatározott készpénz-helyettesítő fizetési eszköz és a forgatható utalvány, a kincstári kártya, az utazási csekk, a kifizetőt terhelő adó mellett vagy adómentesen adható, korlátozott körű áruk vagy szolgáltatások ellenértékének kiegyenlítése céljából törvény alapján kibocsátott utalvány és a váltó, feltéve, hogy kivitelezése, kódolása vagy a rajta lévő aláírás folytán a másolás, a meghamisítás vagy a jogosulatlan felhasználás ellen védett.”⁴⁰

Jogosulatlannak minősül a fizetőeszköz megszerzése, ha azt az elkövető lopással (akár fizikailag veszi magához a bankkártyát, vagy pedig erre készített eszközzel megszerzi az azon szereplő adatokat) vagy erőszakkal, fenyegetéssel, megtévesztéssel, illetőleg más jogellenes módon veszi birtokba.

A bűncselekmény sértettje (passzív alanya) lehet természetes és jogi személy, akinél a kár keletkezik.

Tiltott adatszerzés

„(1) Aki személyes adat, magántitok, gazdasági titok vagy üzleti titok jogosulatlan megismerése céljából

- a) más lakását, ahhoz tartozó egyéb helyiségét vagy az azokhoz tartozó bekerített helyet titokban átkutatja,
- b) más lakásában, ahhoz tartozó egyéb helyiségében vagy az azokhoz tartozó bekerített helyen történeteket technikai eszköz alkalmazásával titokban megfigyeli vagy rögzíti,
- c) más postai küldeményét vagy egyéb zárt küldeményét titokban felbontja vagy megszerzi, és annak tartalmát technikai eszközzel rögzíti,
- d) elektronikus hírközlő hálózat vagy eszköz útján, illetve információs rendszeren folytatott kommunikáció tartalmát titokban kifürkészi, és az észlelteket technikai eszközzel rögzíti,
- e) információs rendszerben kezelt adatokat titokban kifürkészi, és az észlelteket technikai eszközzel rögzíti...

⁴⁰ Btk. 459. § 19. pont.

Az (1) bekezdés szerint büntetendő, aki személyes adat, magántitok, gazdasági titok vagy üzleti titok jogosulatlan megismerése céljából

a) nyilvános vagy a közönség részére nyitva álló helyen kívül más helyiséget vagy területet – a közösségi közlekedési eszköz kivételével –, járművet, továbbá más használatában levő tárgyat titokban átkutat,

b) nyilvános vagy a közönség részére nyitva álló helyen kívül más helyiségben vagy területen, továbbá – a közösségi közlekedési eszköz kivételével – járművön történeteket titokban technikai eszköz alkalmazásával megfigyeli vagy rögzíti.

(2) Az (1) bekezdés szerint büntetendő, aki fedett nyomozó, illetve titkos információgyűjtés folytatására vagy leplezett eszközök alkalmazására feljogosított szervvel titkosan együttműködő személy kilétének vagy tevékenységének megállapítása céljából az (1) bekezdésben meghatározottakon kívül információt gyűjt.

(3) Az (1) bekezdés szerint büntetendő, aki az (1)–(2) bekezdésben meghatározott módon megismert személyes adatot, magántitkot, gazdasági titkot vagy üzleti titkot továbbít vagy felhasznál.

(4) A büntetés egy évtől öt évig terjedő szabadságvesztés, ha az (1)–(3) bekezdésben meghatározott tiltott adatszerzést

a) hivatalos eljárás színlelésével,

b) üzletszerűen,

c) bűnszövetségben vagy

d) jelentős érdeksérelmet okozva követik el.⁴⁴¹

A bűncselekmény elkövetési (tevékenységi) tárgya: személyes adat, magán-, gazdasági és üzleti titok.

A bűncselekmény elkövetési (tevékenységi) magatartása: minden olyan releváns cselekmény, amely a személyes adat és a fentebb említett titkok megismerésére, rögzítésére, gyűjtésére alkalmas (immateriális tényállás).

A deliktum tettese (aktív alanya) az a személy lehet, aki a személyes adat, a magántitok, a gazdasági titok vagy üzleti titok jogosulatlan megismerése céljából más lakását, egyéb helyiségét vagy az azokhoz tartozó bekerített helyet titokban átkutatja, más lakásában, egyéb helyiségében vagy az azokhoz tartozó bekerített helyen történeteket technikai eszköz alkalmazásával megfigyeli vagy azt rögzíti, más közlést tartalmazó zárt küldeményét felbontja vagy megszerzi, és annak tartalmát technikai eszközzel rögzíti, elektronikus hírközlő hálózat – beleértve az információs rendszert is – útján másnak továbbított vagy azon tárolt adatot kifürkészi, és az azon észlelteket technikai eszközzel rögzíti.

Az elkövetés helye mint esetleges tárgyi elem, kiemelés érdemel, ugyanakkor ez alapján nem vonható a törvényi tényállás alá az a magatartás, amikor munkahelyi irodákban, egyéb helyiségekben kerül sor az ott történetek technikai

⁴⁴¹ Btk. 422. §.

eszköz alkalmazásával való megfigyelésére vagy rögzítésére. De lege ferenda kívánatos volna az elkövetés helyének kiterjesztő értelmezése.

Információs rendszer vagy adat megsértése

„(1) Aki információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve vagy azt megsértve bent marad, vétség miatt két évig terjedő szabadságvesztéssel büntetendő.

(2) Aki

a) az információs rendszer működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza, vagy

b) információs rendszerben lévő adatot jogosulatlanul vagy jogosultsága kereteit megsértve megváltoztat, töröl vagy hozzáférhetetlenné tesz,

büntett miatt három évig terjedő szabadságvesztéssel büntetendő.

(3) A büntetés büntett miatt egy évtől öt évig terjedő szabadságvesztés, ha a (2) bekezdésben meghatározott bűncselekmény jelentős számú információs rendszert érint.

[...]

(5) E § alkalmazásában adat: információs rendszerben tárolt, kezelt, feldolgozott vagy továbbított tények, információk vagy fogalmak minden olyan formában való megjelenése, amely információs rendszer általi feldolgozásra alkalmas, ideértve azon programot is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja.”⁴²

A tényállás jogi tárgyai: a számítástechnikai rendszerek integritása, biztonsága. Btk. 423. § (1) bekezdés b) pontjában az információs rendszerek biztonságos működése, azaz a jogosultság kereteinek megsértése, ezáltal a számítógépen vagy az információs rendszeren tárolt adat megváltoztatása (a rendszerhez jogosult személy olyan szándékos magatartása értendő ez alatt, amikor a magatartása az adat rosszindulatú megváltoztatására irányul).

A bűncselekmény elkövetési (tevékenységi) tárgyai: az információs rendszer (a számítógép vagy számítástechnikai rendszer) és az abban tárolt számítógépes programok és elektronikus adatok.

Az információs rendszer fogalmát a Btk. 459. § (1) bekezdés 15. pontja határozza meg: az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezés vagy az egymással kapcsolatban lévő ilyen berendezések összessége.

⁴² Btk. 423. §.

Az informatikai hálózat esetében megkülönböztetünk belső hálózatot (intranet), vagy az internet részét képező hálózatot (például egy bank, biztosító hálózata), vagy a szerver feltalálási helyét a valós térben vagy a virtuális térben (mint például az úgynevezett *cloud* szerverek esetében). A hálózatok egy része publikus, azaz minden felhasználó által, céljának megfelelően használható, a hálózatok másik része azonban a nyilvánosság elől elzárt és csak a beavatottak által ismert jelszóval, egyéb azonosítóval használható.

A bűncselekmény elkövetési (tevékenységi) magatartásai:

1. A *jogosulatlan belépés*, amely megtörténhet egy más által jogszerűen birtokolt, használt számítástechnikai rendszerbe, úgy, mintha jogosult használó lenne (színlelés), vagy a számítástechnikai rendszeren keresztül egy védett hálózatba.

Szükséges az, hogy a számítógép vagy az informatikai hálózat, számítástechnikai hálózat bármilyen biztonsági és/vagy védelmi megoldásokkal aktívan védve legyen (vagyis a belépéskor minden egyes felhasználó legalább külön-külön felhasználónévvel és jelszóval, illetve egyéb azonosítóval tudjon csak jogszerűen belépni).

Jogosulatlan belépés, ha valaki ezen feltételek fennállása esetén, tehát az *aktív védelem ellenére*, az (aktív) védelemmel ellátott számítógépbe vagy számítástechnikai rendszerbe vagy védett hálózatba a jogosultsága kereteit túllépve

- a biztonsági rendszer hiányosságait kihasználva jogosulatlanul belép, vagy
- más felhasználó nevével és annak belépési kódjával lép be.

A bűncselekmény elkövetése szempontjából nem számít, hogy hogyan jut a tettes a belépéshez szükséges adatokhoz, azaz a megszerzésének módja lényegtelen. Lehetséges megtévesztéssel (*social engineeringgel*), kifürkészéssel, a felhasználó hanyagságának kihasználásával – a *clean desk* (tisztá asztal) szabályának megszegésével, a monitoron, a munkasztalon vagy egyéb elérhető/látható helyen hagyott felhasználónév és jelszó otthagynak következtében –, illetve a világhálón is elérhető kódmegismerő program segítségével.

A belépés nem tekinthető jogosulatlannak, ha a számítástechnikai rendszer nincs ellátva semmilyen védelemmel (hálózati, illetve fizikai), vagy a védelem nem aktivált.

2. A *belépési jogosultsága kereteinek túllépésével, illetőleg annak megsértésével* történő bennmaradás. Ebben az esetben a tettes a saját felhasználónévvel és jelszóval lép be az adott információs rendszerbe, de a felhasználói jogosultságát

túllépve olyan műveleteket akar folytatni, amelyekre a jogosultsága már nem terjed ki.

Ennek megállapítása nem igényel különleges szakértelmet, hiszen az információs rendszerekhez történő hozzáférés előre meghatározott, így annak véletlenszerű elkövetése szinte kizárt.

Sem az információs rendszer elleni támadásokról szóló 2013/40/EU irányelvben, sem a Btk.-ban nem található annak pontos meghatározása, hogy mit is értenek a jogosultság kereteinek túllépésén, és milyen helyzetben rendeli büntetni a törvény, illetve milyen esetek képezhetik ez alól a kivételt. Így előfordulhat olyan vis major eset egy rendszerben, amikor a kárelhárítás érdekében történt jogosultság kereteinek túllépése is büntethető.

Az információbiztonság alapjai: a hálózatok

Bevezetés

Az infokommunikációs hálózatokban az információbiztonság megteremtése mindig is nagy kihívást jelentett a számítógépek, a rádiótelefonok megjelenése óta, és különösen nagy figyelmet kell fordítanunk rá az internet, a globális telefonhálózatok elterjedése és az általunk használt eszközök (okostelefonok, táblagépek, számítógépek, IoT-eszközök) világméretű hálózatba kapcsolása óta. Ezt a folyamatot kiválóan foglalja össze Muha Lajos doktori értekezésének bevezetőjében, amikor a következőket írja:

„A modern állam, annak minden szervezete és polgára kiszolgáltatottá vált a számítógépekből, kommunikációs eszközökből és automata rendszerekből álló bonyolult, többszörösen összetett információs infrastruktúrának. Napjainkban ezen eszközök nélkül életünk elképzelhetetlenné vált. Vezetékes és mobil telefonon tartjuk szeretteinkkel a kapcsolatot, ha pénzre van szükségünk, a bankjegykiadó automatához (ATM) fordulunk, amelynek a lényege egy személyi számítógép, ami vezetékes telefonvonalon keresztül a bankunk vagy az elszámoló központ számítógépére csatlakozik, és digitális kommunikációjuk dönti el, hogy kaphatunk-e készpénzt az automatából vagy sem. Munkahelyünkön a munkánkhöz szükséges adatok jelentős része a számítógépen van tárolva. A legtöbb esetben már nem is a saját asztali számítógépünkön, hanem távol, néha több száz vagy ezer kilométerre lévő központi számítógépeken. Ezek a számítógépeken tárolt adatok teszik lehetővé, hogy például a villamosenergia-szolgáltatónk átlássa, hol mennyi áramra van szükség, és honnét tudja azt beszerezni. Ha ezekben a rendszerekben bárhol, bármilyen hiba adódik, máris elindul egy dominóhatás. Villamos energia nélkül más számítógépek is leállnak, sötétség lesz, de még hideg is, mert az elektromosan vezérelt gázfűtésünk is leáll. Ha nem működnek a bankjegykiadó automaták, akkor még a vésztartalék petróleumlámpával világító üzletben sem tudjuk alapvető létszükségleti cikkeinket beszerezni. Ez olyan káoszba torkolhat, amelynek kimenetele nehezen jósolható meg.

Tudomásul kell vennünk, hogy információs rendszereink egyre gyakrabban szembesülnek az igen sokféle forrásból származó biztonsági fenyegetéssel, többek között gazdasági hírszerzéssel, ipari kémkedéssel, számítógépes csalással, szabotázzsal, vandalizmussal, tűzzel vagy árvízzel. A szándékos károkozások olyan formái, mint a számítógépvírusok, a számítógépes betörések vagy a szolgáltatás-megtagadásra vezető támadások egyre gyakoribbá, általánosabbá válnak, ugyanakkor ezek egyre vakmerőbbek és egyre bonyolultabbak is. Egyre nagyobb fenyegetést jelent sérülékeny információs rendszereinkre

a hadviselés új formája, az információs hadviselés, de még inkább a békeidőkben is állandóan fenyegető terrorizmus számítógépes változata, a kiberterrorizmus.”⁴³

Napjainkban jellemzően a terheléses támadások végrehajtásához szükséges botnetvírusok, illetve a zsarolóvírusok (*ransomware*) a jellemző veszélyforrások.⁴⁴

Éppen az itt leírtak okán célszerű megvizsgálni, hogy az infokommunikációs hálózatokban melyek az információvédelem alapelvei, milyen védelmi megoldásokkal találkozhatunk, miket alkalmazhatunk a napi gyakorlatban, mik a szolgáltató és mik a felhasználó felelősségi körébe tartozó feladatok. Ezek alapján pedig az is körülhatárolható, hogy melyek lehetnek a kibernetizáció számára releváns információk forrásai.

Az információbiztonság alapjai

Mindenekelőtt azt érdemes tisztázni, hogy mit értünk információbiztonság alatt. Ez ugyanis nem egyezik meg az adatvédelemmel vagy az informatikai biztonság fogalmával, ugyanakkor ezek között nyilvánvalóan szoros kapcsolat áll fenn.

Le kell azonban itt szögezni, hogy a fogalmi kérdések meghatározásánál alapelveként kell kezelni, miszerint „a terminológiai kérdések vizsgálata során a megnevezéssel szemben a tartalomnak van elsődlegessége”.⁴⁵ Ez már csak azért is fontos, mert – mint a későbbiekben látható lesz – mára számtalan olyan elnevezés került be a gyakorlati életbe (például informatikai biztonság, elektronikus információbiztonság, de akár még az információbiztonság is), amelyeket sokszor vállalatoknál, intézményeknél is pontatlanul, olykor egymás szinonimájaként is használnak. A kibernetizáció számára azért is fontos a tartalom megismerése, ezek tisztázása, mert egy nyomozás során meg kell találni azokat az egyéneket, csoportokat, akik a számára releváns kérdéseket meg fogják tudni válaszolni.

Az előző fejezetben már ismertetett fogalmi különbségek mellett meg kell jegyeznünk, hogy az adat és információ megnevezés sokszor még a szakirodalomban is együtt, akár egymás szinonimájaként jelenik meg, vagy pontosabban

⁴³ Muha Lajos: *A Magyar Köztársaság kritikus információs infrastruktúráinak védelme*. PhD-értékezés. Budapest, ZMNE, 2007b. 4–5, 127.

⁴⁴ Mezei Kitti – Nagy Zoltán András: *A zsarolóvírus és a botnet mint napjaink két legveszélyesebb számítógépes vírusa*. In Gaál Gyula – Hautzinger Zoltán (szerk.): *Szent Lászlótól a modern kori rendészettudományig*. Pécs, Pécsi Határőr Tudományos Közlemények, 19. kötet. (2017). 163–168.

⁴⁵ Munk Sándor: *Információbiztonság vs. informatikai biztonság*. *Hadmérnök*, Különszám. Robot-hadviselés 7. Tudományos Szakmai Konferencia 2007. november 27.

fogalmazva adott témák szempontjából nem feltétlenül tesznek a szerzők különbséget a két fogalom között. (Például az Ibtv.-ben sem, bár az értelmező rendelkezésekben megjelenik a két fogalom definíciója, a törvényben együtt használatos az adat és az információ, ami tudományosan helytelen.) Így például, amikor egy infokommunikációs rendszerben tárolásról, továbbításról, feldolgozásról beszélünk, akkor annak technikai eszközei és módszerei nagyrészt függetlenek lehetnek attól, hogy adatról vagy információról beszélünk-e. Erre egy példa, amikor adatok, információk tárolásának, megosztásának, titkosításának technikai aspektusairól beszélünk. Ennek megfelelően jelen fejezet a továbbiakban nem választja szét ezeket, hiszen a következőkben ismertetendő témák mind az adatok, mind az információk tekintetében egyaránt helytállóak.

Az adatok (információk) életciklusát az 1. ábra mutatja be.



1. ábra: Az adatok életciklusa

Forrás: Rich: [Data Security Lifecycle 2.0](#). Securosis. Blog. 2011. szeptember 6.

Az adatok (információk) életciklusának 6 állomását biztonsági szempontból 2 fő csoportra bonthatjuk, az *adatmozgással járó* (előállítás, használat, megosztás, törlés) és az *adatmozgással nem járó* (tárolás, archiválás) műveletekre.

Ezt a bontást azért célszerű megtenni, mert napjainkban, amikor egyre több felhőalapú rendszert használunk, ha a felhasználó egy ilyen rendszer használatakor bármilyen aktív műveletet végez, akkor az az adatok mozgásával, utazásával fog járni. Márpedig ekkor olyan kockázatokat is kezelni kell, mint a felhasználó és a szolgáltató közötti adatforgalom passzív lehallgatása, közbeékelődéses

támadások, visszajátszásos támadások stb. Ráadásul így a felhasználó és a szolgáltató felelősségi körét jobban szét lehet választani, hiszen az adatmozgással járó műveleteknél a felhasználónak nagyobb a felelősségi köre, mint az adatmozgással nem járó műveleteknél. Ezekről a későbbiekben még részletesebben lesz szó.

A következőkben pedig vizsgáljuk meg az adatvédelem, az informatikai biztonság, a kiberbiztonság és az információbiztonság fogalmát, azok tartalmát, a közöttük lévő különbségeket és adott esetben az azonos tartalmi részeket!

Mindenekelőtt azonban érdemes tisztázni az egyes rendszerek, így az informatikai rendszer, az infokommunikációs rendszer és az elektronikus információs rendszer közötti különbséget. Amíg például az 1990-es években még nagyon markánsan szét lehetett választani például egy analóg rádióhálózatot egy lokális számítógép-hálózattól, addig mára a funkcióbeli különbségek eltűntek, a technológiai konvergencia okán ma sokkal inkább infokommunikációs rendszerekről vagy – a jogszabályokban található terminológia szerint – elektronikus információs rendszerekről beszélünk, beszélhetünk. Mára a szakemberek is sokszor egymás szinonimájaként használják az említett fogalmakat, és valljuk meg, nagyon nehéz is közöttük különbséget tenni. Ma már nem nagyon létezik olyan számítógép-hálózat, amely ne kapcsolódna más hálózatokhoz (például interneten keresztül), ne lenne benne elérhető elektronikus levelezés, de például az okostelefonunk is sokkal többre alkalmas, mint pusztán telefonálásra vagy sms-küldésre/fogadásra. Éppen ezek miatt, szem előtt tartva jelen mű fő témáját, itt nem (vagy inkább már itt sem) érdemes különbséget tenni ezen rendszerek között. Ennek megfelelően a továbbiakban az informatikai rendszer, az infokommunikációs rendszer és az elektronikus információs rendszer alatt ugyanazt értjük.

A vizsgálatot az információbiztonsággal érdemes kezdeni.

Az információbiztonság fogalma

Az információbiztonságon komplex, az alábbi három dimenzió mindegyikében megvalósuló védelmet kell értenünk:

- *fizikai dimenzió*: az információbiztonság kapcsán ez a különböző információs infrastruktúrák, infokommunikációs rendszerek elemei elleni, többnyire úgynevezett „kemény típusú” (*hard kill*) támadásokat, valamint azok fizikai védelmét jelenti;
- *információs dimenzió*: az információbiztonság kapcsán ez a különböző információs folyamatok, adatszerzés, adatfeldolgozás, kommunikáció stb.

elleni, többnyire elektronikus úton történő, „lágy típusú” (*soft kill*) támadásokat, valamint azok többnyire logikai védelmét jelenti;

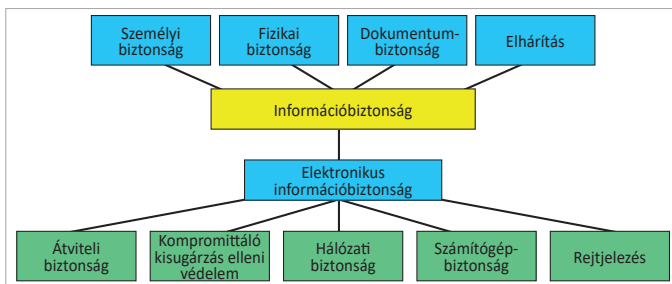
- *tudati dimenzió*: az információbiztonság kapcsán a közvetlenül az emberi gondolkodás – észlelés, érzékelés, értelmezés, vélemény, vélekedés – elleni támadásokat, valamint azok védelmét jelenti.

Az információbiztonság megvalósítása során tehát komplex és integrált védelmet kell kialakítani annak érdekében, hogy mindhárom dimenzióban megvédezhessük a kritikus információkat. Kritikusnak tekintendő minden olyan információ, amelyet a támadó felhasználhat a saját érdekei érvényesítésében és/vagy döntési folyamataiban, vagy kárt okozhat számunkra, akadályozhatja, esetleg ellehetetlenítheti a saját döntési folyamatainkat.

Az információbiztonság, így a kritikus információk védelme, főleg az alábbi biztonsági komponensekre, az itt alkalmazható védelmi megoldásokra kell hogy kiterjedjen:

- a személyi biztonság;
- a fizikai biztonság;
- a dokumentumbiztonság;
- az elhárítás (vagy felderítés elleni tevékenység);
- az elektronikus információbiztonság.

Ezt, valamint a könyv témájának szempontjából leglényegesebb információbiztonsági részterületet, az elektronikus információbiztonság alterületeit mutatja be a 2. ábra.



2. ábra: A komplex információbiztonság elemei

Forrás: Haig Zsolt: Az információbiztonság komplex értelmezése. Robothadviselés 6. Tudományos Szakmai Konferencia 2006. november 22. *Hadmérnök.* Különszám.

Az információbiztonság részterületei az alábbiak szerint jellemezhetők:

A *személyi biztonság*: az érzékeny adatokhoz, kritikus információkhoz való hozzáférés engedélyezéséhez szükséges biztonsági követelmények összessége. Ezen adatokhoz, információkhoz csak azok a személyek férhetnek hozzá, akik igazoltan megfelelnek bizonyos követelményeknek, előírásoknak, és a munkájukhoz az adatok, információk megismerésére ténylegesen szükség van. A személyi biztonságra legjellemzőbb példa, hogy a nemzeti minősített adatok megismeréséhez szükséges a kockázatmentes nemzetbiztonsági ellenőrzés megléte, az ezek alapján kiállított személyi biztonsági tanúsítvány, valamint az aláírt titoktartási nyilatkozat is.

A *fizikai biztonság*: azon szabályzatok, fizikai akadályok, jelzőrendszerek (például sorompók, falak, beléptetőrendszerek, riasztórendszerek, behatolásjelzők, tűzjelzők stb.) összessége, amelyek megakadályozzák az illetékteleneket a kritikus információkhoz, az azokat tartalmazó dokumentumokhoz, eszközökhöz való hozzáférésben, a számukra nem engedélyezett épületekbe, épületrészekbe, helyszínekre történő bejutásban, valamint meggátolják az ezek elleni fizikai támadást. A fizikai biztonságra jellemző példa az előerős őrség felállítása a bejáratoknál, a kamerarendszer és az úgynevezett proximity kártyaalapú beléptető használata az épületeken belül.

A *dokumentumbiztonság*: azon szabályzatok, előírások és intézkedések összessége, amelyek segítségével az összes dokumentumot azok minősítése, azaz a bennük lévő információk érzékenysége szerint tudjuk védeni. Fontos kitétel, hogy az érzékeny adatokat, kritikus információkat tartalmazó dokumentumokhoz csak azok férjenek hozzá, akiknek ez feltétlenül szükséges, az ő számukra azonban a hozzáférés biztosított legyen. Miután valamennyi elektronikus adathordozó egyben dokumentumnak is minősül, az információbiztonság többi részterületével ellentétben a dokumentumbiztonság közvetlen módon is kapcsolódik az elektronikus információbiztonsághoz. A dokumentumbiztonságra jellemző példa a nemzeti minősített adatoknál használandó titkos ügykezelés (TÜK).

Az *elhárítás* (vagy felderítés elleni tevékenység): azon védelmi jellegű módszerek és tevékenységek összessége, amelyek ellenérdekelt felek (például ellenérdekelt hírszerző szolgálatok, [kiber]bűnözők, [kiber]terroristák, hacktivisták, ártó szándékú belső munkatársak és/vagy külső közreműködők stb.) tevékenységének felderítésére és kivédésére irányul. Az elhárításra jellemző példa az infokommunikációs rendszerek védelme érdekében használt úgynevezett fenyegetettségekkel kapcsolatos hírszerzési tevékenység (*cyber threat intelligence*). Ez az adott védendő objektumra (szervezet, információk stb.)

a kibertérből potenciálisan fenyegetést jelentő támadók, támadási formák fel-
derítésére és a lehetséges támadások megelőzésére, valamint a már megtörtént, de
a szervezet által még fel nem ismert támadásokból származó információk – első-
sorban a dark weben történő – felkutatására és a kárenyhítéshez szükséges
intézkedés előkészítésére szolgáló tevékenység.

Az elektronikus információbiztonság fogalma:

„a biztonsági rendszabályok alkalmazása a kommunikációs, információs és más elektro-
nikus rendszerekben a feldolgozott, tárolt vagy továbbított információ bizalmasságának,
sértetlenségének vagy rendelkezésre állásának véletlen vagy szándékos elvesztése ellen,
és e rendszerek sértetlenségének vagy rendelkezésre állásának elvesztése ellen”.⁴⁶

Az elektronikus információbiztonság alterületei:

- *Átviteli biztonság:* azon szabályzatok, intézkedések és tevékenységek összessége, amelyek jelentősen megnehezítik, vagy akár el is lehetetlenítik az információk átvitele során az átviteli folyamatba történő illetéktelen beavatkozást, így különösen azok megváltoztatását, törlését, lehallgatását. Jellemző példa a rejtjelző eszközök alkalmazása az átvitel során.
- *Kompromittáló kisugárzás elleni védelem:* olyan aktív és passzív védelmi intézkedések és eszközök alkalmazása, amelyek jelentősen megnehezítik, vagy akár el is lehetetlenítik, azt, hogy az elektronikai eszközök, berendezések másodlagos sugárzásának elemzésével illetéktelenek hozzáférjenek a védendő információkhoz. Jellemző példa a berendezések és az azoknak helyet adó helyiségek árnyékolása.
- *Hálózati biztonság:* azon szabályzatok, intézkedések és tevékenységek összessége, amelyek védik a hálózatba kötött eszközöket és a hálózati szolgáltatásokat az azokon elérhető szolgáltatások szintjének csökkenése vagy ellehetetlenülése ellen, valamint jelentősen megnehezítik, vagy akár el is lehetetlenítik, illetéktelenek számára az azokban kezelt, tárolt, feldolgozott stb. adatok, információk megismerését, megváltoztatását vagy megsemmisítését. A hálózatok összekapcsolásának védelmi feladatai is ebbe a csoportba tartoznak. Jellemző példa a kiberbiztonsági operatív központ működtetése (amelynek feladata többek között a hálózatban elhelyezett speciális védelmi eszközökből és a hálózatban lévő alapműködést

⁴⁶ Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana. *Bolyai Szemle*, 17. (2008), 4. 137–156.

szolgáló eszközökön futtatott védelmi szoftverekből kapott jelzések alapján a hálózatot érő támadások felismerése, kezelése), vagy a folyamatos kockázatelemzés végrehajtása (a kockázatok feltárása, értékelése, a feltárt kockázatok hatásainak elfogadható mértékűre csökkentése stb.).

- *Rejtjelzés*: a védendő információk olyan átalakítása (titkosítása), amely jelentősen megnehezíti, vagy akár el is lehetetleníti azt, hogy illetéktelenek megismerjék azokat. A rejtjelzés része az információk eredeti formátumúvá történő visszaalakítása is. A rejtjelzést az adatéletciklus (előállítás, tárolás, használat, megosztás, archiválás, törlés) több szakaszában is lehet használni. Jellemző példa a számítógépek, okostelefonok háttértárának teljes titkosítása (például Windows operációs rendszer esetén a BitLocker használatával), így azokon minden adatot, információt titkosítottan tárolnak.
- *Számítógép-biztonság*: azon szabályzatok, intézkedések és tevékenységek összessége, amelyek védik az egyes infokommunikációs eszközöket az azokon elérhető szolgáltatások szintjének csökkenése vagy ellehetetlenülése ellen, valamint jelentősen megnehezítik, vagy akár el is lehetetlenítik, illetéktelenek számára az azokban kezelt, tárolt, feldolgozott stb. adatok, információk megismerését, megváltoztatását vagy megsemmisítését. Ma már jobbra a hálózati biztonsággal együtt kezelik, egyrészt az egyedi, hálózatba nem kötött számítógépek alacsony száma miatt, másrészt annak okán, hogy egyedi gépeknél alkalmazott védelmi szoftverek csupán részhalmazát képezik a hálózati biztonság kapcsán a hálózati végponti eszközökön használt védelmi szoftverek halmazának. Jellemző példa a vírusirtó szoftverek használata.⁴⁷

Az információbiztonság tehát komplex védelmet jelent, amely „a szóban, rajzban, írásban, a kommunikációs, informatikai és más elektronikus rendszerekben, vagy bármilyen más módon kezelt információk védelmére vonatkozik”.⁴⁸

⁴⁷ Vö. Haig (2006): i. m.

⁴⁸ Muha Lajos – Krasznay Csaba: *Az elektronikus információs rendszerek biztonságának menedzselése*. Budapest, Nemzeti Közszerológiai Egyetem, 2018.

Adatvédelem

A Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) honlapján található Adatvédelmi Értelmező Szótár szerint az „adatvédelem: a személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége”.⁴⁹ Azaz az adatvédelem kizárólag a személyes adatok védelmére vonatkozik, a személyiségi jogokkal összefüggő tevékenység. Ennek okán nem fedí le az összes információt, hanem annak csak egy bizonyos részét. Így az adatvédelem jelen fejezet témája szempontjából az információbiztonság egy – speciális – részhalmozának tekinthető. Erről a témáról bővebb információk jelen könyv adatvédelmi ismereteiről szóló fejezetében érhetők el.

Informatikai biztonság

Az *informatikai biztonság* a biztonsági kérdéseket az adott rendszerben létrehozott, tárolt, feldolgozott, továbbított stb. információk mellett kiterjeszti az azokat kezelő rendszerekre is. Az Informatikai Tárcaközi Bizottság 1994-ben kiadott 8. számú ajánlásában, majd különösen a Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága 1996-ban kiadott 12. számú ajánlásában az informatikai biztonság (az adatoknak és információknak az informatikai rendszerekben történő biztonságos kezelése) öt alapkövetelménye között határozta meg az információk rendelkezésre állását, sértetlenségét, bizalmasságát, hitelességét és a teljes informatikai, illetve információs rendszer működőképességét.⁵⁰ Később ez módosult a mára már általánosan elfogadott és a hatályos hazai jogszabályokban (például Ibtv.) is megjelenő három alapkövetelményre (bizalmasság, sértetlenség, rendelkezésre állás).

Az informatikai biztonság teljes egészében az információbiztonság részének tekinthető, hiszen minden intézkedést, tevékenységet, amelyet az informatikai biztonság érdekében teszünk, az adott rendszerekben tárolt adatok, információk bizalmasságának, sértetlenségének és rendelkezésre állásának az érdekében

⁴⁹ Vö. *Adatvédelmi Értelmező Szótár*.

⁵⁰ Vö. Munk (2007): i. m.; Bodlaki Ákos et al.: *Informatikai rendszerek biztonsági követelményei*. Budapest, Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága (MeH ITB), 12. számú ajánlása. 1996.

tesszük. Mára, ahogy azt fentebb kifejtettük, az informatikai rendszert, az infokommunikációs rendszert és az elektronikus információs rendszert azonosnak tekinthetjük, ezért az informatikai biztonságot (informatikai rendszerek biztonságát), az infokommunikációs rendszerek biztonságát és az elektronikus információs rendszerek biztonságát is azonosnak tekinthetjük.

Az elektronikus információs rendszer biztonsága

Az Ibtv. 1. § (1) bekezdés 15. pontja megfogalmazza az elektronikus információs rendszer biztonságának definícióját:

„az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos”.

Ennek megfelelően az elektronikus információs rendszer biztonsága felfogható az előbbiekben tárgyalt informatikai biztonság pontosabb, napjaink fogalmait jobban lefedő megfogalmazásának is.

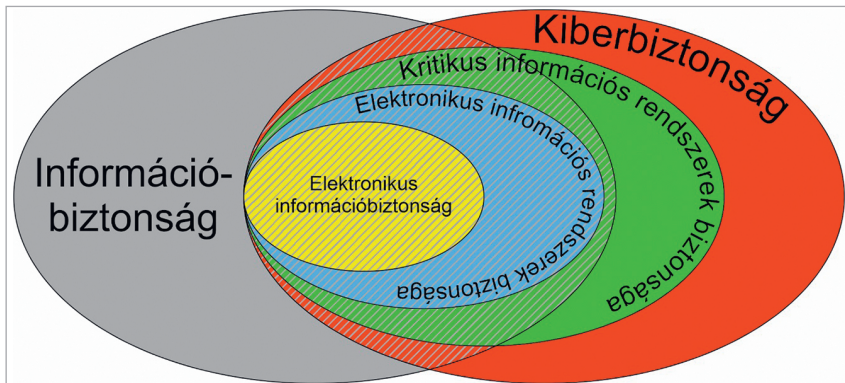
Kiberbiztonság

Az Ibtv. 1. § (1) bekezdés 26. pontja szerint a

„kiberbiztonság: a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez.”

Ennek megfelelően a kiberbiztonság tag fogalom, amely az információk védelmén kívül még nagyon sok mindenre kiterjed. Így a kiberbiztonság és az információbiztonság is egymást részben átfedő fogalmak, amelyek viszonyát szintén lehetne ábrázolni. (Fontos megemlíteni, hogy a halmazok nagysága ebben az esetben nem reprezentálja a benne lévő elemek számosságát.) A kiberbiztonság és az informatikai biztonság viszonyát tekintve az informatikai biztonság

a kiberbiztonság részének tekinthető, így a továbbiakban mindenhol a kiberbiztonság fogalmat használja a fejezet. A fent említettek kapcsolatát és egymáshoz való viszonyát mutatja be a 3. ábra.



3. ábra: Az információbiztonság, a kiberbiztonság, a kritikus információs rendszerek biztonsága, az elektronikus információs rendszerek biztonsága és az elektronikus információbiztonság egymáshoz való viszonya

Forrás: a szerző szerkesztése Muha–Krasznay (2018): i. m. alapján

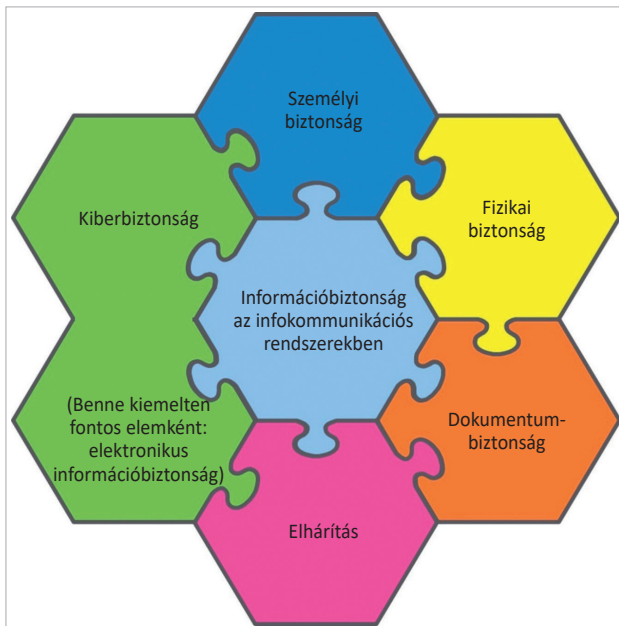
A kritikus (vagy a vonatkozó jogszabályokban használt terminológiával élve létfontosságú) információs infrastruktúrák biztonságát jelen mű keretei és témája okán most nem érdemes elemezni.

Az információbiztonság magában foglalja az elektronikus információs rendszerek biztonságát és az elektronikus információbiztonságot teljes egészében, illetve egészen kis szeleteket a kritikus információs infrastruktúrák biztonságából és a kiberbiztonságból is.

Információbiztonság az infokommunikációs rendszerekben

Az előző alfejezetben részletesen bemutattuk a különböző fogalmakat, amelyek az információk biztonsága kapcsán napjainkban felmerülhetnek, valamint ezek összefüggéseit, egymáshoz való viszonyukat is. A fentiek alapján elmondható, hogy a kritikus információk védelmét az infokommunikációs hálózatokon csak komplex módszerekkel lehet hatékonyan biztosítani, amelynek

az információbiztonság mellett a kiberbiztonságnak az információbiztonságon kívül eső elemeit is tartalmaznia kell. Ezt mutatja be a 4. ábra.



4. ábra: Az információbiztonság elemei az infokommunikációs rendszerekben

Forrás: a szerző szerkesztése

Az ábrán az egyes elemeket szimbolizáló puzzle-darabok mérete ebben az esetben sem mutatja azok tényleges, a többi elemhez viszonyított mértékét. Az infokommunikációs hálózatokban a leghangsúlyosabbnak a kiberbiztonság, ezen belül pedig az elektronikus információbiztonság tekinthető, amelyeket itt – a fent leírtak okán – a 3. ábra szerint egy közös elemként ábrázoltunk.

Amikor infokommunikációs rendszerekben lévő információk kapcsán beszélünk információbiztonságról, akkor biztonság alatt egy olyan állapotot értünk, amelyben az érintett számára kielégítő módon valósul meg az adott rendszer *zárt, teljes körű, folytonos és a kockázatokkal arányos védeleme*. Ezek alatt – az Ibtv. alapján – az alábbiakat értjük:

- „zárt védelem: az összes számításba vehető fenyegetést figyelembe vevő védelem;
- teljes körű védelem: az elektronikus információs rendszer valamennyi elemére kiterjedő védelem;
- folytonos védelem: az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem;
- kockázatokkal arányos védelem: az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével.”

Ezt a zárt, teljes körű, folytonos és a kockázatokkal arányos védelmet úgy lehet kialakítani, hogy az előző alfejezetben ismertetett, és a 4. ábrán bemutatott, az infokommunikációs rendszerekben elvárt komplex információbiztonsághoz szükséges összes elemmel foglalkozunk. Mielőtt azonban erre rátérnénk, még egy kérdést fontos tisztázni.

Amikor jelen esetben infokommunikációs rendszerekről beszélünk, akkor – a korábban leírtak szerint – az Ibtv.-ben meghatározott elektronikus információs rendszereket értjük.

„1. § (1) [...] 14b. elektronikus információs rendszer:

- a) az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlő hálózat;
- b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi; vagy
- c) az a) és b) pontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok.”

Ezt a meghatározást a 2018. évi CXXI. törvény 111. § (3) bekezdése módosította.

A korábbi, 2013. évi L. tv. 1. § 2. pontja a következő, kevésbé általános – ám jelen téma megértését talán jobban szolgáló – meghatározást használta az elektronikus információs rendszerek fogalmának meghatározására: „Elektronikus információs rendszer az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese.”

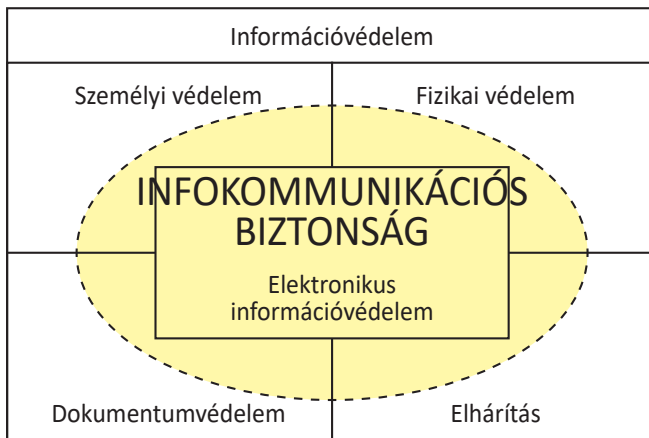
A fenti definíciót alapul véve a Muha–Krasznay szerzőpáros leírása szerint

„az elektronikus információs rendszerekhez tartoznak:

1. a számítástechnikai rendszerek és hálózatok;
2. a helyhez kötött, mobil és egyéb rádiófrekvenciás, valamint műholdas elektronikus hírközlési hálózatok, szolgáltatások;

3. a rádiós vagy műholdas navigáció;
4. az automatizálási, vezérlési és ellenőrzési rendszerek (vezérlő és adatgyűjtő, távmérő, távérzékelő és telemetriai rendszerek stb.);
5. a fentiek felderítéséhez, lehallgatásához vagy zavarásához használható rendszerek.”⁵¹

Az információvédelem, az infokommunikációs biztonság és az elektronikus információvédelem kapcsolatát mutatja az 5. ábra.



5. ábra: Az infokommunikációs biztonság, az elektronikus információvédelem és az információvédelem kapcsolata

Forrás: Muha (2007b): i. m.

Mivel a téma szempontjából – ahogy azt már feljebb is kifejtettük – az elektronikus információs rendszerek és az infokommunikációs rendszerek között nincs számottevő különbség, sőt ma már azonosnak tekinthetők, az egyszerűség kedvéért a továbbiakban elektronikus információs rendszerek biztonsága alatt az infokommunikációs rendszer biztonságát, az elektronikus információs rendszerek alatt pedig infokommunikációs rendszereket is értünk.

Muha meghatározása szerint:

„Az elektronikus információs rendszer biztonsága az elektronikus információs rendszer olyan – az érintett számára kielégítő mértékű – állapota, amelyben annak védelme

⁵¹ Vö. Muha–Krasznay (2018): i. m.

az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.”⁵²

Ahol az Ibtv. 1. § 19) bekezdése szerint:

- „bizalmasság: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról; (8. pont)
- rendelkezésre állás: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek; (38. pont)
- sértetlenség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárattal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható; (39. pont).”⁵³

A továbbiakban ezeket átvéve és elfogadva vizsgáljuk meg az elektronikus információs rendszerekben a szolgáltató és a felhasználó feladatait, felelősségét, valamint a kibernetizáció számára releváns információk forrásait.

A szolgáltató és a felhasználó feladatai, felelőssége, valamint a kibernetizáció számára releváns információk forrásai

A fentiek bemutatása és értelmezése után azt kell tisztázni, hogy az elvárt zárt, teljes körű, folytonos és a kockázatokkal arányos védelmet ki és hogyan tudja biztosítani egy infokommunikációs (elektronikus információs) rendszerben. Minden ilyen rendszer általában két szereplőre, a szolgáltatóra és a felhasználóra bontható. (Léteznek természetesen speciális esetek is, amikor például valamely vállalat önmagában a rendszer szolgáltatója [ebben az esetben üzemeltetője] és felhasználója is, akkor azonban minden védelmi elemről neki magának kell gondoskodnia.)

⁵² Vö. Muha–Krasznay (2018): i. m.

⁵³ Ibtv. 1. §.

A következőkben a felhőalapú rendszerek kapcsán vezetjük végig a szolgáltató és a felhasználó felelősségét az információvédelemben. Egyrészt azért, mert napjainkra talán ezek a legjellemzőbb infokommunikációs szolgáltatások; másrészt azért, mert az összes lehetséges eset vizsgálatára jelen mű keretei szűkek; harmadrészt pedig azért, mert a téma szempontjából, azaz a kiberyomozók számára nagy valószínűséggel ennek az esetnek a vizsgálata a legfontosabb, azaz ezekkel a kérdésekkel fog a leggyakrabban találkozni.

Ahhoz, hogy az információbiztonsági feladatok említett szétválasztását elvégezhessük, először is célszerű áttekinteni a felhőalapú rendszereket, azok tulajdonságait.

A felhőalapú rendszerek rövid összefoglalása

A NIST (*National Institute of Standards and Technology Information Technology Laboratory*) által *The NIST Definition of Cloud Computing* címen kiadott és mára kvázi szabványnak tekinthető tanulmány szerint akkor beszélhetünk felhőalapú szolgáltatásról, ha az alábbi tulajdonságok egy rendszerben (részben vagy egészben) fellelhetők:

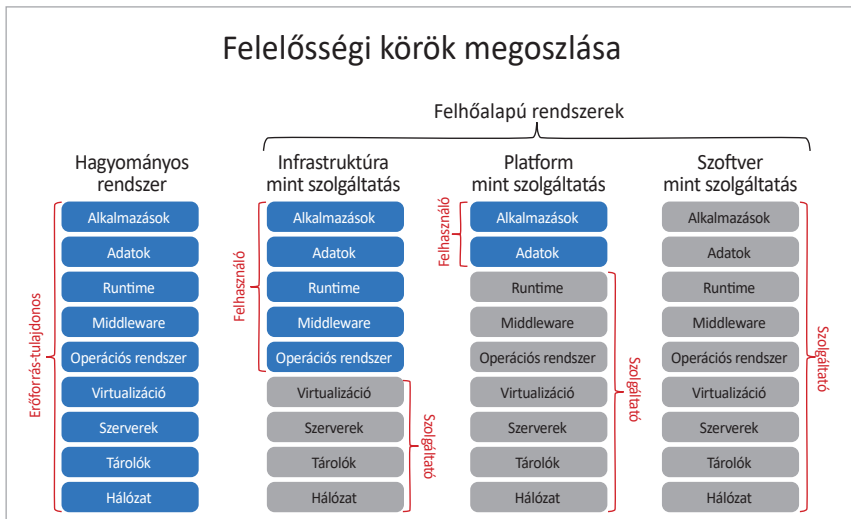
- igény szerinti önkiszolgálás (*on-demand self-service*): a felhasználók szükségleteik szerint képesek változtatni az igényelt számítási kapacitásokat;
- jó hálózati hozzáférés (*broad network access*): hálózaton, szabványos mechanizmusokon keresztül, heterogén eszközökkel elérhetők a szolgáltatások;
- erőforráskészletek (*resource pool*): a szolgáltató több-bérlős modell szerint, a fogyasztói kereslet függvényében dinamikusan osztja ki és osztja újra az erőforrásokat, amelyek pontos helyét a felhasználó általában nem ismeri, vagy nem tudja kontrollálni;
- teljes rugalmasság (*rapid elasticity*): a felkínált kapacitások gyorsan és rugalmasan változtathatók, fel- és leskálázhatók az aktuális igények szerint;
- mért szolgáltatások (*measured service*): a felhasznált erőforrások ellenőrizhetők, használatuk pontosan mérhető.

A felhőalapú rendszereket az alábbi szolgáltatási és telepítési modellek szerint csoportosítják.

Szolgáltatási modellek (service models)

Szoftver mint szolgáltatás (*cloud software as a service – SaaS*): a felhasználó számára nyújtott képességeket a felhő-infrastruktúrában futó szolgáltatói alkalmazások teszik lehetővé. Az alkalmazások különböző eszközökön, vékony kliensfelületen, például webböngészőn elérhetők (ilyen például a webmail-szolgáltatás). A felhasználó néhány felhasználóspecifikus alkalmazás korlátozott konfigurációs beállítási lehetőségétől eltekintve semmilyen hatással sincs a mögöttes infrastruktúrára, hálózatra, szerverekre, operációs rendszerekre, a tárolás módjára, vagy akár egyedi alkalmazások képességére.

Platform mint szolgáltatás (*cloud platform as a service – PaaS*): ebben az esetben a szolgáltató által támogatott programnyelveken és eszközökkel a fogyasztó által készített vagy megszerzett alkalmazásokat a szolgáltató telepíti egy felhő-infrastruktúrába. A felhasználó itt sem képes menedzselni vagy ellenőrizni a mögöttes felhő-infrastruktúrát, beleértve a hálózatot, szervereket, operációs rendszereket vagy a tárolókat, de kontrollálja a telepített szolgáltatásokat és az azok fogadására szolgáló környezet konfigurációját.



6. ábra: Felelősségi körök megoszlása a szolgáltatási modellekben

Forrás: a szerző szerkesztése Zaid Kartit et al.: *Network Issues in cloud computing and counter-measures*. 2014. 4. alapján.

Infrastruktúra mint szolgáltatás (*cloud infrastructure as a service – IaaS*): a felhasználó számára ebben az esetben olyan számítási, tárolási, hálózati és egyéb alapvető informatikai erőforrásokat kínál a szolgáltató, amelyekre és amelyekeken tetszőleges szoftvereket telepíthet és futtathat, beleértve az operációs rendszereket és alkalmazásokat. A felhasználó nem képes menedzselni vagy ellenőrizni a mögöttes felhő-infrastruktúrát, de kontrollálni tudja az operációs rendszereket, tárhelyeket, telepített alkalmazásokat, és esetleg korlátozott hatása lehet a hálózati elemek (például tűzfalak) kiválasztására.

A hagyományos (azaz a felhasználó tulajdonában és üzemeltetésében lévő, valamint az egyes szolgáltatási modelleknél a felhasználó és a szolgáltató felelősségi körébe tartozó feladatokat jól szemlélteti a 6. ábra.

Telepítési modellek (deployment models)

Magánszámítási felhő (*private cloud*): a felhő-infrastruktúra kizárólag egy szervezet számára működik. Ezt a felhasználó szervezet, de akár egy másik fél is menedzselheti, fizikailag lehet akár a felhasználó telephelyén, akár azon kívül.

Közösségi számítási felhő (*community cloud*): ebben az esetben a felhő-infrastruktúrát több szervezet megosztottan használja úgy, hogy az az adott közösség közös érdekeit támogassa (például közös küldetés, biztonsági követelmények, előírások, megfelelési szempontok). Ezt menedzselheti akár a felhasználó szervezet, akár egy másik fél is, fizikailag lehet a felhasználó telephelyén, akár azon kívül.

Nyilvános számítási felhő (*public cloud*): a felhő-infrastruktúra ebben a modellben bárki (a nagyközönség vagy egy nagy [ipari] csoport) számára elérhető, de a felhőszolgáltatást nyújtó szervezet tulajdonában van. Ez tekinthető ma a legismertebb telepítési modellnek.

Hibrid számítási felhő (*hybrid cloud*): a felhő-infrastruktúra ekkor több, az előző modellek szerint felépülő rendszer (magán-, közösségi, nyilvános) keveréke, ahol a felhők megtartják egyedi jellegzetességeiket, azokat szabványosított vagy szabadalmazott technológiák kötik össze, lehetővé téve az adatok és alkalmazások hordozhatóságát (például *cloud bursting* technológia a felhők közötti terhelés kiegyenlítésre, amikor a magánfelhőben rendelkezésre álló erőforrások elfogynak, és azokat más, tipikusan nyilvános felhőben meglévővel pótolják ki).

A szolgáltatási és a telepítési modellekből egyfajta mátrix képezhető. Ebben a mátrixban kell megtalálnia a felhasználónak a számára megfelelő szolgáltatást, ide kell elhelyeznie saját (meglévő vagy tervezett) hálózatát, majd ennek a mátrixnak a megfelelő mezőjébe pozicionált termékek közül kell kiválasztania a számára megfelelőket.⁵⁴

A fentiek közül a téma szempontjából a nyilvános számítási felhő (*public cloud* – PC) és a szoftver mint szolgáltatás (*cloud software as a service* – SaaS) típusú rendszereket (PC/SaaS felhőalapú rendszerek) vizsgáljuk tovább. Ezek azok a mindenki számára – a meglévő személyi használatú infokommunikációs eszközök (például notebook, okostelefon stb.) felhasználásával, akár csekély számítástechnikai tudással is használható, olcsón, sokszor ingyenesen – igénybe vehető rendszerek, szolgáltatások (mint például Facebook, Gmail, Dropbox, Twitter, Skype stb.), amelyek ma már szerves részét képezik mindennapi életünknek, kommunikációnknak. Az „átlagfelhasználók” ezeket a rendszereket használják leggyakrabban, de nagyon jellemző ezek (akár még nagy-) vállalati alkalmazása is. Éppen ezért a kibernetizáció számára is ezek a legfontosabbak.

A következőkben az információbiztonság 4. ábra szerint bemutatott részterületeit vizsgáljuk meg a szolgáltatói és felhasználói felelősség oldaláról megközelítve, valamint azt is bemutatva, hogy a kibernetizáció honnan juthat számára releváns információkhoz.

A személyi biztonság a PC/SaaS felhőalapú rendszerekben

A szolgáltató felelőssége: A PC/SaaS felhőalapú rendszerekben a szolgáltatók felelőssége a saját rendszereikhez hozzáférő személyek (saját alkalmazottak, alvállalkozók) ellenőrzése, erre a felhasználónak nincs ráhatása, de még csak rálátása sem. A felhasználó nem szabhatja meg, vagy kérheti számon a szolgáltatót, hogy hogyan végzi ezt, mit követel meg az érintett emberektől. Éppen ezért az ilyen rendszerekben tárolt, kezelt stb. adatokat a felhasználónak ennek megfelelően kell védenie (például titkosítottan tárolni stb.) A kibernetizáció személyi biztonsággal kapcsolatos információkat csekély eséllyel kap a szolgáltatóktól, jellemzően ilyenek a hazai internet- és/vagy felhőszolgáltatóktól szerezhető be. Ugyanakkor ezen információk nem is igazán relevánsak számára, hiszen sok

⁵⁴ Kovács Zoltán: *Az infokommunikációs rendszerek nemzetbiztonsági kihívásai*. Doktori értekezés. Budapest, Nemzeti Közszolgálati Egyetem, 2015.

esetben nem is lehet pontosan felmérni az adott adatokhoz a szolgáltatói oldalon esetlegesen hozzáférők körét (például technikai rendszer karbantartásáért felelős alvállalkozók, egy másik országba, de vállalaton belül kiszervezett, távoli eléréssel rendelkező helpdeskesek stb.).

A felhasználó felelőssége: A felhasználó ugyanakkor teljes ráhatással rendelkezik a szolgáltatások eléréséhez használt végponti eszköz, leggyakrabban a hordozható infokommunikációs eszközök felett, így afelett is, hogy azokhoz ki, milyen jogosultságokkal fér hozzá. Számukra az adatok, információk körének, minősítésének stb. megfelelően előírhatja a hozzáféréshez szükséges engedélyek körét, követelmények listáját. A kibernyomozó a felhasználótól érdemi információkhoz juthat ebben a kérdéskörben.

A fizikai biztonság a PC/SaaS felhőalapú rendszerekben

A szolgáltató felelőssége: A PC/SaaS felhőalapú rendszerekben a szolgáltatók felelőssége a saját rendszereik fizikai védelme, erre a felhasználónak nincs ráhatása, de még csak rálátása sem. Ugyanúgy, mint az ezen rendszerek eléréséhez használt internetszolgáltatás során használt infrastruktúrák esetében sem. A felhasználó nem szabhatja meg, vagy kérheti számon a szolgáltatót, hogyan és hány emberrel, milyen technikai berendezésekkel, vasráccsal stb. őrzi például az adatközpontjait. Éppen ezért az ilyen rendszerekben tárolt, kezelt stb. adatokat a felhasználónak ennek megfelelően kell védenie (például titkosítottan közlekedtetni, tárolni stb.) A kibernyomozó fizikai védelemmel kapcsolatos információkat csekély eséllyel kap a szolgáltatóktól, jellemzően ilyenek a hazai internet- és/vagy felhőszolgáltatóktól szerezhetők be. Ugyanakkor ezen információk nem is igazán relevánsak számára, hiszen például nem lehet pontosan tudni, hogy az adott adatok mely internetszolgáltatók milyen infrastruktúráján haladtak pontosan keresztül.

A felhasználó felelőssége: A felhasználó ugyanakkor teljes ráhatással rendelkezik a szolgáltatások eléréséhez használt végponti eszköz, leggyakrabban a hordozható infokommunikációs eszközök védelme felett. Így ezek fizikai védelme teljes egészében a felhasználó feladata, ráadásul több veszélyt is megelőzhet, vagy azok kockázatát csökkentheti, ha felelősen végzi ezt a tevékenységet. Megakadályozhatja a készülék eltulajdonítását, így egyrészt elkerülhet egyfajta információvesztést, másrészt azt, hogy illetéktelenek hozzáférjenek az adataihoz. A fizikai felügyeletnek azonban nem csak a készülék elvesztése,

eltulajdonítása és az ezzel járó anyagi és információveszteség miatt van jelentősége. A néhány percre, órára magára hagyott eszköz lehetőséget biztosíthat illetéktelenek számára az eszközön lévő adatokhoz való hozzáférésre, azok lemásolására, vagy valamilyen rosszindulatú szoftver telepítésére is. Ez utóbbival pedig nemcsak a készüléken éppen fent lévő adatokhoz, hanem a felhasználó későbbiekben folytatott kommunikációjához, felvitt adataihoz, mozgási (hely) adataihoz stb. is hozzáférhetnek a támadók. A kibernyomozó a felhasználtól érdemi információkhoz juthat ebben a témában.

A dokumentumbiztonság a PC/SaaS felhőalapú rendszerekben

A szolgáltató felelőssége: A PC/SaaS felhőalapú rendszerekben az esetek 99%-ában kizárólag elektronikus dokumentumokról beszélhetünk, hiszen még a felhasználói szerződést is így fogadják el a felhasználók. Ezek védelméről *Az elektronikus információbiztonság–kiberbiztonság a PC/SaaS felhőalapú rendszerekben* alfejezetben lesz szó. A kibernyomozó ezzel kapcsolatban releváns információkhoz a szolgáltatóktól ritkán juthat, talán még a hazai internet-és/vagy felhőszolgáltatóktól szerezhet be papíralapú szerződések védelmével kapcsolatos információkat – már ha vannak ilyenek egyáltalán.

A felhasználó felelőssége: A felhasználó ugyanakkor teljes ráhatással rendelkezik a saját dokumentumaival kapcsolatban. (Az elektronikus dokumentumok védelméről ebben az esetben is *Az elektronikus információbiztonság–kiberbiztonság a PC/SaaS felhőalapú rendszerekben* alfejezetben lesz szó.) A nála papíralapon (is) keletkező, a PC/SaaS felhőalapú rendszerekben felhasznált, feltöltött stb. dokumentumok védelmét a saját, valamint erre vonatkozó egyéb (például jogszabályi) előírások, szabályok szerint tudja kezelni. A kibernyomozó a felhasználtól ebben a témakörben is érdemi információkhoz juthat.

Az elhárítás a PC/SaaS felhőalapú rendszerekben

A szolgáltató felelőssége: A PC/SaaS felhőalapú rendszerekben a szolgáltatók felelőssége a saját rendszereikkel kapcsolatos elhárító tevékenység végzése, amelyet a legtöbbször valamilyen saját és/vagy vásárolt kibertérből származó fenyegetettségekkel kapcsolatos hírszerzési (*cyber threat intelligence*) szolgáltatás igénybevételével hajtanak végre. Erre a felhasználónak nincs ráhatása, de

még csak rálátása sem, nem szabhatja meg, vagy kérheti számon a szolgáltatót, hogyan és milyen módon végzi, vagy egyáltalán végzi-e ezt a fajta tevékenységet. A kibernyomozó ezzel kapcsolatban releváns információkhoz a szolgáltatóktól ritkán juthat, talán még a hazai internet- és/vagy felhőszolgáltatóktól szerezhet be ilyen jellegű információkat.

A felhasználó felelőssége: A felhasználó ugyanakkor teljes ráhatással rendelkezik a saját adatai, információi felett, így ezekkel, valamint saját magával és/vagy vállalatával kapcsolatban végezhet, végeztethet fenyegetettségekkel kapcsolatos hírszerzési tevékenységet. Ezt kritikus esetekben és jelentős megszorításokkal (amelynek jogi és a szolgáltatókkal kapcsolatos bizonyos információkhoz való korlátozott hozzáférés az oka), de kiterjesztheti a szolgáltatóra is. (Például keresheti, hogy a szolgáltatótól került-e ki bármilyen adat az elmúlt időszakban a dark webre.) Ugyanakkor – néhány nagyvállalattól eltekintve – ma még nem jellemző, hogy ilyen tevékenységet végeznének, végeztetnének cégek, főleg nem magánszemélyek. A kibernyomozó a felhasználótól ebben a témakörben is érdemi információkhoz juthat.

Az elektronikus információbiztonság–kiberbiztonság a PC/SaaS felhőalapú rendszerekben

A PC/SaaS felhőalapú rendszerekkel kapcsolatos információbiztonsági vizsgálatok során ez a legfontosabb témakör.

A szolgáltató felelőssége: A PC/SaaS felhőalapú rendszerekben az elektronikus információbiztonság–kiberbiztonság megteremtése a szolgáltatók felelőssége. Erre a felhasználónak nincs ráhatása, de még csak rálátása sem. A védelemmel kapcsolatos részletes adatok (például használt védelmi eljárások, eszközök, szoftverek pontos típusa stb.) – biztonsági okokból – a szolgáltatók egyik legféltebb információi. Ugyanakkor bizonyos általános információkat a szolgáltatók jól felfogott üzleti megfontolások alapján megosztanak a felhasználókkal, érdeklődőkkel. Ilyen lehet például, hogy a szolgáltató milyen tanúsítványokkal (például ISO 27001) rendelkezik, vagy milyen egyéb biztonsági előírásoknak felel meg (például *NIST Cybersecurity Framework*). A kibernyomozó ezzel kapcsolatban releváns információkhoz legtöbb esetben a szolgáltatók honlapjain juthat, ennél bővebb információkat leginkább a hazai internet- és/vagy felhőszolgáltatóktól tud beszerezni.

A felhasználó felelőssége: A felhasználó ugyanakkor teljes ráhatással rendelkezik a saját adatai, információi és a PC/SaaS felhőalapú rendszerek által nyújtott szolgáltatások igénybevételéhez használt eszközök felett, így azok védelmét a saját, valamint erre vonatkozó egyéb (például jogszabályi) előírások, szabályok szerint tudja kezelni. A kibernyomozó a felhasználótól ebben a témakörben is érdemi információkat szerezhet be.

Ki kell emelni azt is, hogy Magyarországon, de akár külföldön működő kibervédelmi szervezetek – elsősorban a CERT-ek és CSIRT-ek – is szolgálhatnak a kibernyomozó számára releváns információkkal. Éppen ezért adott esetekben célszerű elsősorban a Nemzetbiztonsági Szakszolgálat keretein belül működő Nemzeti Kibervédelmi Intézetet (NKI), az Országos Katasztrófavédelmi Főigazgatóság szervezetében található Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központot (LRLIBEK), vagy a Honvédelmi Minisztérium saját hálózatbiztonsági vészhelyzeteket elhárító csoportját megkeresni. Segítségükkel, rajtuk keresztül kapcsolatot lehet teremteni külföldi kormányzati CERT-ekkel, CSIRT-ekkel is, akiktől a kibernyomozó szintén hasznos információkhoz juthat.

Összefoglalás

Jelen fejezet bemutatta az információbiztonság alapjait, részterületeit, tisztázta az ezzel kapcsolatos legfontosabb fogalmakat, valamint azok összefüggéseit. Ismertette, hogy az infokommunikációs hálózatokban hogyan lehet értelmezni az információbiztonság egyes részterületeit, majd a nyilvános számítási felhő és szoftver mint szolgáltatás típusú rendszereken (PC/SaaS felhőalapú rendszerek) keresztül bemutatta a szolgáltató és a felhasználó információbiztonsággal kapcsolatos feladatait és felelősségét, valamint azt, hogy a kibernyomozó a számára releváns információkat mely forrásokból gyűjtheti be.

Az egyes részeket olyan szintig mutattuk be, amely lehetővé tette a legfontosabb alapelvek és PC/SaaS felhőalapú rendszerek bizonyos működési sajátosságainak megértését, és az abból kinyerhető, a nyomozó számára fontos információk forrásainak bemutatását. Amennyiben a kibernyomozó a fentiekben leírtaktól eltérő infokommunikációs rendszerrel találkozik, akkor a fent leírtak megfelelő – az adott rendszer sajátosságainak figyelembevételével és az alapokat ismerve a megfelelő szakemberrel történt konzultációt követő – adaptálásával

a többi rendszerre ki tudja terjeszteni, át tudja alakítani, így a szükséges elemzést el tudja végezni.

Az infokommunikációs hálózatokkal kapcsolatos információbiztonsági nyomozói feladatok során a kibernyomozók a legritkább esetben találkoznak rutinszerű ügyekkel, feladatokkal. Ez azt jelenti, hogy egy adott ügy megoldásához kreativitás, a korábbiaktól eltérő információigénylési és -feldolgozási metodika, valamint ehhez az adott infokommunikációs rendszer bizonyos ismerete szükséges. Ennek megfelelően mindig érdemes és célszerű a lehetőségekről a felhasználó, de lehetőség szerint a szolgáltató erre a célra dedikált – általában biztonsági – szakembereivel konzultálni. Ugyancsak célszerű adott esetben a Nemzeti Kibervédelmi Intézetet (NKI), és/vagy a Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központot (LRLIBEK) és/vagy a Honvédelmi Minisztérium saját hálózatbiztonsági vészhelyzeteket elhárító csoportját megkeresni, akik a sok hasznos információ mellett lehetővé teszik a külföldön működő kibervédelmi szervezetek megkeresését, amelyek szintén szolgálhatnak a kibernyomozó számára releváns információkkal. Külföldi infokommunikációs szolgáltató esetén ugyanis a szükséges információk beszerzése sokszor nehézségekbe ütközik, ebben segíthetnek ezek a szervezetek.

Az infokommunikációs eszközök

Bevezetés

Jelen fejezet a kibernetizáció, illetve az informatikai nyomozó szakirányok oktatásában *Az infokommunikációs eszközök* címet viselő kurzus tananyagának gerince. Számos helyen terjedelmi korlátok miatt a vonatkozó szükséges tananyagok a jelen fejezetben, illetve az oktató által megküldött internetes linken elérhetők.

Bemutatjuk az infokommunikációs eszközök csoportjait hardver- és szoftveroldalról, és gyakorlati feladatok segítségével a kurzus célja, hogy a hallgató ismerje a különféle eszközök belső működésének elvi alapjait, azok felépítését, és képes legyen azok működtetésére.

A tananyag egymásra épülése okán az eszközök megismerését követően azok hálózataival ismerkedhet meg a hallgató annak érdekében, hogy azok alapot adjanak a későbbi kurzusokhoz – amelyek a kibertérhez kapcsolódó nyomozások eredményességét támogatják.

Kérdésként merülhet fel, hogy mi az infokommunikáció, mi az információ- és kommunikációtechnológia (IKT)?

Az infokommunikáció az Európai Unió hivatalos szóhasználatában az információtechnológia és az elektronikus hírközlés konvergenciáját, integrálódását fejezi ki. Magyarország 2014–2020 közti időszakra kiadott Nemzeti Infokommunikációs Stratégiájában infokommunikáció alatt mindazon információtechnológiai és elektronikus hírközlési eszközöket, technológiákat és alkalmazásokat, illetve azok használatát kell érteni, amelyek az egyén, a vállalkozás és az állam szintjén egyaránt értelmezhető minőség-, hatékonyság- és eredményességjavulást eredményeznek.⁵⁵

Bizonyos értelmezésben az IKT fogalma: olyan eszközök, technológiák, szervezési tevékenységek, innovatív folyamatok összessége, amelyek az információ- és a kommunikációközlést, -feldolgozást, -áramlást, -tárolást, -kódolást elősegítik, gyorsabbá, könnyebbé és hatékonyabbá teszik. Az IKT-t olyan médiának tekinthetjük, amely lehetővé teszi az interakció és a kommunikáció

⁵⁵ Nemzeti Infokommunikációs Stratégia 2014–2020.

különböző típusait: a gép-gép, az ember-gép és különösen az ember-ember közötti interakciót.⁵⁶

Az *információ- és kommunikációtechnológia* fogalmat gyakran használják az információtechnológia szinonimájaként (IT), azonban ez egy sokkal speciálisabb szakkifejezés, amely az egységes kommunikáció szerepére, a telekommunikáció integráltságára, számítógépekre és audiovizuális rendszerekre fókuszál. A fogalom lényege, hogy ezen eszközök felhasználói képesek hozzáférni, tárolni, továbbítani, valamint kezelni az információkat.⁵⁷

Témánkat ennek megfelelően nem szűkítjük csak a személyi számítógépekre, hanem annál szélesebb körben vizsgáljuk a hardverelemeket és az azokat üzemeltető szoftvereket. Az IKT-eszközökhöz sorolt hálózati eszközök, valamint a telekommunikációs és hírközlési eszközök hardver- és szoftveroldáról is későbbi könyvfejezetek és kurzusok tárgyai lesznek.

A témánk szempontjából lényeges IT-ICT-eszközök:

- személyi számítógépek (asztali/desktop, laptop, tablet);
- mobil telekommunikációs eszközök (mobiltelefonok, IP-telefonok);
- játékkonzolok;
- navigációs berendezések;
- hálózati eszközök (szerverek, routerek, swichek, repeaterok, NAS-ok stb.);
- műholdvevő berendezések beltéri egységei;
- különféle berendezések, ipari létesítmények vezérlő számítógépei (gépjárművek vezérlő és multimédia rendszerei, orvostechnikai eszközök, gyártósori robotok, SCADA rendszerek,⁵⁸ közlekedési jelzőlámpák, munkagépek vezérlése stb.);
- automatikus értékesítésre szolgáló berendezések (tömegközlekedési jegy-, parkolójegy-, élelmiszer- stb. automaták);
- ATM-berendezések;
- kriptovaluta-bányászó céleszközök;
- a felsoroltakkal jelentős átfedésben lévő csoport az Internet of Things (IoT-) eszközök (RFID-azonosítórendszerek, ügyfélirányító rendszerek,

⁵⁶ Molnár György: *Az IKT-val támogatott tanulási környezet követelményei és fejlesztési lehetőségei*. 2008. 261.

⁵⁷ Sallai, Gyula: [Defining Infocommunications and Related Terms](#). *Acta Polytechnica Hungarica*, 9. (2012), 6. 5–15.

⁵⁸ Pletl Szilveszter – Kincses Zoltán: *Supervisory control and data acquisition. SCADA PLC és SCADA rendszerek*. 2014.

hordható okoseszközök, háztartási berendezések IoT-funkciókkal, különféle szenzorok [időjárás, közúti forgalom] stb.).

A felsoroltak közül két berendezéssel szükséges súlyozottan foglalkozni: a személyi számítógépekkel, valamint a mobiltelefon-készülékekkel, mivel: a működést tekintve a legjellegzetesebb ismeretek itt sajátítandók el; a legelterjedtebbek; bűnüldözési szempontból ezekből a berendezésekből nyerhető a legtöbb releváns információ.

Elméleti alapok

Mi a digitális? Mi a bináris? Mi a hexadecimális?

Sok esetben az átlagfelhasználó a *bináris* és *digitális* jelzőket szinonimaként használja, azonban ez a két fogalom nem azonos.

A *bináris* – mint jelző/prefixum – azt jelenti, hogy egy adott dolog két értéket képes felvenni. Jelentése az informatikában megegyezik a kettes számrendszerrel.⁵⁹ A kettes számrendszer vagy bináris számrendszer olyan helyiérték-jelölő számrendszer, amely két számjeggyel ábrázolja a számokat, az arab számírásban a 0-s és az 1-es jegyekkel. Mivel az elektronikus áramkörökben a számrendszerek közül a kettest a legegyszerűbb megvalósítani és vizsgálni, a modern számítógépekben, és gyakorlatilag bármely olyan elektronikus eszközben, amely valamilyen számítást végez, szinte kivétel nélkül ezt használják.

Az informatikán kívüli világban a tízes (decimális) számrendszer az elterjedt. Ez vélhetően azért alakult így, mert az embereknek 10 ujjja van a kezén.⁶⁰

Ha tehát egy jelrendszerben mindössze két elemi jelet használunk, akkor bináris jelrendszerről beszélünk.⁶¹

⁵⁹ Bár két lehetséges jelentéstartalom megjelenik egy elektromos kapcsolónál is, de más tudományterületeken is alkalmazzák, mint például a politológiában. Bővebben lásd Pokol Béla: *Politikaelmélet: Társadalomtudományi trilógia III.* Budapest, Századvég, 2004.

⁶⁰ Megjegyzendő, hogy az ujjainkon is képesek vagyunk a kettes számrendszer szerint számokat mutatni egészen 2-nek a 10. hatványán 1024-ig. Ha a jobb oldali első ujjunk van nyitva, az az 1, ha az első kettő, az a három. (Vajon hogyan jelöljük a 4-et és a 84-et...?)

⁶¹ Kettes számrendszerből tízes számrendszerbe váltás: jobbról balra haladva minden egyes számjegy a 2 eggyel nagyobb hatványát fejezi ki. A kettes számrendszerben ábrázolt szám értékét úgy kapjuk meg, hogy összeadjuk azokat a kettőhatványokat, amelyek helyiértékénél 1 áll, vagy használjuk a Windows számológépének programozó modulját.

A következő kifejezés a *digitális*, ami annyit jelent: valamely változó jelenségnek vagy fizikai mennyiségnek diszkrét (nem folytonos), megszámlálhatóan felaprózott, s így számokkal meghatározható, felírható értékeinek halmaza. Az informatikában ez a jel.

A digitális rendszerek leginkább számokat (leginkább bináris számokat) használnak bevitelhez, feldolgozáshoz, átvitelhez, tároláshoz vagy megjelenítéshez – ellentétben az analóg rendszerekkel, amelyek az értékek folytonos spektrumát használják –, ilyenek a nem numerikus szimbólumok, a betűk vagy ikonok.

Az informatikában az információkat konvertálják át bináris számokká. Ilyenek például a digitális hang(zás) és a digitális fényképezés is. A digitális adatátvivő jelek az elektronikus vagy optikai impulzus két lehetséges értéke közül az egyiket vehetik fel: a logikai 1 (van impulzus) vagy 0 (nincs impulzus) értékeket.

Nem minden digitális jel szükségszerűen bináris. Például a füstjeleknél a takaróval létrehozott füstgomolyagok, a morzekód 5-féle jele, vagy a Braille-írás jelei, amelyek 6 darab bites kódba képezik le a betűjeleket – tehát mindegyik számokká alakítja az információt –, így digitálisak, de nem binárisak.

A bináris számrendszerben az adatokból képezett számok kimondása, leírása meglehetősen nehéz volna az ember számára, de ez a számítógépek szinte kizárólagos nyelve.

Az információ mértékegysége a bit (*binary digit*). Egy biten kétféle érték lehetséges. Jel vagy jel hiánya. A bithez kapcsolódóan fontos megjegyeznünk, hogy a számítástechnikában a 8 bites gépi szót a byte-ot (bájt) mint önállóan is értelmezhető mértékegységet használjuk.

Az informatikában a bináris jelek mindkét alapegységét használjuk, a bitet és a bájtot is.

Az információáramlás sebességét a gyakorlatban adatátviteli sebességnek nevezzük. Leggyakrabban használt mértékegysége: bps (*bit per secundum*), amellyel az egy másodperc alatt továbbított bitek számát mérjük. Többszörösei:

- Kbps (ezer bit per szekundum),
- Mbps (millió bit per szekundum),
- Gbps (milliárd bit per szekundum),
- Az adatmennyiségnél viszont a bájt az irányadó mértékegység és annak 2^{10} (1024) hatványai.

1. táblázat: Byte-mértékegységek

Byte-mértékegységek					
SI ⁶² -prefixumok			Bináris prefixumok		
Név (Szimbólum)	SI Standard	Értéke	Név (Szimbólum)	Értéke	
kilobyte (kB)	$10^3 = 1000^1$	2^{10}	kibibyte (KiB)	2^{10}	
megabyte (MB)	$10^6 = 1000^2$	2^{20}	mebibyte (MiB)	2^{20}	
gigabyte (GB)	$10^9 = 1000^3$	2^{30}	gibibajt (GiB)	2^{30}	
terabyte (TB)	$10^{12} = 1000^4$	2^{40}	tebibajt (TiB)	2^{40}	
petabyte (PB)	$10^{15} = 1000^5$	2^{50}	pebibajt (PiB)	2^{50}	
exabyte (EB)	$10^{18} = 1000^6$	2^{60}	exbibyte (EiB)	2^{60}	
zettabyte (ZB)	$10^{21} = 1000^7$	2^{70}	zebibyte (ZiB)	2^{70}	
yottabyte (YB)	$10^{24} = 1000^8$	2^{80}	yobibyte (YiB)	2^{80}	

Forrás: a szerző szerkesztése

Fontos, hogy az SI-standard szerinti 10-es hatványok és a hozzájuk kapcsolódó kilo- (ezer), mega- (millió), giga- (milliárd) előtagok mindig 1024-szeresen emelkednek. Ez a különbség a terabájtnál már 10%, a yottabájtnál már 20%-os különbséget eredményez.⁶³

A *hexadecimális számok*. A számítástechnikában gyakran használják a tizenhatos – azaz hexadecimális (zsargonban: hexa) – számrendszert, amely az informatika kulcsfontosságú számrendszere a kettes számrendszer mellett. A tizenhatos számrendszer a 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 számjegyeken kívül az A, B, C, D, E, F betűket (vagy ezeknek kisbetűs megfelelőjét; mindkettő használat megengedett) használja, ezek segítségével ábrázolja a számokat.

A 0–9 számjegyek használata értelemszerű (azaz: a tízes számrendszernek megfelelő), az A számjegy 10-et, a B számjegy 11-et, a C számjegy 12-t, a D számjegy 13-at, az E számjegy 14-et és az F számjegy 15-öt jelöl (ez összesen 16 számjegy, tekintettel arra, hogy a nulla az első).

Egy hexadecimális szám éppen négy bitet (1 nibble-t) képvisel. Így tehát egy bájtnak értéke kifejezhető éppen egy kétjegyű hexadecimális számmal (a 00H – FFH intervallumban). Ezzel az ábrázolással egyszerűbb a bitsorozatot leírni, könnyebb olvasni, és nehezebb eltéveszteni.

⁶² Nemzetközi Mértékegységrendszer, röviden *SI* (*Système International d'Unités*).

⁶³ Lambert Miklós: *Bináris prefixumok. Műszerügyi és Méréstechnikai Közlemények*, 37. (2001), 67.

Az adatok tárolása

Az információ legkisebb, önállóan még értelmezhető részét elemi adatnak nevezzük. A számítógép által feldolgozott elemi adatokat három csoportba soroljuk: 1. számok, 2. szöveges információk, 3. logikai típusú adatok (igaz-hamis értékű).

A számítógépekben az információ kódolására különböző kódrendszereket alkalmaznak. A kódolás során egy jelkészlet elemeit megfeleltetik egy másik jelkészlet elemeinek.

A karakter (betűhely) egy leütés: egy betű, egy szám, egy írásjel, egy szóköz összefoglaló neve. Ezt tekintjük az információ egységének. A gépi ábrázolásban a karakterek esetében minden karakternek megfeleltetnek egy számot, a számítógép ezt a számot tárolja. A karakterek tárolásához sokféle kódrendszert alakítottak ki. A két legelterjedtebb kódkészlet az ASCII és az UNICODE.

Az ASCII kódtábla (*American Standard Code for Information Interchange* – ASCII [kiejtve: eszki]) szöveges adatokhoz használt, nemzetközileg egységes, szabványos 1 bájtos (8 bites) karakterkódolási séma, amely 256 jelet tartalmaz (0–255 között). Például a @karakter hexa kódja: 40, decimális kódja: 64.

Az UNICODE kódtábla egy nemzetközileg egységes 16 bites karakterkódolási szabvány. Valamennyi nép valamennyi jelét tartalmazza. Ez már 65 536 lehetséges jelet tartalmaz.

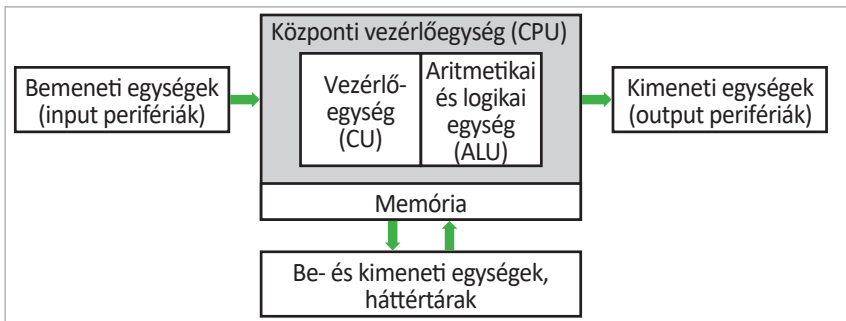
A személyi számítógépek felépítése

Az első mai értelemben vett (elektronikus) digitális számítógépnek az Atanasoff–Berry Computert (ABC) nevezzük 1937–1942-ből.

A Neumann-architektúra (7. ábra), más néven a Neumann-modell egy számítógép-architektúrára kidolgozott modell, Neumann János és társai 1945. június 30-án publikálták. A Neumann-architektúra szerint egy digitális számítógép a következő egységekből áll:

- aritmetikai-logikai egység (regiszterek);
- vezérlőegység, ez tartalmazza a programszámlálót és az utasításregisztert;
- operatív tároló az adatok és az utasítások tárolására – memória;
- háttértár és a perifériákhoz tartozó be- és kiviteli mechanizmusok – input-perifériák és output perifériák.

A Neumann-architektúra mára a tárolt programú számítógép fogalmává vált.



7. ábra: A Neumann-architektúra

Forrás: a szerző szerkesztése

A központi vezérlőegység – a processzor

Részei:

- Vezérlőegység (*control unit* – CU) gondoskodik az utasítások lehívásáról, értelmezéséről és végrehajtásáról.
- Aritmetikai-logikai egység (*arithmetic logical unit* – ALU) végzi el a processzor regisztereiben elhelyezett adatokkal az utasításokban kijelölt aritmetikai (számtani) és logikai műveleteket. Eredetileg a logikai műveletek (például *és/vagy*, *kizáró-vagy*, *tagadás* stb.) mellett kizárólag összeadásra volt képes, de a mai processzorok már a kivonás, szorzás és osztás mellett ezeknél bonyolultabb műveletekre is képesek.
- A regiszterek a processzor belső tárolóelemei, amelyeket „munkamemóriaként” használ. Az aktuális utasításhoz éppen szükséges adatok és memóriacímek tárolódnak itt.

A processzor egyik legfontosabb tulajdonsága az órajel, amelynek ütemére végzik feladataikat a processzorok. Amikor megkapja egy elektronikus jel formájában az órajelet, akkor elvégzi a soron következő műveletet, amikor megkapja a következő jelet, akkor a következő műveletet végzi el. Egy másodperc alatt egy mai processzor egysége több milliószor kap jelet.

A személyiszámítógép-piacon manapság két nagy processzorgyártó vetekszik egymással, az Intel és az AMD. Az Intel a nagyobb, belőle vált ki az AMD. Mind a két processzorgyártónak nagy részesedése van a videokártyák piacán is.

Az Intel-processzorok jelölésével kapcsolatban például az Intel Core i7 7500 U azt jelöli, hogy az Intel Core a márkajelzés, az i7 egy brandváltozó, amely a termékcsaládot jelöli, a négyjegyű szám első karaktere a generációt mutatja, a másik három magát a típust azonosítja, a mögötte lévő betű(k) pedig azt, hogy milyen tulajdonsággal ruházták fel a processzort.

Brandek:

Intel Core (M/i3/i5/i7),

- Intel Pentium (desktop processzorok 2 maggal),
- Intel Celeron (gyengébb desktop processzorok),
- Intel Atom (például tableteknél, MID-eszközöknél használt processzor),
- Intel Xeon (szerverekbe szánt termékek).

A legnagyobb körben használt brand az Intel Core. A többi három szám minél nagyobb, annál erősebb a chip, nagyobb az órajel, a cache⁶⁴ stb.⁶⁵ A vállalat 2020-ban tart a 10. generációnál,⁶⁶ így Core i9-10900K elnevezésben az Intel a Core i) márka alatt a 10. generációs 900-as típusú asztali gépbe szánt szorzószármentes processzor.

Az AMD-processzorok

Az AMD-processzorok esetében az elmúlt időszakban x86-os architektúra (tipikusan 32 bites szoftverekhez) szerinti K5, K6, K7 széria, majd az x86-64 archi-

⁶⁴ Gyorsítótár, amely memóriaként szolgál a processzor aktuális működésének támogatására. Jellemző a processzorral egybeépítve. A processzor először a gyors cache-ből próbálja elérni a szükséges adatot, és ha ott nem találja, akkor keresi a központi RAM-memóriában. Mérete a számítási kapacitást növeli.

⁶⁵ Az utótagokat tekintve generációktól függ, hogy miből melyet adnak ki; például az 5. generációnál voltak még C és R végű processzorok, K – szorzószármentes, tuningolható asztali processzor, T – gyengébb, kevesebbet fogyasztó asztali processzor, H – erősebb grafikus képességekkel bíró mobil processzor, HK – erősebb grafikus képességekkel bíró, szorzószármentes mobil processzor, HQ – erősebb grafikus képességekkel bíró, quad-core mobil processzor, Y – erősen gyengített, energiatakarékos mobil processzor, U – még jobban gyengített mobil processzor. Az Intel Core M típusú processzoroknál legfontosabb dolog az energiahatékonyság, tehát alapvetően igen alacsony órajelen működnek, viszont agresszív turbóval látták el őket, így ha kell, tudnak teljesíteni.

⁶⁶ Itt már a processzoron belüli áramkörök 10 nm-es vastagságúak. Egy nanométer a méternek egymilliárdod része. (Érdekesség, hogy például az emberi köröm egy másodperc alatt 1 nanométert nő.)

tektúra szerint (64 bites szoftverekhez) K8, K9, K10 sorozatok jelentek meg. A K10 sorozaton belül Bulldozer, Bobcat, Jaguar, Zen architektúracsoportok jelentek meg. Ezek mindegyikén belül számos fantázianevet adtak az egyes processzoroknak attól függően, hogy laptopba, asztali vagy mikroszerverekbe tervezték-e.

A 2010-es évek végéig az AMD eladásai sokkal alacsonyabbak voltak az Intelnél, de aztán a RYZEN processzorcsalád (Athlon, R3, R5, R7,⁶⁷ R9) versenyképes termékekkel jelentkezett, ezzel piaci versenyt teremtve.

Az AMD-processzorok nevében a G elnevezés azt jelenti, hogy grafikai chippel ellátott, míg az F sorozat ilyen chippel nem rendelkezik.

A két processzorgyártó közti verseny jelen sorok írásának időszakában is zajlik. Az optimalizált felhasználói választást a célzott felhasználási módok határozzák meg.⁶⁸

A mobiltelefonokban használt processzorok órajele, illetve számítási kapacitása az elmúlt évek felhasználói igényeinek változásával hatalmas fejlődésen ment keresztül, de ezen processzorokat egy másik jegyzetben ismertetjük.

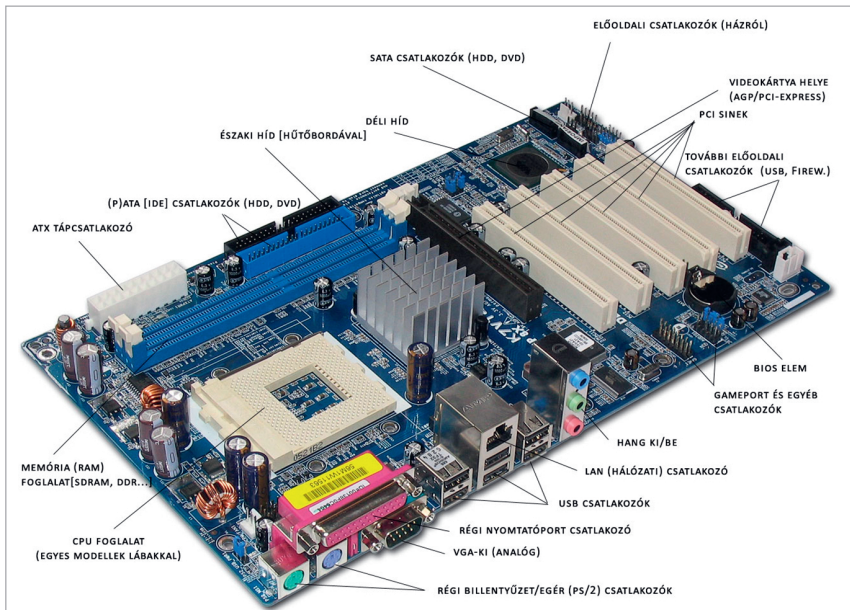
Az alaplap

Az alaplap a központi vagy elsődleges áramköri lapkája egy számítógépes vagy más összetett elektronikai rendszernek.

A számítógép elektronikus elemei az alaplapra vannak építve. Az alaplap egy többrétegű nyomtatott áramköri lap, amelyen az egyes elemek fogadására több különböző méretű és alakú csatlakozó, illetve néhány előre beépített eszköz helyezkedik el. Ezek az elemek, illetve a kialakított csatlakozók eleve meghatározzák, hogy az alaplap milyen processzort tud fogadni, milyen frekvencián dolgozik, mekkora a RAM-memória, hány és milyen fajtájú bővítőkártyahely található rajta, milyen a felhasználható memória típusa és maximális mérete stb. Az alaplapon olyan csatlakozók is találhatók, amelyek a „külső” kapcsolatokra szolgálnak: tápfeszültség, billentyűzet, egércsatlakozó, gombakkumulátor helye a CMOS RAM számára. Ugyancsak idekapcsolódnak a számítógép előlapján található jelzőfények érintkezői, a házon található kapcsolók stb. (lásd 8. ábra).

⁶⁷ Ezek jellemzően az Intel core i3, i5, i7, i9 processzorcsaládnak felelnek meg sok paraméterükben.

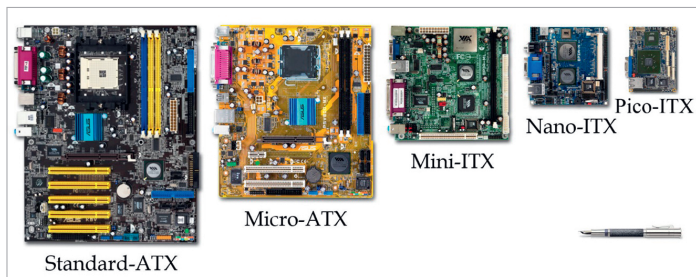
⁶⁸ Azaz nem mindegy, hogy videószerkesztéshez, mérnöki programokhoz vagy számítógépes játékokra használjuk-e.



8. ábra: Az alaplap

Forrás: a szerző szerkesztése

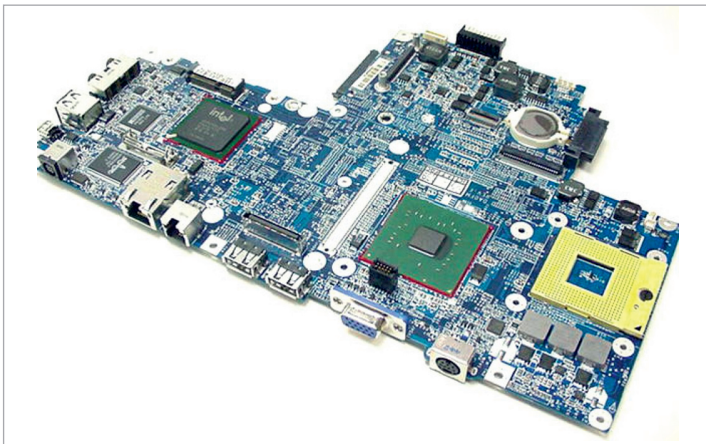
Alaplapgyártók nagy számban működnek a világon: ASRock, Asus, Biostar, EVGA Corporation Gigabyte Technology, MSI (*Micro-Star International*) stb. Méretüket illetően a 9. ábra nyújt segítséget:



9. ábra: Az alaplapok mérete

Forrás: www.educba.com/types-of-motherboard/

A laptopokon belül azonban az alaplapok jellemzően nem négyzet alakúak, mivel azok az egyes laptopházak belső kialakítása – azaz a vastagabb belső alkatrészek – vagy a hűtés miatt nagyon változó formában működnek. Példa a szabálytalan laptopalaplapp-formára a 10. ábra.

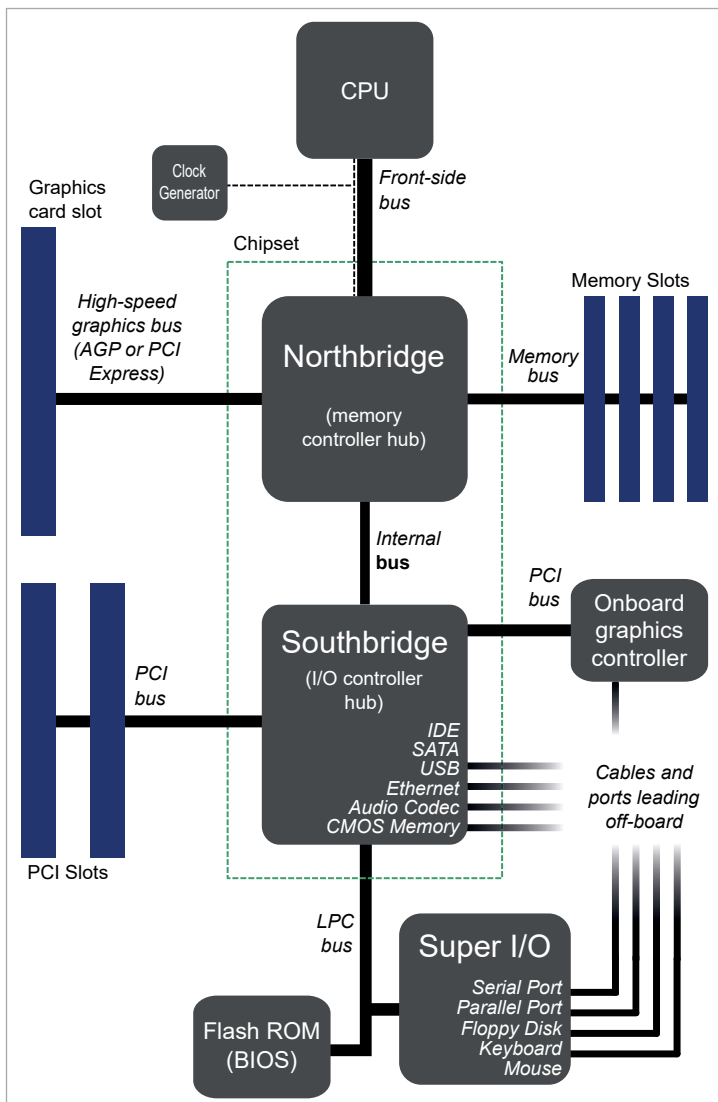


10. ábra: Szabálytalan laptopalaplapp

Forrás: www.indiamart.com/proddetail/laptop-motherboard-repairs-14273562288.html

Az alaplapok sematikus vázát a 11. ábra mutatja be. Az ábrában szereplő angol kifejezések:

- CPU (Central processing unit) – központi feldolgozóegység, processzor
- Clock generator – órajel generátor
- Front side bus (FSB) – földali adatsín
- Chipset – rendszervezelési feladatokat ellátó áramkörös családok
- High-speed graphics bus (AGP or PCI Express) – nagy sebességű grafikus adatsín
- Graphics card slot – grafikus kártya csatló
- Memory bus – memória adatsín
- Internal bus – belső adatsín
- PCI bus (Peripheral Component Interconnect) – a CPU és a perifériák összekötésére szolgáló processzorfüggetlen adatsín
- Onboard graphics controller – alaplappra integrált videomegjelenítő áramkör
- LPC (Low Pin Count) bus – busz alacsony átviteli sebességű eszközöknek a CPU-val való összekötésére szolgáló adatsín
- Flash ROM (BIOS – Basic Input Output System) – alapvető bemeneti-kimeneti rendszer
- Cables and ports leading off-board – kilepő kábelek és vezetékek
- Northbridge – északi híd: a jelölt komponenseket összekötő tokozás
- Southbridge – déli híd: a jelölt komponenseket összekötő tokozás
- Super I/O – bemeneti kimeneti interfész (soros és párhuzamos port, floppy meghajtó, billentyűzet, egér)



11. ábra: Az alaplapok sematikus váza

Forrás: <http://el-gibbor.synthasite.com/my-assignments-2.php>

A fenti ábrában szereplő PCI (*peripheral component interconnect*) a CPU és a perifériák összekötésére szolgáló processzorfüggetlen adatsín (illetve „busz”).

A PCI slotokon keresztül párhuzamos port csatlakozót, hangkártyát, hálózati kártyát, játék port csatlakozót stb. lehetett az alaplaphoz illeszteni. A jelentősége az elmúlt időszakban megszűnt.

A PCIe (express) leginkább grafikus kártyák fogadására alkalmas, és magasabb adatáramlást tesz lehetővé, mint a PCI busz vagy a korábban használt AGP-csatlakozó (*accelerated graphics port*).

PCIe csatlakozókból az alaplapon jellemzően x16-os és x1-es van.⁶⁹ Míg a PCI 1.0 generáció 1x csatlakozón 250MB/s-ra volt képes, addig a PCIe 4.0 2000MB/c sebességre képes.⁷⁰

A ROM BIOS a bekapcsoláskor végrehajtandó programot tartalmazza.

A BIOS (*basic input output system* [Alapvető bemeneti-kimeneti rendszer]) a számítógép szoftveres és hardveres része közötti interfész megvalósítására szolgál.⁷¹ Fizikailag az alaplapon lévő BIOS, az egyes bővítőkártyákon található BIOS és ezek eszközmeghajtói (*driver*ek) együtt alkotják a számítógép BIOS-át. Ezek közül az alaplapi BIOS-a a BIOS legfontosabb része, mert ez tartalmazza az alapvető konfigurációs beállításokat és hajtja végre a diagnosztikai ellenőrzéseket.

A BIOS-t egy, az alaplapon elhelyezkedő integrált adattároló-áramkör tartalmazza (a régebbi típusokban ROM-ba égetve, később EEPROM, manapság Flash RAM-ban). A BIOS chipjének a kapacitását megabitekben (Mb) mérjük, egy chip általában 1–4 Mb memóriát tartalmaz. Két része van: fix rész, variábilis rész.

Annak érdekében, hogy biztosítsuk a számítógép helyes működését, a BIOS-nak ismernie kell a gép paramétereit, valamint a jelenlegi konfigurációt. Ez az információ egyrészt magába a BIOS-ba van bekódolva, másrészt a CMOS RAM (complementary metal-oxide semiconductor RAM) tárolja. A CMOS⁷² egy digitális integrált áramkörépítési technológia, amely az elektrosztatikus feszültségre is nagyon érzékeny. Táplálását akkumulátor vagy elem segítségével oldják meg. Ez is az alaplapon található. Ennek a rendszernek köszönhető, hogy a CMOS adatai a gép kikapcsolása után sem tűnnek el.

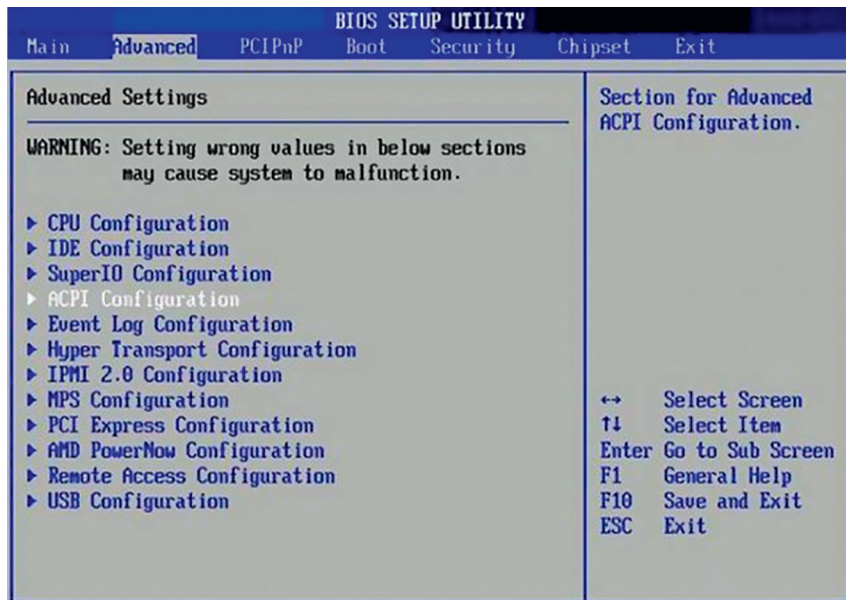
⁶⁹ Az x2, x4, x8 jelentősége nem olyan nagy, ritkábban találkozhatunk vele.

⁷⁰ Tervezés alatt áll a PCIe 6. verziója is, amely x16 csatlakozón elvileg 126GB/s-ra lesz képes.

⁷¹ Lásd: www.drivereasy.com/knowledge/how-to-enter-bios-on-windows-10-windows-7/

⁷² Complementary metal-oxide semiconductor jelentése: komplementer fém-oxid félvezető.

A BIOS tulajdonképpen egy firmware,⁷³ amely jellemzően grafikus felületen biztosít lehetőséget a számítógép alapbeállításaira. Az egyes gyártók eltérő BIOS-okat alakítottak ki, de a menürendszerek hasonlóak.



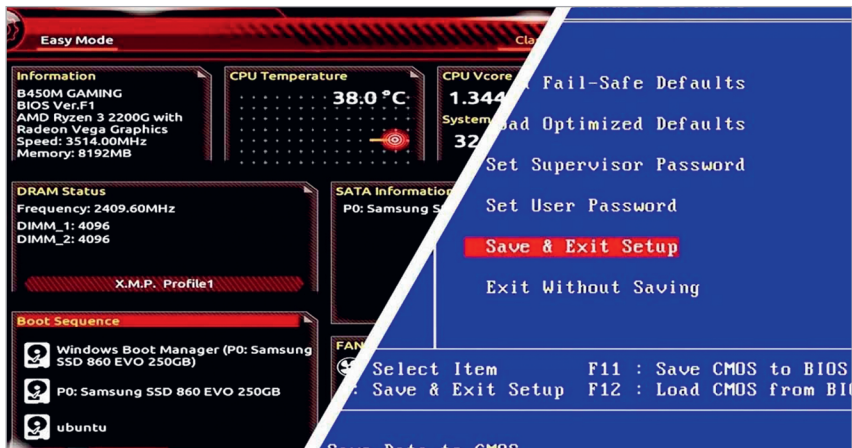
12. ábra: Belépés a BIOS-ba

Forrás: <https://technewspedia.com/configure-bios-to-boot-windows-7-from-usb-guide-%E2%96%B7-2020/>

A BIOS menüjébe csak a gép bootolása során lehetséges belépni, gyártónként eltérő módon, de a Del, F1, F2, F3, ESC billentyűgombok lenyomásával. Ha Win 8, 10 operációs rendszer működése során nem jön fel bootoláskor a boot menü, akkor kikapcsoláskor a shift billentyű lenyomása után a következő induláskor megjelenik a boot menü, és választható a BIOS-belépéshez használható billentyű.

⁷³ Az elektronikai rendszerekben és a számítástechnika területén firmware alatt azokat a rögzített, többnyire kis méretű programokat és/vagy adatstruktúrákat értjük, amelyek különböző elektronikai eszközök vezérlését végzik el. Nincs éles határ a firmware és a szoftver között.

Az elavultnak számító BIOS utódjaként 2011-től az EFI (*extensible firmware interface*), majd 2014-től az UEFI (*unified extensible firmware interface* [egységes bővíthető firmware interfész]) jelenik meg, amely már támogatja a grafikus megjelenést és a Secure Boot opciót, amely csak elektronikus aláírással ellátott kódot enged betölteni, ezáltal sokkal biztonságosabb.⁷⁴ A megjelenítés különbségeit mutatja a 13. ábra.



13. ábra: A megjelenítés különbségei

Forrás: <https://itigic.com/uefi-history-and-characteristics-of-this-interface-for-pc/>

Az alaplapok egyik legfontosabb tulajdonsága a processzor/CPU tokozása, foglalatja.

Az egyes processzorgyártók egyes processzorcsaládjaiknak más és más foglalatot követelnek meg. Eszerint az elmúlt időszak gyakrabban használt foglatai: LGA1151, Socket H4, Socket AM2, Socket SP3, Socket TR4, LGA 2066, Socket sTRX4 stb.

Ezek a processzoron elhelyezett csatlakozótüskék száma, kialakítása, sűrűsége és a kapcsolat sebessége alapján eltérőek.

⁷⁴ Online: <https://arstechnica.com/information-technology/2016/08/microsoft-secure-boot-firmware-snafu-leaks-golden-key/> és <https://how2do.org/how-to-update-the-pc-bios-uefi>

A RAM-memória

Az alaplapok másik fontos tulajdonsága az elhelyezhető RAM-memória foglalta.⁷⁵

A RAM (*random access memory* [tetszőleges hozzáférésű memória, közvetlen hozzáférésű memória, véletlen hozzáférésű memória, bár ez utóbbi helytelenül terjedt el]) egy véletlen elérésű írható-olvasható adattároló eszköz. Az elnevezés némileg félreérthető; a RAM-ba nem tartozik bele a szintén véletlen elérésű, csak olvasható memória, a ROM. A RAM tárolja a CPU által végrehajtandó programokat és a feldolgozásra váró adatokat. Az adatok csak addig maradnak meg benne, amíg a számítógép feszültség alatt van: kikapcsoláskor a benne tárolt adatok elvesznek. Mivel a RAM jóval lassabb, mint a processzor, ezért a processzorban saját, gyors memória is van, a korábban említett cache.

A magyar *véletlen elérés* kifejezés nem pontos, hiszen a memória elérése nem véletlenszerűen, hanem pontos címzések alapján történik, az angol *random* szó itt arra utal, hogy egy adott memóriarész elérésének gyorsasága független az elhelyezkedésétől⁷⁶ (ellentétben például egy merevlemez adattárolással, amikor az egyes pozícióktól a távoli adatokat hosszabb idő elérni).

A RAM-memóriák korábban használt típusai voltak 1995 előtt az SRAM (*static random-accessmemory*), majd 2001-ig fejlesztették a DRAM-ot (*dynamic random-accessmemory*), később az SDRAM (*synchronous dynamic random-accessmemory*), azaz szinkron dinamikus véletlen hozzáférésű memória. Ennek továbbfejlesztett változata a DDR SDRAM (*double data rate SDRAM*), azaz dupla adatátviteli sebességű SDRAM.

A DDR-memória megjelenése 2000-ben történt. 200–400 MHz működési frekvenciával működött. Majd a DDR2 a 2003. évben jelent meg, és 400–1066 MHz működési frekvenciára képes. A 2007. évben megjelent DDR3 már 800 MHz-től 2133 MHz, majd a 2014-től induló DDR4 generáció 1600 MHz működési frekvenciától használható. 2020-ban a kereskedelmi forgalomban kapható leggyorsabb DDR4-es memória 4600 MHz működési frekvenciára képes.

⁷⁵ Az 1950–1960-as évek mágneses elven működő közvetlen hozzáférésű memóriáinak egyik típusa volt a ferritgyűrűs memória, de jelentősége az 1970-es években elenyészett.

⁷⁶ Mike Meyers: *PC hardver és karbantartása*. Budapest, Panem, 2004.

A DDR-memóriákkal kapcsolatban meg kell említeni a GDDR3 (*graphics DDR3*) memóriát, ami nagyobb sávszélességet biztosítani képes memóriaszabvány. Grafikus kártyákon használták, csak integrált formában érhető el. Úgyszintén csak integrált formában elérhető el a GDDR5-memória, amelyet a grafikus kártyák mellett használnak még processzorok mellett is (például a PlayStation 4-ben). A GDDR5-memória kiépítéstől és modelltől függően körülbelül 50–150 GByte/másodperces sebességet tesz lehetővé.

Tápegység

Bár nem tűnik fontosnak az áramellátás biztosításáról szót ejteni, hisz az elektromos hálózatra illesztve a készülékek működnek, de néhány tulajdonságát fontos figyelembe venni a működés során.

A tápegység (*power supply unit* – PSU) az az alkatrész, amely a számítógép működéséhez szükséges feszültségeket állítja elő. A 230V⁷⁷ váltóáramot egyenárammá és törpefeszültséggé alakítja. Bár a számítógépben a tápegység után már 230V-os feszültséggel nem találkozunk, így az emberi szervezetre kevésbé veszélyes a számítógéphez belső részének megérintése, annál inkább veszélyes a belső berendezésekre, így a PC-k belső részéhez csak áramtalanítás után szabad nyúlni.

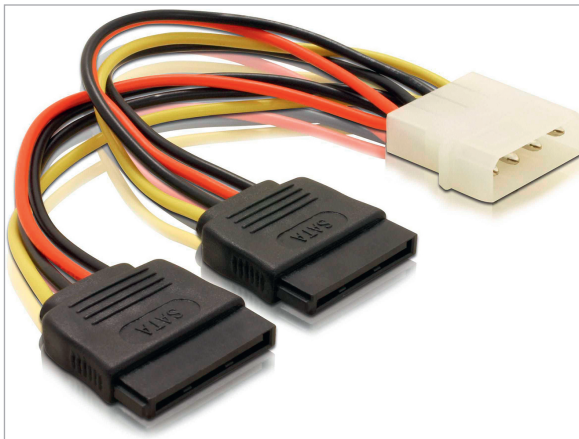
Az egyes alaplappcsaládok eltérő tápfeszültség-csatlakozókat igényelnek. Jelenleg az ATX a leggyakrabban használt tápegységtípus személyi számítógépekben. Ezek használata során az alaplap folyamatosan kap egy alacsony (+5V) feszültséget, így lehetővé válik, hogy a gépet szoftveres úton leállítsuk, illetve külső hardveregység segítségével (például modem, hálózati kártya) felébresszük, tehát az alaplap tudja vezérelni a tápegységet.

A tápegységből jellemzően induló kábelirányok és -típusok:

- alaplapi tápfeszültség-ellátást szolgáló 24 (régebben 20) pólusú csatlakozó, amelyben 3,3 V, 5 V, 12 V feszültségű erek, kommunikációra szolgáló erek működnek szabványosítva;
- az alaplapon szereplő CPU feszültségellátását szolgáló 4 pólusú négyzet alakú csatlakozó;

⁷⁷ A tengerentúlra is tervezett tápegységek automatikusan képesek 110 V feszültséget is a szükséges feszültségre transzformálni.

- FDD- – azaz floppy – csatlakozó – még szerepel a tápegységek csatlakozói közt, de kevésbé használatos;
- HDD-csatlakozó – azaz molex csatlakozó;
- SATA csatlakozó.



14. ábra: Átalakítható csatlakozó

Forrás: a szerző szerkesztése

A HDD- és SATA-csatlakozótípus feszültsége és kábelosztása átalakítható egymásba. Ilyen átalakítható csatlakozó látható a 14. ábrán.

PCI-Express csatlakozó a PCIe grafikus kártyák tápellátását biztosító 6, illetve 8 erű csatlakozó.

Adattárolás – háttértárak

Működési elvük szerint 3 fő csoportra oszthatók:

- Optikai adattárolók: CD-RW, DVD-RW, blu-ray.
- Mágneses adattárolás: ide sorolhatók a korábban használt hajlékony lemezes meghajtók (floppy), szalagos meghajtók, de ezek jelentősége az elmúlt évek során elenyészett.
- Elektronikus adattárolás: szilárd félvezető áramkörre épülő táruk.

Természetesen a korábban említett csoportokban is szükség van az elektromos áramra, de lényeges különbség, hogy itt az adat fizikai térben megvalósuló rögzítéséhez sem lézer(optikai), sem mágneses tér nem szükséges. Idesorolhatók az SSD-, pendrive, flash memóriák.

Optikai adattárolók

Az első, kereskedelmi forgalomba került, ma is működő formátum a CD (*compact disk*) lemez. Az egyes generációk lefelé kompatibilisek, azaz a későbbi technológiát (például *blu-ray*) használó lejátszók olvassák a korábbi szabványokat (például CD).

A CD egy digitális optikai lemezes adattárolási formátum, amelyet a Philips és a Sony invenciójaként adtak ki 1982-ben. A formátumot eredetileg csak a hangfelvételek (CD-DA) tárolására és lejátszására fejlesztették ki, de később az adatok tárolására is (CD-ROM). Ezekből számos más formátum származik, köztük az egyszer írható audio- és adattároló (CD-R), az újraírható adathordozók (CD-RW), a videó kompakt lemez (VCD), a szuper videó kompakt lemez (SVCD), a fénykép CD, a kép CD, a kompaktlemez-interaktív (CD-i) és továbbfejlesztett zenei CD.

A lemezen kb. 6 kilométer⁷⁸ hosszúságú spirálon helyezkednek el az adatok. A gyárilag készített lemezek mester nyomólap segítségével kerülnek rá egy műanyag lemezre, amelyet egy fényes alumínium lemez fed. Az adatok tehát nem a csillogó oldalon, hanem a „hátsó”, jellemzően festéssel fedett oldalon vannak, így arról az oldalról sok esetben sérülékenyebbek. Az írott, illetve újraírt lemezek esetében a tárolási hőmérséklet változása, fény, páratartalom, vegyszerek és mechanikai sérülések is okozhatnak adatvesztést.

1995-ben jelent meg a DVD- (*digital versatile disc* vagy *digital video disc*) lemez. Ehhez szintén lézerefényt használnak. Ennek megfelelően az információ tárolására szolgáló lyukacsok (*pits*) és a nyomok (*tracks*) közti távolságot 0,74 μm -re csökkentették. Az egyoldalas szimpla DVD-lemezek maximális kapacitása 4,7 GB. További újításként bevezették a kétrétegű írást, ennek megfelelően a szabványméretű lemezek kapacitását 8,5 GB-ra növelték. A kétoldalas DVD-n már 17 GB adat rögzíthető.

⁷⁸ Lásd: www.lightbyte.com/SpiralLength.htm

Fizikai mérete megegyezik a CD-lemez méretével. A DVD-lemezek fizikai felépítése hasonló a CD-lemezekéhez, csak a bemélyedések egymástól való távolsága kisebb, mint a CD-lemezekén (a fele – azaz 400 nm). Ezáltal nagyobb az adatsűrűség, és nagyobb tárolókapacitás érhető el. Itt is van egyszer íráható (DVD-R, DVD+) és újraírható (DVD-RW, DVD+RW).⁷⁹

Mágneses adattárolás

A rögzítés elméleti alapja, hogy digitális adatokat, azaz a jel és a jel hiányát egy adathordozó megmágnesezett felületén tulajdonképpen fizikai/analóg jellé alakítjuk olyan formában, hogy azt gépi feldolgozással a lehető leggyorsabb rögzítési és kiolvasási lehetőséggel megbízhatóan tárolhassuk.

Fizikai valóságában a megmágnesezhető anyag fölött elektromágneses tekercsek mozognak (vagy az adathordozó mozog a megmágnesezhető anyag alatt, vagy mindkettő mozog a másikhoz képest), és a tekercsekben elektromos impulzusok hatására keletkező mágneses tér fizikai nyomot hagy az anyagban, amely később újra kinyerhető – visszaolvasható.

A felülethez közel író- és olvasófej működik.⁸⁰ Az olvasófejben a mágnesezett felületnél elektromos áram keletkezik a tekercsben, és az információ meghatározható a visszaolvasott jel polarizációjából.

Több ilyen megmágnesezhető anyag áll rendelkezésre, amelyeknek az IT-hardver-gyártóknál történő megjelenését vagy háttérbe szorulását leginkább az előállításához szükséges technikai fejlettség, az előállítási költségek és a megbízhatóság befolyásolják.⁸¹

⁷⁹ Létezik DVD RAM is, amelynek adattárolási struktúrája szorosan kapcsolódik a merevlemez-technológiához, de gyártását már megszüntették. Volt HD DVD, amelyet a blu-ray versenytársának szántak, de alulmaradt.

⁸⁰ A fejlesztések során a külön író- és olvasófejeket egy egységbe rendezték, majd több ilyen egység kapott helyet, amelyek több sávon keresztül írták, olvasták a jeleket.

⁸¹ A buborékmemóriás adattárolás mozgó alkatrészek nélkül volt képes adatot tárolni, de merevlemez és a félvezető memóriachipek kiszorították ezeket az 1980-as években.

Mágnesszalag

1951-ben UNIVAC-I⁸² számítógépben az UNISERVO volt az első mágnesszalagos adattároló eszköz, amelynek a tényleges átviteli sebessége másodpercenként körülbelül 7200 karakter volt.

Azt gondolhatnánk, hogy a mágnesszalagon történő adatrögzítést az elmúlt időszakban a technológia túlhaladta, de valójában csak egy speciális szegmensre szorult vissza. Vállalati környezetben, ahol fontos a nagy mennyiségű adat megbízható tárolása olcsón, és nem fontos szempont a gyors adatelérés, ott helye van jelenleg is az ilyen rendszereknek. Az üzletmenet folytonosságának (*business continuity*) előfeltétele nemcsak a rendszeres adatmentés, adatarchiválás, hanem a biztonsági mentés telephelyen kívüli, *offsite* elhelyezése is. Az archív adatokat tartalmazó adathordozókat sok esetben mágnesszalagos adathordozókon helyezik el. Ilyen lineáris szalagmegnyitású (LTO-) rendszereket⁸³ kínálnak a nagy IT-gyártók, például: IBM, HP, Fuji, Sony, Maxell stb.

Szintén mágnesszalagos rögzítés történik a VHS- és audiokazettákon is, de itt a jelek analóg formában kerülnek a szalagra.

Mágnesszalagos rögzítés a bankkártyákon található mágnescsík is, amelyet egyre jobban kiszorít a chipes⁸⁴ adattárolás, amíg azonban nem történik meg a készpénzkímélő fizetési megoldások közül a mágnescsíkos azonosítás teljes körű kizárása, addig van lehetőség az ezekkel való visszaélésre.

A mágnescsík a plasztikkártyákon tulajdonképpen a VHS-kazettákkal azonos technológiával készült szalag, amely egy szabványos 85,60 mm × 53,98 mm lekerekített sarkú PVC – poli(vinil-klorid) – kártyára van felragasztva.

A mágnescsíkon 3 sávban lehetséges a szabvány⁸⁵ szerint adatokat rögzíteni, amelyek tartalmazzák/tartalmazhatják a kártyához tartozó számlaszámot, a kártyabirtokos nevét, a lejáratí időt, a szolgáltatási kódot, az ellenőrző kódot stb. A tárolási megoldás egyrészt sérülékeny a fizikai behatásokra is, de különösen a mágneses külső hatásokra. A fő sérülékenysége azonban nem ebben áll, hanem abban, hogy nagyon olcsó eszközökkel teljes funkcionalitását,

⁸² Ez volt az első általános célú elektronikus digitális számítógép üzleti alkalmazásra 2,25 MHz-es órajellel és 7,6 tonna súllyal.

⁸³ További szalagos adattárolók: DLT, SDLT, RDX, DAT DDS, AIT, QIC kazetták.

⁸⁴ Az EMV-chipről bővebben lásd: www.creditcards.com/credit-card-news/emv-faq-chip-cards-answers-1264/

⁸⁵ ISO/IEC 7813:2006. Részletesen lásd: www.iso.org/standard/43317.html

adattartalmát át lehet másolni egy másik mágnescsíkos kártyára, és abban az esetben, ha az azonosítás csak a mágnescsík alapján történik, a visszaélések könnyen megvalósíthatók.

Floppy disk – hajlékonylemez

A hajlékonylemez kör alakú, mindkét oldalán mágnesezhető réteggel ellátott vékony műanyag lap. A külső fizikai behatásoktól tok védi meg, az író-olvasó fej(ek) és a forgató mechanika hozzáférését a tokon megfelelő rések kivágásával teszik lehetővé. Készült belőle 8”, 5,15” és legelterjedtebb formájában 3,5 hüvelykes méretben – utóbbi adattárolási képessége 1,44 MiB, illetve 2,88 MiB volt. Jelentősége a 2000-es évek végére megszűnt.

Merevlemez

A mágneses adattárolás legelterjedtebb formája a merevlemez, amely egy vagy több, mágneses anyaggal bevont, merev, gyorsan forgó korong/tálca/lemez segítségével valósul meg. A lemezek együtt működnek a mágneses író-olvasó fejekkel, amelyek általában egy mozgó működtető karon elrendezve helyezkednek el. A megmágnesezett felületen az egyes blokkok és az adatok bármilyen sorrendben tárolhatók és lehívhatók. A HDD-k tartós tárolók, amelyek a tárolt adatokat még kikapcsolt állapotban is megtartják. Részletes működésüket, felépítésüket lásd később, külön jegyzetben.

Elektronikus adattárolás – Félvezető memória. A félvezető memória félvezető alapú integrált áramkör (*integrated circuit* – IC) chipeket használ az információk tárolására. Az adatokat általában fém-oxid-félvezető (*metal-oxide-semiconductor* – MOS) memóriacellákban tárolják. A félvezető memóriachip több millió memóriacellát tartalmazhat, apró MOS mezőhatású tranzisztorokból (*metal-oxide-semiconductor field-effect transistor* – MOSFET) és/vagy MOS-kondenzátorokból állva.

A századforduló óta a flash memória folyamatosan teret hódít az otthoni számítógépek offline tárolóinak piacán. A notebook és az asztali számítógép gyártói már 2006-ban elkezdtek a flash alapú tartós állapotú meghajtók (*solid-state drives* – SSD) használatát alapértelmezett konfigurációs beállításként a másodlagos tároláshoz, a hagyományosabb HDD mellett vagy ahelyett.

Jelentőségéből adódóan a kibernyomozó, illetve informatikai nyomozó szakirányon tanulmányokat folytató hallgatók számára az utóbbi két csoportba tartozó eszközökön (HDD, valamint SSD és flash memória) történő adattárolás technológiája, a fájlrendszerek, a kriminalisztika szempontjából lényeges további tulajdonságok kiemelt jelentőséggel bírnak, de kifejtésük meghaladja jelen könyv terjedelmi korlátait, így azt önálló jegyzet keretein belül tesszük meg.

Vákát

Infokommunikációs hálózatok – hírközlő hálózatok

Bevezetés

Az infokommunikációs hálózatok alapjait a hírközlő hálózatok teremtették meg. Graham Bell az 1876. október 5–11. között megrendezett Centennial Exhibition of Arts, Manufactures and Products of the Soil and Mine elnevezésű philadelphiai világkiállításon mutatta be már működő, hangátvitelre képes első telefonkészülékét. 1877 februárjában pedig már a Salemet Bostonnal összekötő, mintegy 25 kilométeres szakaszon a gyakorlatban is demonstrálta a hangátvitel lehetőségét elektronikus eszközökkel.⁸⁶ Az első telefonközpontot Puskás Tivadar ötlete alapján valósították meg az Egyesült Államokban. Puskás 1876 őszétől 1877 nyaráig Thomas A. Edison mellett a Menlo Park-i műhelyekben maga is dolgozott ennek megtervezésén, majd magának a telefonközpontnak az elkészítésén is. Ezek a találmányok tették lehetővé, hogy elektronikus úton hangkapcsolatot létesítsünk közvetlenül emberek, cégek között; ennek alapján fejlődtek ki a modern hírközlő hálózatok.

A technológia fejlődésével, az egyre újabb ötletek, találmányok megjelenésével és beépülésével mára gyökeresen átalakult – és további átalakulás alatt áll – a hírközlés. Az internet jelentette szabadság felhasználásával olyan alternatív távközlési módok jelentek meg, amelyek a következő évtizedekben nemcsak a hírközlés technológiáját, de az immár a több mint száz éve fennálló szolgáltatói modellt is várhatóan teljes mértékben megváltoztatják. Ha csak a hangátvitelt nézzük, akkor az internetprotokoll (IP) felhasználása ennek technológiájában, vagy a hagyományos hírközlési szolgáltatókat megkerülő, internetalapú kommunikációs szolgáltatók (ezeket hívjuk OTT-knek vagy alkalmazásszolgáltatóknak) és szolgáltatások megjelenése (például Skype) és elterjedése jól mutatják ezt a folyamatot.⁸⁷

Mindezek mellett azonban ma még működnek, és várhatóan még jó néhány évig, de akár évtizedig fennmaradhatnak az olyan, jelenleg is üzemelő hírközlő hálózatok, mint a fix (helyhez kötött) telefonok. Éppen ezért célszerű áttekinteni

⁸⁶ Szücs Péter: Technológiai fejlődés és hatása napjaink titkosszolgálataira. In Boda József – Dobák Imre (szerk.): *A nemzetbiztonság technikai kihívásai a 21. században*. Budapest, NKE Szolgáltató Nonprofit Kft., 2015. 21–26.

⁸⁷ Vö. Kovács (2015): i. m.

a ma prosperáló, a téma szempontjából, azaz a nyomozati munkában releváns hírközlő hálózatokat, valamint azt, hogy a nyomozás során milyen jellegű információkhoz juthat hozzá a nyomozó.

A kibernyomozók számára releváns hírközlő hálózatok

A hírközlési hálózatokon nyújtott szolgáltatások közül a kibernyomozók számára elsősorban az alábbiak lehetnek relevánsak:

- fix (helyhez kötött) telefonszolgáltatások;
- telefonalközponti szolgáltatások;
- mobiltelefon-szolgáltatások;
- mobilinternet-szolgáltatások.

2. táblázat: Magyarország bekapcsolt hangátviteli csatornák száma az NMHH adatai alapján

Bekapcsolt hangátviteli csatornák száma (db)		
Időszak		Teljes piacra vonatkozó becsült érték (db)
év	hónap	
2018.	november	3 075 532
	december	3 079 730
2019.	január	3 078 517
	február	3 081 023
	március	3 074 304
	április	3 073 230
	május	3 072 389
	június	3 071 418
	július	3 071 872
	augusztus	3 067 483
	szeptember	3 065 633
	október	3 056 594
	november	3 051 943

Megjegyzés: A Magyar Telekom Nyrt., a Digi-csoport: (Invitel Zrt., DIGI Kft.), a Vodafone-csoport (UPC Magyarország Kft., Vodafone Magyarország Zrt.), a PR-TELECOM Zrt., a Tarr Kft., a ViDaNet Zrt. és a PARISAT Kft. adatai alapján. Ezek a szolgáltatók lefedik a vezetékes hangpiac 96%-át. (Bekapcsolt hangátviteli csatornák száma/lakosság szám)*100

Forrás: a szerző szerkesztése

Több ok miatt foglalkozik ezekkel a szolgáltatásokkal ez a fejezet. Egyrészt ezen szolgáltatásokhoz kapcsolódnak olyan hírközlési hálózatok, amelyek Magyarország területén megtalálhatóak, így azokból a megfelelő információk a nyomozók számára elérhetők és kinyerhetők. Másrészt ezen szolgáltatások használata még mindig jellemző hazánkban, még akkor is, ha egyes szolgáltatások (például fix – helyhez kötött – telefonszolgáltatások) felhasználási aránya folyamatosan csökken. Ezt mutatja be az alábbi, 2. táblázat.

Harmadrészt ezek közül az internetelérést biztosító szolgáltatásokhoz használt kiszolgáló infrastruktúra adja meg a lehetőséget az OtT-szolgáltatók vagy alkalmazásszolgáltatók által nyújtott, egyre jobban terjedő kommunikációs módok használatára. Jellemző, hogy a széles sávú internetelérést biztosító szolgáltatások aránya folyamatosan emelkedik hazánkban. Ezt mutatja az alábbi, 3. táblázat.

3. táblázat: Magyarországi nagysebességűinternet-előfizetések aránya az NMHH adatai alapján

Optikai és Docsis 3 hálózaton igénybe vett internet-előfizetések száma		
Időszak		Nagysebességű (30 Mbit/s feletti) internet-előfizetések aránya
év	hónap	
2018.	november	69,6%
	december	69,9%
2019.	január	70,3%
	február	70,5%
	március	70,9%
	április	71,1%
	május	71,5%
	június	71,8%
	július	72,2%
	augusztus	72,5%
	szeptember	72,9%
	október	73,5%
	november	74,0%

Megjegyzés: A Magyar Telekom Nyrt., a Digi-csoport: (Invitel Zrt., DIGI Kft.), a Vodafone-csoport (UPC Magyarország Kft., Vodafone Magyarország Zrt.), a PR-TELECOM Zrt., a Tarr Kft., a ViDaNet Zrt. és a PARISAT Kft. adatai alapján. Ezek a szolgáltatók lefedik a vezetékes szélessávúinternet-piac 90%-át.

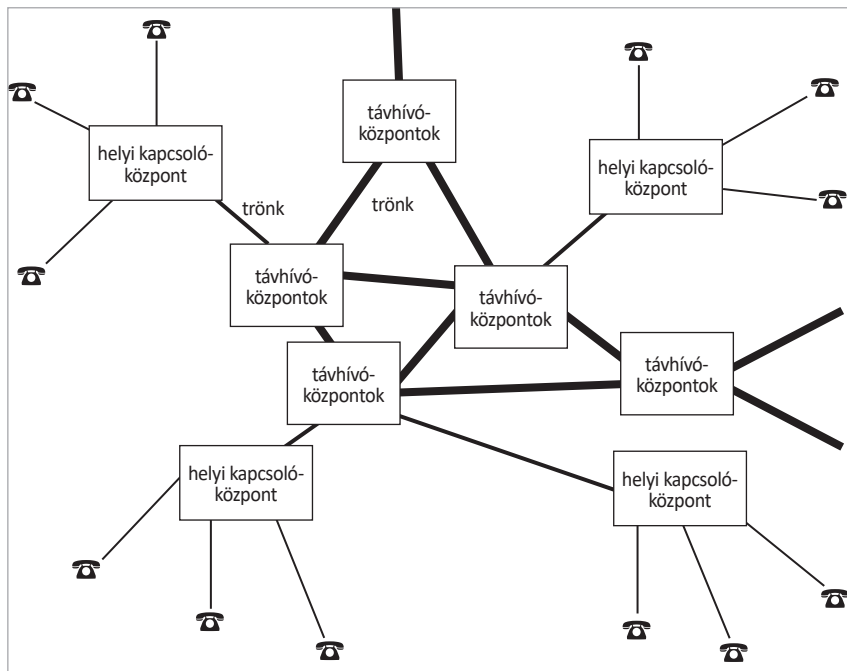
Forrás: a szerző szerkesztése NMHH 2019. alapján

A vezetékesinternet-szolgáltatásokat az *Infokommunikációs hálózatok – IT-hálózatok* fejezet mutatja be.

Fix (helyhez kötött) telefonhálózatok

Fix (helyhez kötött) telefonhálózatok felépítése

A fix (helyhez kötött) telefonhálózatok sematikus felépítését a 15. ábra mutatja.



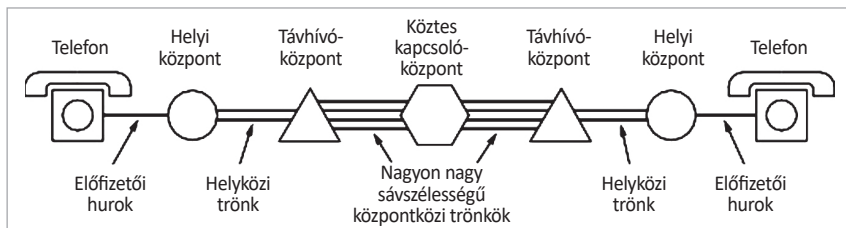
15. ábra: Telefonhálózatok sematikus felépítése

Forrás: a szerző szerkesztése Andrew Tanenbaum – David Wetherall: *Számítógép-hálózatok*. Panem Könyvek. Budapest, Taramix Kft., 2013 alapján

Az egyes készülékek kapcsolóközpontokon keresztül kapcsolódnak egymáshoz. Amikor A szám (hívó) hívja B számot (hívott), akkor ez a híváskezdeményezés

a helyi kapcsolóközpontba fut be. Amennyiben a hívott szintén ebbe a helyi kapcsolóközpontba van bekötve, akkor az előfizetők összekapcsolását ez a kapcsolóközpont elvégzi. Amennyiben a hívott fél másik helyi kapcsolóközponthoz kapcsolódik, akkor a hívás a távhívóközpontokon keresztül jön létre.

A 15. ábra csak eddig a hierarchiaszintig mutatja be telefonhálózatok működését. Ennél magasabb szintek is léteznek, így a távhívóközpontokat is további, úgynevezett köztes kapcsolóközpontok kötik össze, amelyek segítségével nagy távolságú hívásokat lehet lebonyolítani. Ezt mutatja be a 16. ábra.



16. ábra: Tipikus áramkörti út egy nagy távolságú hívás esetén

Forrás: a szerző szerkesztése Tanenbaum–Wetherall (2013): i. m. alapján

Korábban a rendszer minden eleme és átviteli útja teljesen analóg technológián alapult, ma már jellemzően teljes mértékben digitalizálták azokat. Természetesen köztes megoldások is megtalálhatók még, ahol bizonyos elemek (jellemzően az előfizetői készülékek és a helyi kapcsolóközpont bizonyos részei) még analógok maradtak. Ezek azonban általánosságban nem befolyásolják a nyomozó számára releváns információkat.

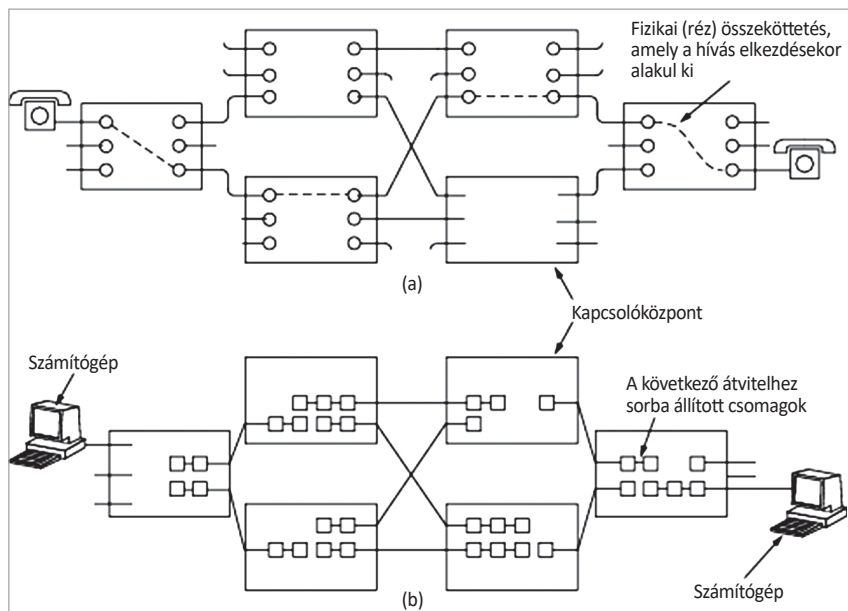
A nyomozások szempontjából fontos információkat a szolgáltatók által üzemeltetett kapcsolóközpontokban lehet fellelni, így a továbbiakban ezekkel foglalkozunk.

Napjainkban jellemzően két különböző kapcsolási módszert használnak a hívások felépítésére: az úgynevezett vonal- (vagy áramkör-) kapcsolt és az úgynevezett csomagkapcsolt technológiát.

Vonal- (vagy áramkör-) kapcsolt technológia

Ebben az esetben a hívás során a két végpont (hívó és hívott) között egy fix, dedikált kapcsolat épül ki, amely a hívás kezdetétől annak végéig folyamatosan

fennmarad. Ha a fizikai kapcsolat megvan, akkor ezen keresztül viszik át az adatokat, majd bontják a vonalat. Erre mutat példát a 17. ábra (a) része.



17. ábra: Vonal- és csomagkapcsolt kapcsolási módok

Forrás: a szerző szerkesztése Tanenbaum–Wetherall (2013): i. m. alapján

Ez persze egy leegyszerűsített ábra. Ebben az egyes dobozok a kapcsolóközpontokat jelképezik, és – a könnyebb érthetőség kedvéért – nem tartalmaz olyan részeket, mint amilyenek a kapcsolóközpontok közötti átviteli utak (ilyenek lehetnek például az üvegszálak, mikrohullámú átvitelek stb.) vagy a kapcsolóközpontok által kezelt akár több ezer ki- és bejövő kapcsolat.

A vonalkapcsolt esetben a kapcsolatnak a beszélgetés (vagy az adatátvitel) előtt ki kell épülnie, az erre szolgáló jelzéseknek és visszaigazolásoknak át kell mennie a rendszeren, és csak ezután kezdődhet meg a tényleges kommunikáció. A hálózat kihasználtsága gyenge, hiszen akkor is fenn kell tartani a dedikált kapcsolatot, amikor éppen nincs kommunikáció a két fél között (például épp nem beszélnek). Éppen ezek miatt – amikor a beszéd átvitelére is jellemzően IP-hálózatokat használunk, ez a kapcsolási technológia egyre jobban háttérbe szorul.

Csomagkapcsolt technológia

Ebben az esetben az üzenetet (legyen az adat vagy hang) adott méretű csomagokra bontja a rendszer, és azokat továbbítja – akár csomagonként más-más útvonalon. Az ezekhez használt útvonalválasztók úgynevezett *tárol és továbbít* módszert alkalmazva, a leggyorsabb és/vagy legolcsóbb irányokat választva továbbítják az egyes csomagokat. Ezen módszer esetében a csomagok a fogadó félhez nem feltétlenül a küldés sorrendjében érkeznek meg, azaz egy később küldött csomag akár hamarabb is megérkezhet, mint egy korábban elindított társa. Így az eredeti üzenetet a fogadó félnél lévő eszköznek kell a beérkező és általa tárolt csomagokból újra összeállítania. Erre mutat példát a 17. ábra (b) része.

A csomagkapcsolt technológiánál jobb a hálózat kihasználtsága, nem érdekes az átvitel (hívás) időtartama, ugyanakkor érdekes az átvitt információ mennyisége (jellemzően ez alapján történik itt a számlázás, míg vonalkapcsolt esetben a hívás időtartama alapján). Ennél a technológiánál egy hálózati elem kiesése nem okoz végzetes problémát az üzenet továbbításában, míg a vonalkapcsolt technológia esetében igen. Az IP-alapú hálózatok ezt a technológiát használják.⁸⁸

A kibernetizáció számára releváns adatok a fix (helyhez kötött) telefonhálózatokban

Egy nyomozás során a szolgáltató a kapcsolóközpontokból általában az alábbi adatokat, információkat képes szolgáltatni a nyomozó számára:

- az előfizetők adatai (név, lakcím, szerződéses adatok, számlázási adatok);
- híváslisták (az adott előfizető által kezdeményezett, fogadott hívások adatai, adott esetben a sikertelen hívások adatai – hívó, hívott fél azonosítói, hívás kezdeti időpontja, időtartama);
- megfelelő engedélyek birtokában az engedélyezett telefonok forgalmazásának lehallgatása.

Meg kell jegyezni, hogy az egyes kapcsolóközpontok, telefonhálózatok mind technikailag, mind pedig topológiában nagyon eltérhetnek egymástól, így adott esetben a fenti adatok, információk nem mindegyike vagy azok nem teljeskörűen férhetők hozzá vagy adott szolgáltató rendszerében. Ugyanakkor adott esetben

⁸⁸ Vö. Tanenbaum–Wetherall (2013): i. m.

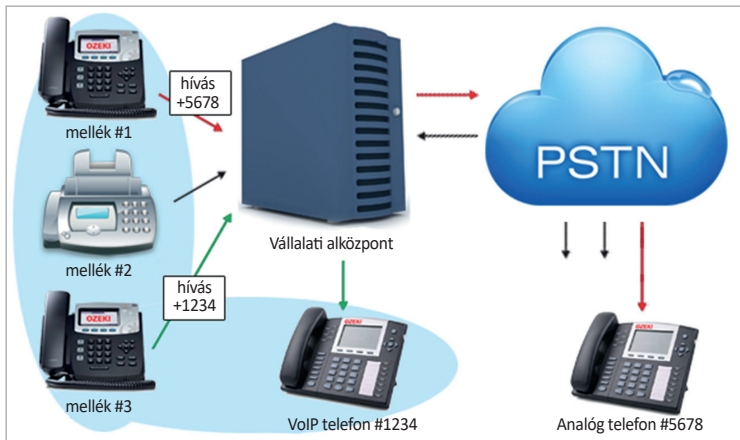
a fent felsoroltak mellett más adatokat, információkat is képes a szolgáltató biztosítani a nyomozók számára. Éppen ezért minden esetben célszerű a lehetőségekről a szolgáltató erre a célra dedikált – általában biztonsági – embereivel konzultálni.

A fix (helyhez kötött) telefonhálózatok esetében az előfizetői készülékek ritkán tárolnak/tartalmaznak olyan információkat, amelyek a nyomozó számára értékesek lehetnek. Ma már egyre ritkábban használnak üzenetrögzítőt otthon, vagy például faxkészüléket az irodában. Mindemellett azonban előfordulhat olyasmi (például számítógép használata végpontként), ami miatt az adott ügyben mindig érdemes átgondolni, hogy kinyerhető-e valamilyen értékes, adott esetben csak ott fellelhető információ az előfizetői készülékekből is.

Telefonalközponti hálózatok

Telefonalközponti hálózatok felépítése

A telefonalközponti hálózatok felépítése viszonylag egyszerű. A hagyományos alközpontok gyakorlatilag néhány, a szolgáltatótól érkező telefonvonalat fogadnak egy telefonalközpontban, és ugyanide kapcsolódnak a belső (általában egy vállalat dolgozóinak kiosztott) telefonkészülékek is.

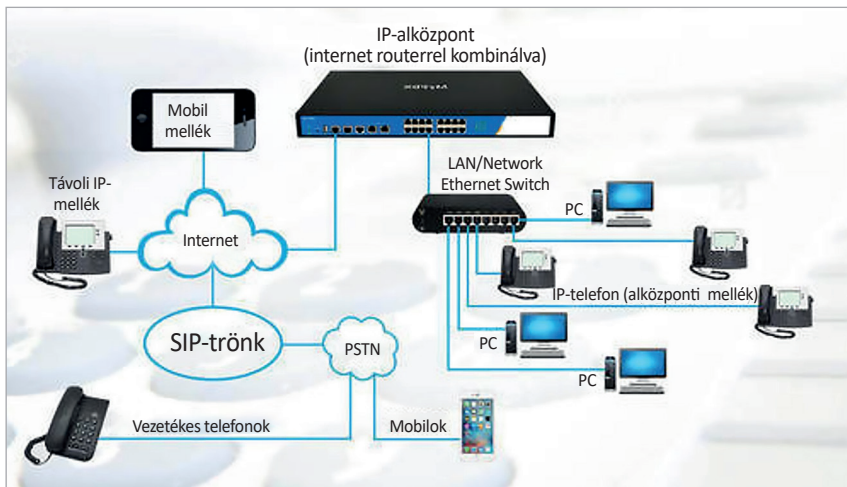


18. ábra: Vállalati telefonalközpont

Forrás: a szerző szerkesztése Ozeki: [CompanyPBX-Voip](#). alapján

Az alközpont egyrészt a belső telefonkészülékek (mellékállomások) egymás közötti kapcsolódását biztosítja, másrészt költséghatékonyan oldja meg a kifelé irányuló hívásokhoz a külső telefonvonalak hozzárendelését (így jóval kevesebb külső vonal elég, mintha minden mellékállomásra saját fővonalat kötnénk), harmadrészt lehetővé teszi, hogy a kintről érkező hívások a megfelelő melléken végződjenek. Egy telefonalközpont felépítését mutatja a 18. ábra.

Ma már a telefonalközpontok jellemzően IP-alapú hálózatokat és jelátvitelt használnak. Ezek felépítése csupán némileg különbözik a hagyományos (analóg vagy digitális, de még nem IP-alapon működő) telefonalközpontokétól, azonban szolgáltatásai sokkal kiterjedtebbek (például videohívást is lehetővé tesznek, akár a mellékállomások között is). Egy ilyen mutat be a 19. ábra.



19. ábra: IP vállalati telefonalközpont

Forrás: a szerző szerkesztése

Ma már megjelentek a különféle virtuális alközpontok is, amelyek lényege, hogy egy külső szolgáltató (lehet az hírközlési szolgáltató is, például a Vodafone Magyarország Zrt. is kínál ilyen szolgáltatást) távolról nyújtja az alközpont funkcionálisát. Ebben az esetben a vállalat helyi kommunikációs eszközei nem

a vállalatnál elhelyezett alközponton keresztül, hanem egy felhőalapú megoldás segítségével állnak egymással összeköttetésben.⁸⁹ Egy ilyen mutat be a 20. ábra.



20. ábra: Virtuális telefonalközpont

Forrás: <https://thevoicesolutions.com/cloud-pbx/> alapján

A kibernyomozó számára releváns adatok a telefonalközponti hálózatokban

A nyomozás során egy alközpontból általában az alábbi adatokhoz, információkhoz lehet hozzájutni:

- az alközponthoz kapcsolódó belső készülékek (mellékállomások) azonosító adatai, az azokat használó felhasználó azonosító adatai;

⁸⁹ Nick Campanella: *The Beginner's Guide to Virtual PBX*. Getvoip, 2017. szeptember 8.

- az alközpont által használt külső kapcsolódási vagy más néven fővonali adatok (vezetékes szolgáltatások telefonszámai, mobiltelefon-szolgáltatások telefonszámai, IP-címek);
- híváslisták (az alközponthoz kapcsolódó belső készülékek vagy más néven mellékek, egymás közötti és külső irányba/irányból bonyolított forgalmazásának adatai);
- megfelelő engedélyek birtokában az engedélyezett mellékek forgalmazásának lehallgatása.

Meg kell jegyezni, hogy az egyes alközpontok mind technikailag, mind pedig beállításokban nagyon eltérhetnek egymástól, így adott esetben a fenti adatok, információk nem mindegyike vagy azok nem teljeskörűen férhetők hozzá egy adott alközpontban. Ugyanakkor adott esetben a fent felsoroltak mellett más adatok, információk is kinyerhetők. Éppen ezért minden esetben célszerű a lehetőségekről az alközpont üzemeltetőjével konzultálni.

Amennyiben egy adott vállalat virtuális alközpontot vesz igénybe, akkor is az adott vállalatnak kell teljesítenie a hatósági megkeresést, ám elképzelhető, hogy a fenti információk megszerzéséhez, a technikai lebonyolítás érdekében (például lehallgatás megvalósítása) adott esetben a virtuális alközpont szolgáltatóját is meg kell – vagy legalábbis célszerű – keresni.

A telefonalközpontok esetében az előfizetői készülékek jellemzően akkor tárolnak/tartalmaznak olyan információkat, amely a nyomozó számára értékes lehet, ha azok valamilyen többlettudással, funkcionalitással ellátott eszközök (például számítógép, okostelefon, IP-telefon). Emiatt szintén minden esetben érdemes konzultálni az alközpont üzemeltetőjével.

Mobiltelefon-hálózatok

Napjainkban a mobil infokommunikációs hálózatokat használjuk leginkább. A szóhasználat itt nem véletlen, hiszen a mobil rádiótelefon-hálózatokat ma már messze többre használjuk, mint telefonálásra. A szolgáltatók a hagyományosnak tekinthető hanghívás és SMS-küldés mellett ma már széles sávú internetelérést is biztosítanak, mobil készülékeink, okostelefonjaink pedig sokkal inkább nyújtják egy kis méretű, hordozható számítógép szolgáltatásait, amelyen – mellesleg – telefonálni is lehet. A mobilkommunikáció változását jól szemlélteti az alábbi, az egyes generációk képességét is tartalmazó 21. ábra.

1G	2G	3G	4G	5G
1981	1992	2001	2010	2020 (?)
2 Kbps	64 Kbps	2 Mbps	100 Mbps	10 Gbps
Hang- szolgáltatás analog	Hang- szolgáltatás és üzenetek (SMS) digitális	hang, üzenetek és adatátvitel digitális	hang, üzenetek és széles sávú adatátvitel digitális	hang, üzenetek, széles sávú adatátvitel, IoT digitális
				

21. ábra: Mobilkommunikáció generációi

Forrás: a szerző szerkesztése

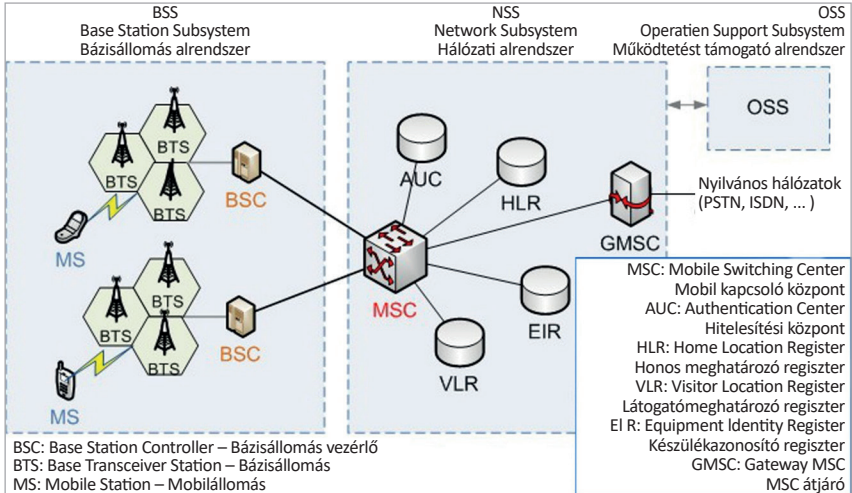
Mobiltelefon-hálózatok felépítése

A mobiltelefon-rendszerek felépítésének magyarázatát a beszédátvitelre alkalmas 2G-rendszer felépítésével célszerű kezdeni. Egyrészt azért, mert ma is ez képezi a beszédátvitelkor használt hálózatok alapját (napjainkban ugyan a nagy sebességű adatátvitelre tervezett 4G-rendszerekben már használnak a szolgáltatók IP-alapú beszédátvitelt, ez az úgynevezett VoLTE,⁹⁰ ám ez többnyire csak a honos hálózaton érhető el, jelenleg külföldi hálózat használatakor, úgynevezett roaming alkalmával még jellemzően nem), másrészt ezt kiegészítve egyszerűen be lehet majd mutatni az adatátvitelt is. Az alábbi alfejezet, természetesen, ahol a téma igényli, rövid kitekintéseket is tartalmaz a magasabb fejlettségű (3G-, 4G-) hálózatok bizonyos jellemzőivel, tulajdonságaival kapcsolatosan.

⁹⁰ VoLTE: Voice over LTE, vagyis hang átvitele a 4G LTE-n. LTE: a long term evolution (tükörfordításban: hosszú távú fejlődés) rövidítése, amely egy negyedik generációs mobil adatátviteli szabvány.

A 2G GSM-rendszer felépítése

A GSM-rendszer vázlatos felépítését a 22. ábra mutatja be.



22. ábra: A GSM-rendszer felépítése

Forrás: a szerző szerkesztése Miguel A. Vega-Rodriguez – José M. Chaves-González: *Multiobjective frequency assignment problem*. MSTAR::UNEX, 2020 alapján

A GSM-rendszer négy főbb alrendszerből tevődik össze:

1. mobilállomás (MS) (a 22. ábra BSS részében található, azonban a téma szempontjából mindenképp különálló alrendszernek tekintendő);
2. hálózati alrendszer (*network and switching sub-system* – NSS);
3. bázisállomás alrendszer (*base station sub-system* – BSS);
4. működtetést támogató vagy üzemeltetési alrendszer (*operations support sub-system* – OSS).⁹¹

⁹¹ Michel Mouly – Marie-Bernadette Pautet: *The GSM system for mobile communications*. Telecom Publishing, 1992.

A mobilállomás

Gyakorlatilag az előfizetői készülékeket jelenti. A mobilállomások felépítésével, képességeivel jelen fejezet nem foglalkozik bővebben, csupán néhány, a nyomozások szempontjából lényeges dolgot emelünk ki.

Az előfizetői készülékeket sokféleképpen lehet csoportosítani, ám jelen könyv témájának szempontjából két osztályba sorolhatók a készülékek:

- Hagyományos szolgáltatásokat biztosító, úgynevezett „buta” telefonkészülékek. Jellemzően telefonálást, SMS és jobb esetben MMS küldését és fogadását biztosítják, jellemzően még nyomógombos kivitelűek. Ebben az esetben magának a készüléknek a vizsgálatából kevés pluszinformációt fog tudni a nyomozó megszerezni, a számára értékes információk zömét a szolgáltató biztosítja majd.
- Sokrétű szolgáltatást biztosító úgynevezett okostelefon-készülékek. Jellemzően érintőképernyős, sokfunkciós, a számítógépek tudását hordozható méretben biztosító, GSM-modullal ellátott és a hagyományos mobiltelefon-készülékek szolgáltatásait is nyújtó készülékek. Használatuk jellemzően az interneteléréshez kapcsolódik (például levelezés, webböngészés, internetalapú alkalmazások [például Facebook, Viber stb.]), így maga a készülék is rengeteg olyan, a nyomozó számára hasznos információt rejt, amelyet a mobilszolgáltató nem tud biztosítani. Így az okoskészülékek vizsgálatával mindenképp érdemes számolni a nyomozás során.

Hálózati alrendszer

A mobiltelefon-rendszerek alapvető működtetéséhez szükség van a mobilállomások azonosítására, tartózkodási helyének meghatározására, valamint a kívánt kapcsolataik (kimenő és bejövő hívások) felépítésére más mobil- vagy állandó helyű állomásokkal (telefonkészülékkel). Az ezekhez szükséges összekapcsolásokat és adatbázis-funkciókat a hálózati alrendszer végzi el. A hálózati alrendszer felépítését szintén a 22. ábra szemlélteti.

A hálózati alrendszerben az alábbi funkcionális egységek találhatók:

MSC (*mobile switching center*): mozgószolgálati kapcsolóközpont. Az MSC általában egy digitális, tárolt programvezérlésű kapcsolóközpont, hasonló ahhoz, mint ami más, fix (helyhez kötött) telefonrendszerekben is megtalálható. Gyakorlatilag ez a rendszer agya, ez végzi a mobilállomások egymás közötti vagy más

(például vonalas előfizetői) állomásokkal történő kapcsolatának menedzselését (hívásfelépítést, irányítást, ellenőrzést, megszakítást). A hívások felépítéséhez az MSC a – később ismertetendő – HLR-ben, VLR-ben és AuC-ben összegyűjtött és tárolt előfizetői információkat használja fel, amikor azok éppen szükségesek a kommunikáció valamely fázisához.

A mobiltelefon-hálózatok esetében is – hasonlóan a fix (helyhez kötött) telefonhálózatokhoz – általában több MSC található egy szolgáltató hálózatában. Ezek kapcsolódása hasonló ahhoz, mint amelyet a 15. ábra szemléltet, így ezt itt nem mutatjuk be ismételten.

GMSC (*gateway MSC*): átjáró (vagy kilépőponti) kapcsolóközpont. A GMSC a mobiltelefon-hálózat és más külső hálózatok (például más mobiltelefon-hálózatok, vezetékes nyilvános távbeszélő-hálózatok, ISDN stb.) közötti kapcsolatot biztosítja – legyen az akár belföldi, akár nemzetközi –, azaz a továbbírási (*routing*) feladatokat látja el. Minden külső hálózathoz érkező vagy oda irányuló jelzés a GMSC-n fut keresztül. A befelé érkező jelzések innen továbbítódnak a hálózaton belül található megfelelő MSC-hez, a hálózaton belülről érkező jelzések pedig a megfelelő külső hálózathoz. A GMSC általában nem egy különálló központ, hanem valamelyik, a hálózatban található, dedikált MSC részét képezi.

HLR (*home location register*): honos meghatározó regiszter. Itt tartják nyilván az adott hálózathoz tartozó mobil-előfizetőtől származó adatokat. Ebben az előfizető összes úgynevezett statikus adata megtalálható, így például a HLR tartalmazza az adott előfizető előfizetői adatait, a hozzáférési képességét a hálózathoz, az általa elérhető előfizetői és a kiegészítő szolgáltatásokat. De a HLR úgynevezett dinamikus adatokat is tárol az előfizetőről, itt található a mobilállomás aktuális helyzete. Ennek kapcsán a HLR információkat tartalmaz azokról az MSC-területekről, ahol a mobilkészülék bolyong (roamingol), és ahonnan az MSC le tudja kérdezni a mobilállomás aktuális helyzetét. Ezek alapján bármely bejövő hívást közvetlenül a hívott előfizetőhöz (azaz az adott mobilállomáshoz) tud irányítani.

AuC (*authentication center*): hitelesítési (illetékességet megállapító) központ. Ez a központ az előfizetői jogosultságokat ellenőrzi, valamint a biztonsági és a titkosítási kódokat kezeli. Összegyűjti azokat az információkat, amelyek a mobil-előfizető kommunikációjának az úgynevezett levegő interfészen (*air interface*) keresztül történő lehallgatása elleni védelméhez szükségesek. (Az illetéktelen lehallgatás szempontjából a mobiltelefon-hálózatokban mindig a levegő interfész a legkritikusabb rész. Az illetéktelen lehallgatás megakadályozására a szolgáltatók olyan speciális intézkedéseket alkalmaznak a hálózatok

működtetése során, mint a továbbított információk titkosítása, és ebben kiemelt szerepet kap a levegő interfész védelme.) A titkosítási kulcsok és az egyéb biztonsággal kapcsolatos paraméterek is az AuC-ban gyűlnek össze. Az AuC technikailag általában nem önálló egységként jelenik meg, hanem a HLR részeként.

VLR (*visitor location register*): látogatómeghatározó regiszter. Ez a regiszter tartalmazza átmenetileg mindazokat az adatokat, amelyek a szolgáltatóhálózatban az adott MSC ellátási körzetében tartózkodó, idegen (nem honos, azaz roamingoló), az adott időpontban aktív mobil-előfizetőktől származnak. Ennek során aktív adatcserét folytat azokkal a HLR-ekkel, ahol a körzetében tartózkodó mobilállomások honosak, innen kapja meg az adott előfizető jogosultságait (szükséges statikus adatait). A VLR összegyűjt minden információt arról a mobilról, amelyik belép az általa lefedett területre, és az annak honos HLR-étől kapott jogosultságoknak megfelelően engedélyezi a bejövő és kimenő hívásokat bármikor, bárhonnan jönnek, vagy bárhová irányulnak is. Ugyanakkor a VLR és a honos HLR között a dinamikus előfizetői adatok kapcsán is, amikor erre szükség van – például lokációs területváltás alkalmával vagy kommunikáció során a számlázás miatt – intenzív adatsere zajlik.

EIR (*equipment identity register*): készülék- (mobilállomás-) azonosító regiszter. Ebben tárolják az információkat minden legálisan regisztrált mobilállomásról (például típus, IMEI), de ebben van lehetőség a lopott vagy egyéb okokból (például csalás miatt) nem engedélyezett készülékek tiltására is.

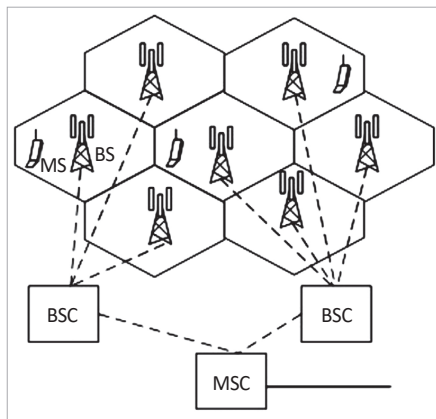
A GSM-rendszer a mobilállomás azonosítása során mindig két ellenőrzést hajt végre, egyrészt magát a felhasználót, másrészt a kommunikációhoz használt készüléket is azonosítja. Ez utóbbihoz a készülék egyedi azonosítóját (IMEI), míg az előbbihez a felhasználó által használt úgynevezett SIM-kártyán található felhasználóazonosítót (IMSI) használja fel. Ezek az adatok teszik lehetővé többek között azt is, hogy a lopott készülékeket és lopott SIM-kártyákat helyileg is azonosítani lehessen, vagy akár ki is lehessen tiltani a rendszer(ek)ből, ezzel lehetetlenné téve azok további használatát. Ezt a tiltási folyamatot szolgálja az is, hogy egy adott országban működő minden szolgáltató, valamint a különböző országokban működő, de egymással kapcsolatban álló szolgáltatók is rendszeres időközönként kicserélik a lopott vagy más okból (például csalás miatt) tiltott készülékek listáját (ez az úgynevezett feketelista [*blacklist*]).

Sajnálatos módon a tiltások hatékonysága több ok miatt sem megfelelő. Egyrészt a szolgáltatóknak az az érdeke, hogy a saját hálózaton minél nagyobb forgalom legyen, így egy másik szolgáltató által tiltott (úgynevezett feketelistára tett) készülék saját hálózaton belüli tiltása nem minden esetben érdeke az adott

szolgáltatónak. Másrészt a tiltott készülékek listájának cseréjére nem egységes fórum és egységes technikai platform áll rendelkezésre, hanem azok szolgáltatóként, országonként is változnak. Ezen fórumok, technikai platformok nem mindegyike érhető el egy adott szolgáltató számára. De az elérhető listák nyomon követése is a legtöbb esetben olyan technikai és emberi erőforrásokat igényel, amelyek egyszerűen a pénzügyi megfontolások mentén nem érik meg az adott szolgáltatóknak. Harmadrészt a készülékek egyedi azonosítására szolgáló IMEI-szám könnyen hamisítható, sok esetben (jellemzően a kelet-ázsiai országokbeli gyártóktól) több ezer vagy több tízezer készülék kerül forgalomba ugyanazzal az IMEI-számmal. Ez pedig az IMEI-szám alapján történő azonosítást, tiltást jelentősen megnehezíti, adott típusú készülékeknél szinte teljesen el is lehetetleníti.

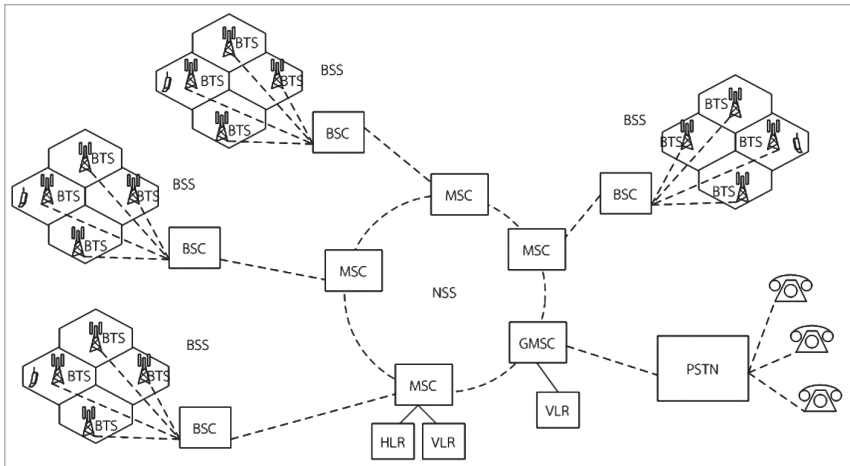
Bázisállomás alrendszer

A bázisállomás alrendszert a bázis adó-vevő állomások, vagy közismert nevén a bázisállomások (*base station transceiver system – BTS*) és a bázisállomás-vezérlők (*base station controller – BSC*) alkotják. A mobiltelefon-hálózatoknál használt úgynevezett cellás rendszer kialakítását mutatja be a 23. és 24. ábra.



23. ábra: A BSS felépítése

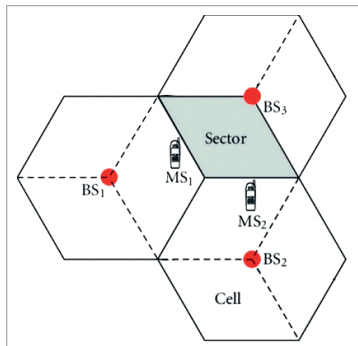
Forrás: a szerző szerkesztése Chokchai Sangdao *Mobile phone evolution. Part 3*. Mahanakorn University of Technology, 2014. október 31. alapján



24. ábra: Cellás mobiltelefon-hálózat felépítése a BSS-ekkel

Forrás: a szerző szerkesztése Sangdao (2014): i. m. alapján

BTS (base station transceiver system): bázisállomás. A BTS egyetlen cella kiszolgálását látja el, és a BSC vezérli. A BTS egy vagy több adó/vevő berendezést (TRX) tartalmaz. Az adó/vevő berendezésekkel a cellán belül több úgynevezett szektort alakítanak ki. Ezt mutatja be a 25. ábra.



25. ábra: Szektorsugárzók egy BTS-en belül

Forrás: a szerző szerkesztése Martin Haardt: *CA topology based on 3-sector-cell system*. 2008. alapján

Ebben az esetben egy cellán belül három, egyenként 120°-os szektor van kialakítva. Ez a téma szempontjából azért érdemel kiemelés, mert segítheti a mobilállomás pontosabb tartózkodási helyének meghatározását a nyomozó számára is.

BSC (*base station controller*): bázisállomás-vezérlő: A BSC egy vagy több BTS-t szolgál ki. Feladatai közül a téma szempontjából elsősorban az alábbiakat érdemes kiemelni:

- vezérli a BTS és az MSC közötti összeköttetéseket;
- döntést hoz, amikor egy mobilállomást az egyik cellától a másiknak át kell adni (például a mobilállomás elmozdult beszélgetés közben, azaz úgynevezett *handover*-t kell végrehajtani, az adott cellában lévő túl sok mobilállomás miatt a kiszolgálása az adott bázisállomáson nem lenne lehetséges, egy másik cellában a kiszolgálása jobb minőségben történhet stb.);
- szükség esetén elvégzi a BTS újrakonfigurálását.

Egyetlen bázisállomás-vezérlő több bázisállomást is vezérelhet. Az egyes cellák mérete a kiszorgálandó területen várható mobilállomások számától függ. Így például amíg vidéki, ritkán lakott körzetekben egy cella akár több tíz kilométerről is elérhető egy mobilállomás számára, addig egy sűrűn lakott városban ez csupán néhány száz méter lehet. Sőt léteznek úgynevezett pikocellák, amelyek akár csupán egyetlen emelet kiszorgálását látják el egy épületen belül. Az újabbak – 3. generációs, vagy más néven 3G-rendszerektől fölfelé – már olyan eljárásokat is alkalmaznak, amelyeknél az adott cellák mérete a felhasználás mértékében (kiszorgált mobilállomások száma és az átviteli sebesség függvényében) változhat. Így amikor sok felhasználó egyidőben használja ugyanazon cellát, akkor annak mérete kisebb, amikor kevesebben használják, akkor pedig nagyobb lesz. Ez az úgynevezett cellalélegzés.⁹²

Működtetést támogató vagy üzemeltetési alrendszer

Az OSS valamennyi protokolljának és az alkalmazásoknak meg kell felelnie az ITU által kidolgozott úgynevezett távközlést menedzselő hálózat (*telecommunications management network* – TMN) követelményeinek. (A TNM keret-

⁹² Béres Roland: *Mobilhálózatok energiatakarékos üzemeltetése*. TDK-dolgozat. Budapest, Budapesti Műszaki és Gazdaságtudományi Egyetem Villamosmérnöki és Informatikai Kar Távközlési és Médiainformatikai Tanszék, 2012.

rendszer, amely lehetővé teszi a kapcsolódást és az együttműködését a különböző gyártók különböző eszközei között.)⁹³

Az OSS része az üzemeltetési és fenntartási központ (*operation and maintenance center* – OMC) és a hálózati irányító központ (*network management center* – NMC).

OMC (*operation and maintenance center*): üzemeltetési és fenntartási központ:

Az OMC alapvetően ugyanazokkal a funkciókkal rendelkezik, mint a fix (helyhez kötött) vagy más néven vezetékes hálózatok OMC-i. Ugyanakkor egy jelentős eltérés azért található közöttük. Ugyanis a mobilhálózat OMC-jének jellemző funkciója a mobilhálózat rádiós részének üzemeltetési és fenntartási feladata, amely fix hálózatok esetében természetesen nincs meg. Az OMC jellemzően az alábbi funkciókkal rendelkezik az előbb említett rádiós interfésszel kapcsolatos feladatokon kívül:

- a közbenső eszközök és a távoli kezelő számára lehetővé teszi a hozzáférést valamennyi hálózati elemhez;
- felügyelet: riasztási állapot és vizsgálati menedzsment;
- forgalmi és számlázási adatok gyűjtése;
- hálózatkonfiguráció megjelenítése és változtatása, az operátortól vagy a hálózati irányító központtól kapott instrukcióknak megfelelően;
- az előfizető adminisztrálása és nyomon követése.

Fontos szerepe van az OMC-nek a – korábban már említett, 3G- és fejlettebb rendszereknél alkalmazott – cellaméret állításakor is. Az OMC tartalmazza a mobilállomások távolságát a bázisállomástól, ezért sok felhasználó esetén az OMC csökkenti a cellaméretet, majd a forgalom csökkenésekor növeli azt.

NMC (*network management center*): hálózati irányító központ:

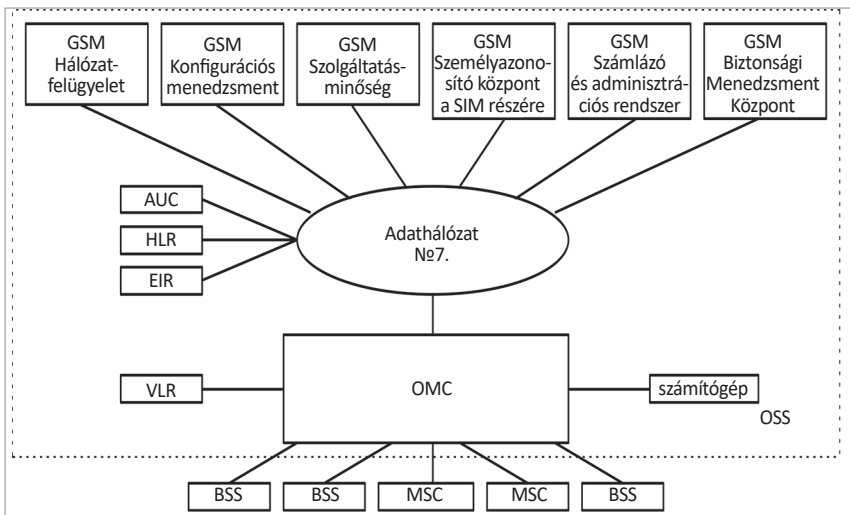
A hálózati irányító központ vezérli a hálózatot, és biztosíthatja a forgalom elemzését, a hívások részleteinek rögzítését, a konfiguráció vezérlését, a hibák észlelését, diagnosztizálását és a karbantartást.⁹⁴

Ezek közül a téma szempontjából a hívások részleteinek rögzítését kell kiemelni.

Az OSS – egy lehetséges – felépítését a 26. ábra mutatja, ám annak ennél részletesebb ismertetését jelen téma nem kívánja meg.

⁹³ Vertel Corporation: *Telecommunications management network (TNM)*. (é. n.)

⁹⁴ Gartner Glossary: *Network management center*.

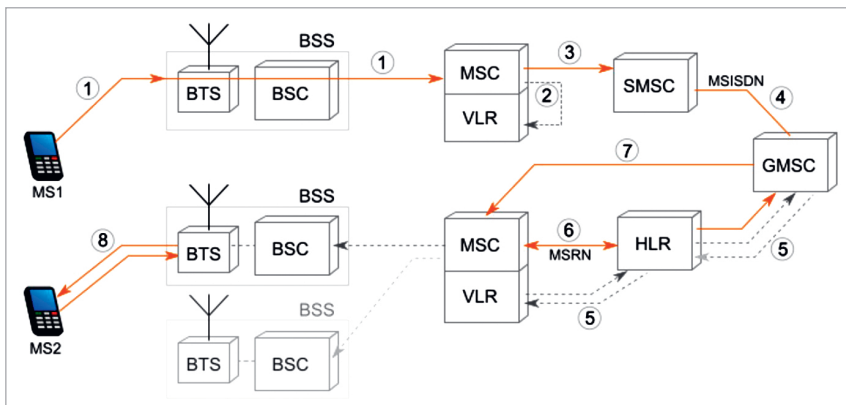


26. ábra: Az OSS felépítése

Forrás: a szerző szerkesztése

Az SMS-rendszer felépítése

A rövid szöveges üzenetek, vagy ismert nevükön SMS-ek célbajuttatásáról egy külön, a fent leírt GSM-hálózathoz kapcsolódó központ, az úgynevezett *short message service center* (SMSC) gondoskodik. Az SMS-ek küldésének folyamatát a 27. ábra szemlélteti.



27. ábra: Az SMS-küldés folyamata

Forrás: a szerző szerkesztése [GSM Functionalities](#) alapján

A folyamat teljes bemutatása a téma szempontjából nem releváns, csupán az alábbiakat célszerű kiemelni. Az SMS-szolgáltatásért felelős SMSC szorosan kapcsolódik a GSM-rendszer többi eleméhez. A megfelelő ellenőrzéseket követően kapja meg az üzenetet és az egyéb szükséges adatokat az MSC-től, elvégzi a fogadó mobilállomás honos hálózatából annak adatainak (például tartózkodási helyének) ellenőrzését, majd ezek alapján továbbítja a megfelelő MSC-nek az üzenetet.

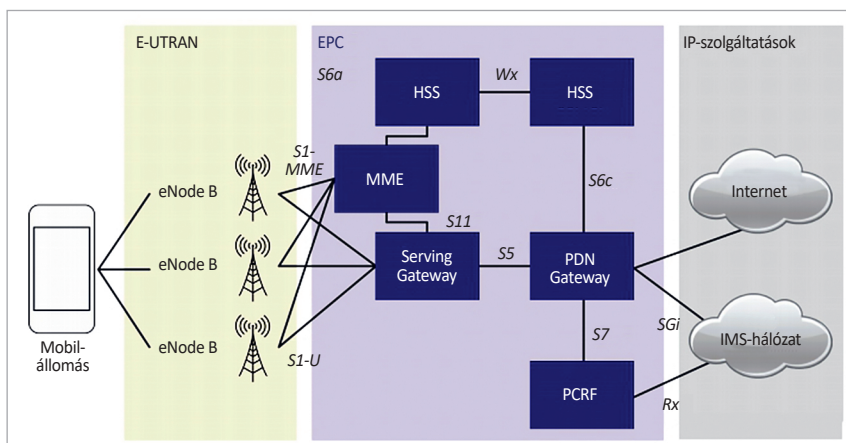
Az adatátvitel és a mobilinternet-szolgáltatás felépítése

Az adatátviteli és a mobilinternet-szolgáltatások kapcsán a korábbi, mára már részben vagy teljesen eltűnt technológiákkal (GPRS [tipikus letöltési sebessége 60-80 kb/s, feltöltési sebessége 20-40 kb/s],⁹⁵EDGE [tipikus letöltési sebessége 180 kb/s, feltöltési sebessége 120 kb/s], UMTS [letöltési sebessége akár 56 Mb/s, feltöltési sebessége akár 22 Mb/s]) jelen fejezet egyáltalán nem foglalkozik, mert azok a téma szempontjából nem képviselnek hozzáadott értéket.

⁹⁵ Athina A. Lazakidou – Konstantinos M. Siassiakos: *Handbook of research on distributed medical informatics and e-health*. Hershey – New York, Medical Information Science Reference, 2009.

A 4G-hálózatoknál használt, úgynevezett LTE- (letöltési sebessége akár 300 Mb/s, feltöltési sebessége akár 150 Mb/s) technológiát is csak olyan mértékig mutatjuk be az alábbiakban, amely elengedhetetlen ahhoz, hogy a nyomozó számára releváns adatok körét meg lehessen ismerni.

Az LTE-hálózaton kizárólag csomagkapcsolt adatátvitel történik, függetlenül attól, hogy azon adatkapcsolatot vagy beszédátvitelt valósítanak-e meg. Ez nagy változás a korábbi (2G-, 3G-) rendszerekhez képest, hiszen azokban eddig a beszédátvitelt a korábban ismertetett hálózat biztosította, míg az adatátvitel egy ehhez kapcsolt IP-alapú hálózaton történt. Ez az első olyan GSM-hálózat, amely a beszédátvitelt is IP-alapon valósítja meg (VoLTE). Maga a hálózat is nagy változáson ment keresztül. Az LTE-hálózat felépítését mutatja be a 28. ábra.



28. ábra: Az LTE-hálózat felépítése

Forrás: a szerző szerkesztése www.3gpteinfo.com/ims-volte-architecture/ alapján

Az LTE-rendszerben a legnagyobb változás az úgynevezett maghálózatban következett be, de – a cellás elv megtartása mellett – azért változott a rádiós (bázisállomás) alrendszer is. A fenti ábrán az EPC (*evolved packet core*) a továbbfejlesztett maghálózatot, az E-UTRAN (*evolved universal terrestrial radio access network*) pedig a továbbfejlesztett rádiós hálózatot jelöli. Ezt a kettőt együtt SAE-nak (*system architecture evolution*) hívják.

A maghálózat az alábbi fő elemekből áll:

MME (*mobility management entity*): mobilitásvezérlő. Az MME az egyetlen ellenőrző elem a hálózatban és ez felelős a legtöbb vezérlő funkcióért is. Ez bonyolítja a mobilállomás és a mobilhálózat közötti kommunikációt, azaz biztosítja a kapcsolat felépítését, fenntartását, lebontását, a biztonságot és a mobilitást, valamint felel az útvonalválasztásért és a mobilállomás helyének lekérdezéséért. Szintén az MME biztosítja az LTE kompatibilitását a korábbi szabványú hálózatokkal.⁹⁶

HSS (*home subscriber server*): honos előfizető-szerver. A HSS tárolja és tartja karban a felhasználók adatait, beleértve a tartózkodási helyét is, de ez felelős a hitelesítésért, engedélyezésért és hozzáférés-kezelésért, amelyhez a szükséges információkat a 3GPP AAA szerverből kapja. Hasonló funkciókat lát el, mint a korábban ismertetett HLR (honos meghatározó regiszter) és AuC (hitelesítési – illetékességet megállapító – központ) együttesen.

3GPP AAA szerver. A 3GPP AAA szerver kiszolgálja a hitelesítési, engedélyezési és hozzáférés-kezelési lekérdezéseket, és AAA proxyszerverként is működhet.

S-GW (*serving gateway*): kiszolgáló átjáró (vagy kilépőpont). Az S-GW létesít kapcsolatot a rádiós hálózat eNode-jai és a maghálózat között. Minden felfelé és lefelé irányú felhasználói csomag (IP-csomag) áthalad rajta. Az S-GW felelős a mobilállomások bázisállomások között történő átadásáért (handover). Ezenkívül információkat tárol, adatot pufferel és számlázási információkat is gyűjt.

P-GW (*packet data network gateway*): adathálózati átjáró (vagy kilépőpont). A P-GW kapcsolja össze a mobilhálózatot a külvilággal (internettel, IMS-sel), biztosítja a felhasználók számára az IP-címek kiosztását, az adatcsomagok szűrését és a garantált szolgáltatásminőség (QoS) vezérlését.⁹⁷

PCRF (*policy and charging rule function*): szabályozási és számlázási egység. A PCRF felelős a számlázási, valamint az előfizetői kapcsolatokat érintő szabályokért és eljárásokért. A PCRF valós időben határozza meg az engedélyezett forgalomtípust, valamint azt is ellenőrzi, hogy hogyan kell elszámlolni az adott

⁹⁶ Pásztor András: *QoS támogatás vizsgálata LTE alapú femtocellák ütemezési kérdéseiben*. TDK-dolgozat. Budapest, Budapesti Műszaki és Gazdaságtudományi Egyetem Villamosmérnöki és Informatikai Kar Híradástechnikai Tanszék, 2012.

⁹⁷ Balog Zsolt: *LTE feletti beszédátvitel monitorozási módszerei a maghálózatban*. TDK-dolgozat. Budapest, Budapesti Műszaki és Gazdaságtudományi Egyetem Villamosmérnöki és Informatikai Kar Távközlési és Médiainformatikai Tanszék, 2016.

forgalmat. A szolgáltatók ezt az információt használják fel számlázási célokra. Így például, amikor a mobilállomás VoLTE hívást indít, a PCRF ellenőrzi, hogy rendelkezik-e az ehhez szükséges előfizetéssel. Amennyiben igen, akkor a PCRF megteszi a szükséges beállításokat az IMS-szolgáltatások eléréséhez.

A rádiós (bázisállomás) alrendszer átalakítását alapvetően a késleltetés csökkentése indokolta. Ezzel a már a 3G-hálózatokban is megkezdett átalakításokat folytatták. Korábban a 3G-hálózatokban ugyanis a BSC-k helyett már megjelentek az úgynevezett Node B-k, a BTS-eket pedig az úgynevezett RNC-k (*radio network controller*, rádióhálózat-vezérlő) váltották fel. Ez a struktúra az LTE-hálózatban még tovább egyszerűsödött. Eltűntek az RNC-k, ezek szerepét a NodeB-k vették át, új nevet, eNode B (*evolved node B*) kapva. Az eNode B közvetlenül kapcsolódik a maghálózathoz, ez lát el minden rádiós hozzáféréssel, átvitelrel, biztonsággal, mobilitással, mérésekkel és erőforrás-gazdálkodással kapcsolatos feladatot, elosztott rádiós hálózatmenedzsmentet valósítva meg. Ez a korábbi GSM-hálózatoknál még központi vezérlés keretében történt. Mindezek mellett természetesen a korábban ismertetett cellás elrendezés megmaradt.

A kiberyomozó számára releváns adatok a mobiltelefon-hálózatokban

A nyomozás során a mobiltelefon-szolgáltató hálózatából a fix (helyhez kötött) telefonhálózatoknál megismert adatok mellett rengeteg más, a nyomozó számára értékes adat is kinyerhető. Ilyenek lehetnek többek között:

- az előfizetők adatai (név, lakcím, szerződéses adatok, számlázási adatok);
- számlafizetéséhez kötődő adatok;
- az előfizető egyenlege;
- előre fizetéses (úgynevezett *pre-paid*) kártyák feltöltési szokásaira vonatkozó adatok;
- pre-paid kártyák éves adategyeztetésére vonatkozó adatok;
- egy előfizető nevén lévő előfizetések száma, adatai;
- híváslisták (az adott előfizető által kezdeményezett, fogadott hívások adatai, adott esetben a sikertelen hívások adatai – hívó, hívott fél azonosítói, hívás kezdeti időpontja, időtartama);
- bővített híváslisták (az előző adatok mellett például cellaadatok, IMEI-kód is megjelenhet);

- cellaforgalmi listák (egy adott cellában, adott időben forgalmazó vagy feljelentkezett készülékek azonosítói: IMSI, IMEI, MSISDN);
- IMSI-IMEI összerendelési adatok (azaz adott IMEI-számú készülékben milyen SIM-kártyá(ka)t használtak, vagy adott SIM-kártyát milyen IMEI-számú készülék(ek)ben használták);
- cellatérkép (bázisállomások pontos földrajzi helye és az általuk lefedett területek);
- meghatározott földrajzi helyet lefedő cellák azonosítói;
- mozgási adatok (egy adott SIM-kártya mozgására vonatkozó adatok);
- kiegészítő szolgáltatásokhoz (például SMS-fizetéshez) kapcsolódó adatok;
- mobilinternet használatához kapcsolódó adatok (például IP-cím, portszám, *MAC address* stb.);
- kapcsolódó szolgáltatásokhoz tartozó adatok (például e-mail-cím);
- megfelelő engedélyek birtokában:
 - az engedélyezett telefonok forgalmazásának lehallgatása,
 - IP-forgalom lehallgatása,
 - e-mailek tartalmának megismerése.

A mobiltelefon-hálózatokból a nyomozók számára kinyerhető információk száma jelentősen magasabb, mint bármely korábbi hírközlési hálózat esetén. De nemcsak ez, hanem a lehetséges felhasználható információk darabszáma is jelentősen magasabb, mint bármely más hírközlési hálózat esetében. Éppen ezért azok feldolgozására mindenképp valamilyen gépi eljárást kell igénybe venni.

Meg kell jegyezni, hogy az egyes szolgáltatók hálózataiból az eltérő felépítés és az eltérő beállítások miatt – a jogszabályok által kötelezően előírt adatokon kívül – eltérő adatokhoz lehet hozzájutni. Éppen ezért bármely, nem „rutinügy” esetén érdemes a szolgáltató szakembereivel konzultálni a kinyerhető adatok köréről és időtartamáról, hiszen ebben az esetben is igaz, hogy adott esetben a szolgáltató a fent felsoroltak mellett más adatokat, információkat is képes biztosítani a nyomozók számára.

A mobilállomások – azok között is elsősorban az okostelefonok – sok, a nyomozó számára értékes információt tárolnak. Az itt elérhető információkkal és azok kinyerésével jelen könyv későbbi fejezetei foglalkoznak.

Összefoglalás

Jelen fejezet bemutatta azokat a hírközlési hálózatokat, amelyek ma a legrelevánsabbak a nyomozók számára. Az egyes hálózatok felépítését olyan szintig ismertettük, amely lehetővé tette az adott hálózat működési sajátosságainak megértését és az abból kinyerhető, a nyomozó számára fontos információk bemutatását.

A hírközlő hálózatokból a nyomozók munkájuk során nagyrészt rutinszerűen kell hogy adatokat nyerjenek ki. Ez azt jelenti, hogy az esetek jelentős részében jól ismert kérdéseket fognak feltenni, amelyekre tudják, hogy válaszokat és jól használható adatokat fognak kapni a szolgáltatóktól. Ugyanakkor nem szabad figyelmen kívül hagyni azt a tényt, hogy mindig lesznek nem „rutinügyek” vagy olyanok, amelyek megoldása kreativitást, a korábbiaktól eltérő információigénylést és -feldolgozást, valamint ehhez a hírközlési hálózatok bizonyos ismeretét igényli. Ezekben az esetekben mindig érdemes és célszerű a lehetőségekről a szolgáltató erre a célra dedikált – általában biztonsági – szakembereivel konzultálni.

Vákát

Az infokommunikációs hálózatok – az IT-hálózatok

Bevezetés

Az emberek az alábbi hálózatokat használhatják:

- postai rendszer,
- telefonhálózat,
- tömegközlekedési hálózat,
- vállalati számítógép-hálózat,
- internet.

A hálózatokon információkat osztanak meg és különféle eljárásokat használnak az információk áramlásának irányításához. Az információ úgy jut el a hálózatban egyik helyről a másikra, hogy a célállomást sokszor eltérő útvonalakon közelíti meg. Például a tömegközlekedési hálózat hasonló az adathálózathoz. Az autók, tehergépkocsik és más járművek olyanok, mint a hálózatban áramló üzenetek. Minden járművezető meghatároz egy indulási pontot (forrásállomás) és egy végpontot (célállomás). Ezen rendszeren belül vannak olyan szabályok, mint a stoptáblák vagy közlekedési lámpák, amelyek irányítják a forrástól a célig áramló forgalmat.

IT-hálózatok

A számítógép-hálózatok olyan hálózatba kötött eszközök összességei, amelyek valamilyen átviteli közeg segítségével kommunikálnak egymással. Boda István ennél pontosabb megfogalmazása szerint: „A számítógépes hálózatok egymással (fizikailag) összekapcsolt számítógépeket jelentenek, amelyek az őket összekapcsoló vonalakon vagy csatornákon képesek egymással adatokat cserélni (kommunikálni).”⁹⁸

A számítógép-hálózatok is szabályokat alkalmaznak az állomások közötti adatforgalom irányításához. Az állomás a hálózaton adatokat küld és fogad. Némelyik eszköz állomásként és perifériaként is működhet. Például egy

⁹⁸ Boda (2019): i. m.

nyomtató, amely a hálózaton lévő laphoz csatlakozik, periféria. Ha a nyomtató közvetlenül a hálózathoz csatlakozik, akkor állomás.

Számos különböző eszköz kapcsolódhat egy hálózathoz:

- asztali számítógép,
- laptop,
- táblagép,
- okostelefon,
- nyomtató,
- fájl- és nyomtatókiszolgáló,
- játékkonzol,
- háztartási berendezések.

A számítógép-hálózatokat világszerte használják az üzleti életben, otthonokban, iskolákban, és állami szervezeteknél. Az egyes hálózatok az interneten keresztül kapcsolódnak egymáshoz. Egy hálózat több különböző adat- és erőforrástípust képes megosztani:

- szolgáltatásokat, például nyomtatást vagy lapolvasást,
- tárhelyet, például merevlemezeket vagy optikai meghajtókat,
- alkalmazásokat, például adatbázisokat,
- más számítógépeken tárolt információt,
- dokumentumokat,
- naptárakat, a számítógép és az okostelefon közötti szinkronizáció érdekében.

Az eszközök csatlakoztatására különböző megoldások léteznek:

- *Rézkábelezés* – elektromos jeleket használ az adatok átviteléhez az eszközök között.
- *Optikai kábelezés* – üveg- vagy műanyag szálakat használ az információk átviteléhez fényimpulzusok formájában.
- *Vezeték nélküli kapcsolat* – rádiójeleket, infravörös technológiát vagy műholdas átvitelt használ.

Jellemzők és előnyök

A számítógépek hálózatba kapcsolásának legnagyobb előnye, hogy ezáltal csökkenthetők a kiadások és növelhető a hatékonyság. Egy hálózatban az erőforrások megosztásával csökken a többszörös adattárolás, illetve az adatvesztés kockázata.

Célok

Erőforrás-megosztás. A megbízhatóság növelése. Sebességnövelés. Emberi kommunikáció.

A számítógép-hálózat tipikusan számítógépekből és perifériás elemekből (például hálózati nyomtató), hálózati kapcsolóelemekből, a fizikai összeköttetést megvalósító eszközökből (kábelekből) és a különböző hálózati alkalmazásokat megvalósító programokból (szoftverekből) épül fel.

Az internet fogalma

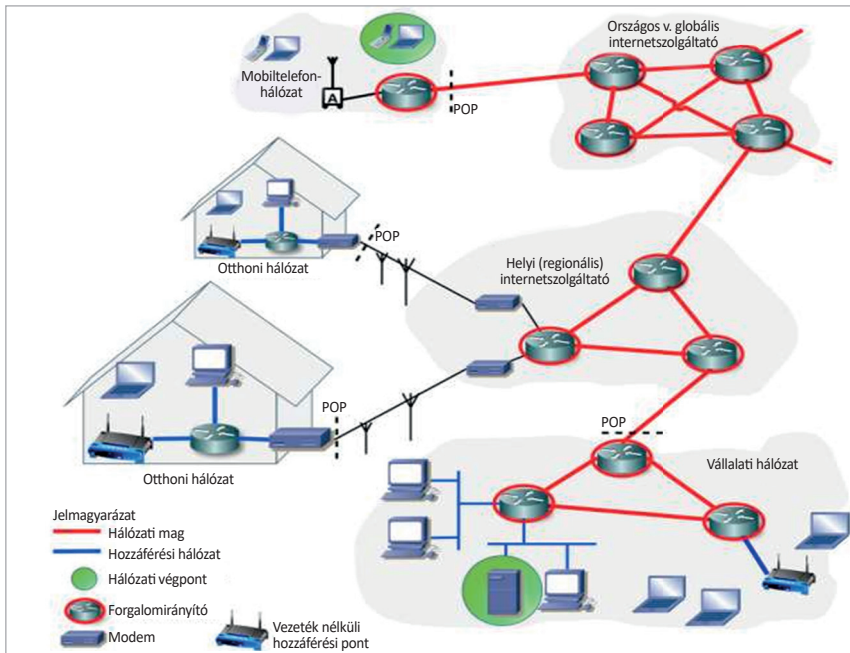
Az internet olyan számítógép-hálózat, amely számítástechnikai eszközök millióit köti össze az egész világon. Amíg korábban ezek a számítástechnikai eszközök elsősorban asztali számítógépek, Linux-munkaállomások és szerverek voltak, addig ma már egyre több végrendszert kapcsolnak az internethez, mint a PDA, tv-k, laptopok stb. Ezeket ma már hostoknak vagy végrendszereknek (*end systems*) nevezzük.

A végrendszereket kommunikációs adatkapcsolatok (*communication link*) és csomagkapcsolók (*packetswitch*) hálózata köti össze.

A különböző összeköttetések különböző sebességgel képesek adatokat továbbítani (átviteli sebesség, *transmissionrate*). Ezeket bit/sec-ban mérjük.

Amikor az egyik végrendszer adatot szeretne küldeni egy másiknak, a küldő végrendszer feldarabolja, szegmentálja az adatokat, és minden darabhoz fejreszbájtokat ad. Ezeket az információcsomagokat packetnek nevezzük.⁹⁹

⁹⁹ James F. Kurose – Keith Ross: *Számítógép-hálózatok működése. Alkalmazásorientált megközelítés*. Budapest, Panem, 2009.



29. ábra: Számítógép-hálózatok működése

Forrás: Kurose – Ross (2009): i. m.

A TCP/IP-protokoll (transmission control protocol/internet protocol)

A TCP és az IP a valóságban az a két fő protokoll, amely az internet alapját képezi.

A TCP/IP (átvitelvezérlő protokoll/internetprotokoll) azokat a szabályokat tartalmazza, amelyek meghatározzák a számítógépek közötti internetes kommunikáció módját. A TCP a megbízható adattovábbítás elsődleges internetes protokollja. Az IP pedig olyan címzési rendszer, amely biztosítja az adatok forrástól célig történő eljutását.

A *transmission control protocol* (átvitelvezérlési protokoll) feladata a továbbítandó adathalmaz darabolásával adatsomagok készítése és címkézése.

Az *internet protocol* (internetprotokoll) meghatározza az útválasztók és a végrendszerek között a küldött és a fogadott csomagok formátumát. A csomagok irányítása, a kommunikációban részt vevők azonosítása a feladata.

Az IP- (internetprotokoll-) cím

Az IP-cím egy olyan szám, amelyet a hálózat eszközeinek azonosítására használnak. Minden eszköznek egyedi IP-címmel kell rendelkeznie a hálózaton, hogy más hálózati eszközökkel kommunikálhasson. Korábbi meghatározásunk szerint az állomás olyan eszköz, amely adatokat küld és fogad a hálózaton. A hálózati eszközök pedig olyan berendezések, amelyek adatokat mozgatnak a hálózaton.

Az IP-cím 4 byte-ból, azaz 32 bitből áll. Leggyakrabban pontozott decimális formában írják: a.b.c.d alakban, ahol mind a négy tag 0-tól 255-ig vehet fel értéket. Például 195.199.49.128.

Az IP-alapú hálózatokban minden gépnek, sőt minden hálózati interfésznek egyedi azonosítója van: az IP-cím. Ha egy hálózatban az interfésznek a TCP/IP-alapú kommunikációban mindig ugyanaz az IP-címe, akkor *statikus IP-címről*, ha az IP-cím egy kiszolgálóhoz való kapcsolódáskor alakul ki, és az esetenként különböző, akkor *dinamikus IP-címről* beszélünk.

Az IP jellemzői

Az IP a TCP/IP-protokollkészlet hálózati rétegbeli szolgáltatása.

Az IP-t kis többletterhelésű protokollnak tervezték. Ennek megfelelően csak azokat a funkciókat tartalmazza, amelyek feltétlenül szükségesek ahhoz, hogy egy csomag összekapcsolt hálózatokon keresztül a forrástól a célig eljusson. A protokollnak nem feladata a csomagok nyomon követése és felügyelete. Ezeket a funkciókat szükség esetén más rétegbeli protokollok biztosítják.

Az IP összeköttetés-mentes

A hálózati réteg feladata a csomagok állomások közötti továbbítása a hálózatra nézve a lehető legkisebb többletterheléssel. A hálózati réteg nem foglalkozik a csomagban zajló kommunikáció típusával, vagy tudatában sincs annak. Az IP

összeköttetés-mentes, ami azt jelenti, hogy az adatküldést megelőzően a végpontok között nem épül ki kapcsolat. Az összeköttetés-mentes kommunikáció hasonló ahhoz, mint amikor egy levelet küldünk anélkül, hogy arról a címzettet előre értesítsenénk.

A MAC- (*media access control*) cím az állomás hálózati csatolójához (*network interface card* – NIC) tartozik, és fizikai címként ismert. A fizikai cím változatlan marad, tekintet nélkül arra, hogy az állomást hová helyezik el a hálózatban, hasonlóan az újjlenyomathoz, amely a személynél marad, függetlenül attól, hová is megy.

A MAC-cím hat darab kétjegyű hexadecimális számból áll, amelyeket kötőjellel (-) vagy kettősponttal (:) választunk el, például: 00-26-6C-FC-D5-AE. Egy hexadecimális számjegy a 0–9 és az A–F intervallumból veheti fel értékeit.

Az IP-cím hasonló az emberek levelezési címéhez. Logikai címként ismert, mert logikailag rendelődik az állomáshoz, elhelyezésétől függően. Az IP- vagy hálózati cím a helyi hálózaton alapul, és a hálózati rendszergazda rendeli a munkáállomásokhoz. Ez a folyamat hasonló ahhoz, ahogy a helyi önkormányzat – a város vagy falu és környékének logikai jellemzői alapján – osztja ki az utcaneveket és házsámokat.

Az IPv4 és IPv6

Az 1990-es évek elején, amikor az IPv4-címek kimerülésével kapcsolatos problémák nyilvánvalóvá váltak, az IETF (*internet engineering task force* – internet mérnöki munkacsoport) más megoldásokat kezdett keresni. Ez vezette el a kutatásokat oda, amit ma úgy ismerünk: IPv6. Napjainkban az IPv6 az IPv4 mellett működik, és lassan kezdi azt felváltani.

Az IPv4-cím 32 bináris számjegyből áll, így címtartománya 2^{32} különböző címet tartalmaz. Ennek decimális értéke hozzávetőleg 4 milliárd, míg a 128 bináris számjegyből álló IPv6-cím címtartományának mérete 2^{128} . Tíz-es számrendszerben jelölve ez megközelítőleg egy hármast követő 38 darab nulla. Ez esetben a személyenként elérhető címek száma körülbelül 10^{30} . Ha az IPv4 címtartományát egy üveggolyóval szemléltetnénk, az IPv6 címtartománya egy majdnem Szaturnusz-méretű gömb lenne.

IPv4

Az IPv4-cím 32 bináris számjegy (egyesekek és nullák) sorozatából áll. Az emberek számára elég nehéz a címek bináris alakjának olvasása. Éppen ezért a 32 bitet négy 8 bites egységbe, az úgynevezett oktettekbe csoportosítjuk. Az IPv4-címet még ebben a csoportosított formában sem könnyű elolvasni, leírni és megjegyezni, ezért minden 8 bites egységet decimális számértékként jelenítünk meg, és az oktettek közé pontot teszünk. Ezt a formátumot pontozott decimális jelölésnek hívjuk.

Amikor egy állomásnak IPv4-címet adunk, pontozott decimális számként állítjuk be, például 192.168.1.5. Képzeljük el, ha a 32 bites bináris megfelelőjét kellene begépelnünk: 110000001010100000000000100000101! Ha csak egy bitet is félreütünk, a cím már más lesz, és az állomás valószínűleg nem lesz képes kommunikálni a hálózaton.

A logikai 32 bites IPv4-cím hierarchikus, és két részből áll. Az első a hálózatot, a második az állomást azonosítja az adott hálózaton. Mindkét rész egyformán fontos. Például ha egy állomás IPv4-címe a 192.168.18.57, az első három oktet, a 192.168.18 jelöli a cím hálózati részét, az utolsó oktet, az 57 pedig a hálózaton belül az állomást. Ez az úgynevezett hierarchikus címezés, mert a forgalomirányítóknak csak azt kell tudniuk, hogyan lehet elérni az egyes hálózatokat, nem kell ismerniük minden állomás helyét. A forgalomirányító olyan hálózati eszköz, amely az adatcsomagokat továbbítja a hálózaton a cél felé.

A számítógép-hálózat előnyei és céljai

A számítógép-hálózat lehetőséget ad a különböző berendezések, perifériák, programok és adatok közös használatára, azaz a külön-külön is meglévő erőforrások megosztására. Ezek az erőforrások a hálózati felhasználók fizikai helyétől függetlenül bárki számára elérhetővé válnak. Lehetőséget ad továbbá a rendszerben lévő eszközök teljesítményének egyenletesebb megosztására, ami által a kialakított rendszer nagyobb biztonsággal működik.

Az egymással kapcsolatban álló számítógépek számítógépes hálózatot képeznek. A gépek egymáshoz kapcsolása a következő előnyökkel jár:

- gyorsabb kommunikációt biztosít a felhasználók között (levelezés, online beszélgetés);
- lehetővé teszi az egyes hardvereszközök (nyomtató, szkennerek, winchester stb.) közös használatát (hardveres erőforrások megosztása);

- megadja a közös adatok (adatbázisok) használatának lehetőségét;
- párhuzamos munkavégzés biztosítása;
- üzem- és adatbiztonság fokozása (egy-egy berendezés meghibásodása esetén is a rendszer működőképességének biztosítása).

LAN (local area network)

Az adathálózatok folyamatosan fejlődnek mind komplexitásban, mind felhasználásban és kivitelben. Egy számítógépes hálózatot a következő jellemző tulajdonságokkal azonosíthatunk:

- a kiszolgált terület,
- az adattárolás módja,
- az erőforrások kezelésének módja,
- a hálózat szervezésének módja,
- a felhasznált hálózati eszközök típusa,
- az eszközök összeköttetéséhez használt átviteli közeg típusa.

A különböző hálózatok az adott típusra jellemző névvel rendelkeznek. Egy önálló hálózat általában egy egységes földrajzi területet fed le, és egy közös irányítás alatt álló szervezet felhasználói számára nyújt szolgáltatásokat és alkalmazásokat. Az ilyen hálózatot helyi hálózatnak (*local area network* – LAN) nevezzük. A LAN-ok több helyi hálózathoz is állhatnak.

A LAN-hoz tartozó helyi hálózatok egy adminisztrációs csoport felügyelete alá tartoznak. Ez a csoport irányítja a hálózat biztonsági és hozzáférés-vezérlési házirendjét. Ebben a megközelítésben a *helyi* szó inkább egy logikailag egységes szabályozásra utal, mint az egymáshoz való fizikai közelségre. A LAN-hoz kapcsolódó eszközök lehetnek fizikailag közel egymáshoz, de ez nem általános követelmény.

Egy LAN lehet olyan kicsi, mint egy háztartásba vagy kisebb irodába telepített egyszerű helyi hálózat. Napjainkban azonban a definíció olyan összekapcsolt helyi hálózatokra is kiterjed, amelyek több helyen és épületben lévő, több száz eszközből állnak.

Vezeték nélküli hálózatok (WLAN)

A vezeték nélküli LAN (*Wireless LAN* – WLAN) olyan helyi hálózat, amely rádióhullámokat használ a hálózati eszközök közötti adattovábbításra. A hagyományos helyi hálózatokban az eszközök rézkábelek segítségével kapcsolódnak egymáshoz, azonban némely környezetben a rézkábelezés nem lenne megvalósítható, kívánatos vagy akár lehetséges. Ezekben az esetekben vezeték nélküli eszközök küldik és fogadják az adatokat rádióhullámok segítségével. Mint a LAN-ok esetében, a WLAN-oknál is megoszthatunk erőforrásokat, például fájlokat, nyomtatókat és az internet-hozzáférést.

Egy WLAN-ban, az adott területen belül a vezeték nélküli eszközök hozzáférési pontokhoz kapcsolódnak. A hozzáférési pontok általában rézkábelrel csatlakoznak a hálózathoz. Ahelyett, hogy minden állomás számára rézkábelezést biztosítanánk, csak a vezeték nélküli hozzáférési pontokat csatlakoztatjuk a hálózathoz. A WLAN tartománya (lefedettsége) az alkalmazott technológiától függően változhat a beltéren számított 30 métertől a szabadtéren elérhető sokkal nagyobb távolságokig.

Személyi hálózatok (PAN)

A személyi hálózat (*personal area network* – PAN) egy egyén közvetlen környezetében található eszközöket köt össze, például egeret, billentyűzetet, nyomtatót, okostelefont és táblagépet. Ezek az eszközök a legtöbb esetben egyetlen állomáshoz csatlakoznak Bluetooth technológiával.

A Bluetooth egy vezeték nélküli technológia, amely egymáshoz közeli eszközök kommunikációját teszi lehetővé. Egy Bluetooth-eszköz legfeljebb hét másik Bluetooth-eszközhöz tud csatlakozni. A műszaki specifikációt az IEEE 802.15.1 szabvány tartalmazza. A Bluetooth-eszközök hang- és adatátvitel kezelésére alkalmasak. A 2,4–2,485 GHz közötti frekvenciatartományban működnek, amelyet ISM- (*industrial, scientific and medical*, ipari, tudományos és orvosi) sávként ismerünk. A Bluetooth-szabvány tartalmazza az adaptív frekvenciaugrást (*adaptive frequency hopping* – AFH), amely lehetővé teszi a jelek tartományon belüli frekvenciaváltását, csökkentve ezzel a interferencia esélyét több Bluetooth-eszköz esetén.

A nagyvárosi hálózatok (MAN)

A nagyvárosi hálózat (*metropolitan area network* – MAN) nagy telephelyre vagy egy egész városra terjed ki. Optikai vagy vezeték nélküli technológiával összekapcsolt, több különböző épületből áll. A kommunikációs összeköttetések és berendezések általában egy üzemeltetői csoport vagy egy internetszolgáltató birtokában vannak, akik a szolgáltatást a felhasználók számára elérhetővé teszik. A MAN nagy sebességű hálózatként is működhet, lehetővé téve a területén található erőforrások megosztását.

Nagy kiterjedésű hálózatok (WAN)

A nagy kiterjedésű hálózatok (*wide area network* – WAN) földrajzilag elkülönülő helyi hálózatokat kötnek össze. A legjobb példa rá az internet. Az internet egy óriási WAN, amely milliónyi összekötött LAN-ból áll. Vállalati vagy kutatási hálózatok összeköttetésére szintén WAN-technológiát használnak. A különböző helyen lévő LAN-okat távközlési szolgáltatók (*telecommunications service provider* – TSP) segítségével kötik össze.

Egyenrangú hálózatok

Egyenrangú hálózat (*peer-to-peer network*) esetén a számítógépek között nincs hierarchia vagy kizárólagos kiszolgáló. Minden eszköznek (ügyfélnek) azonos lehetősége és kötelezettsége van. Az egyéni felhasználók felelősek a saját erőforrásaikért, és eldönthetik, mely adatokat és eszközöket telepítik vagy osztják meg. Mivel az egyéni felhasználók felelősek a saját számítógépük erőforrásaiért, ezért a hálózatban nincs központi irányítás vagy adminisztráció.

Az egyenrangú hálózatok legfeljebb tíz számítógép esetén működnek hatékonyan, azonban lehetnek nagyobb hálózatok részei is. A felhasználók, még egy nagy ügyfélhálózatban is, megoszthatják erőforrásaikat közvetlenül más felhasználókkal hálózati kiszolgáló közbeiktatása nélkül. Ha otthonunkban több számítógéppel rendelkezünk, felállíthatunk egy egyenrangú hálózatot. Megoszthatunk fájlokat más számítógépekkel, küldhetünk üzeneteket a számítógépek között, és nyomtathatunk megosztott nyomtatóra.

Az egyenrangú hálózatoknak hátrányai is vannak:

- Nincs központosított hálózati adminisztráció, ami megnehezíti a hálózati erőforrások felügyeletét.
- Nincs központosított védelem, ezért minden számítógépnek külön biztonsági intézkedéseket kell használnia az adatok védelmére.
- A számítógépek számának növekedésével a hálózat egyre bonyolultabbá és nehezen kezelhetővé válik.
- Valószínűleg nincs központi adattárolás sem. Különálló biztonsági másolatokat kell kezelni, ami az egyéni felhasználók felelőssége.

Ügyfélkiszolgáló hálózat

A kiszolgálók olyan programokat futtatnak, amelyek az ügyfeleknek különböző szolgáltatásokat nyújtanak, például e-mail vagy weboldalak elérése. Minden szolgáltatáshoz külön kiszolgálóprogram szükséges. Például ha egy hálózaton web-szolgáltatást szeretnénk biztosítani, akkor a szerveren webkiszolgáló programot kell telepíteni.

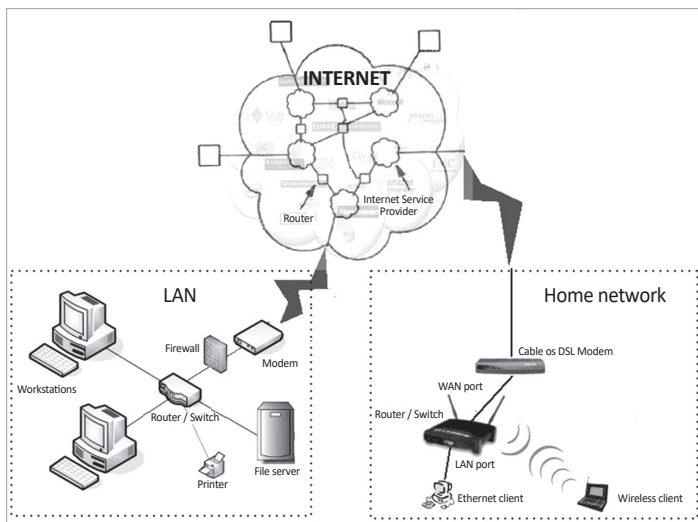
Az ügyfélkiszolgáló (*client-server*, kliensszerver) hálózatban az ügyfelek információt vagy szolgáltatásokat kérnek a kiszolgálótól, a kiszolgáló pedig biztosítja a kért információt vagy a szolgáltatást az ügyfél számára. A kiszolgálók ezekben a hálózatokban gyakran valamilyen adatfeldolgozó feladatot végeznek az ügyfélgépek számára. Például szűrést hajtanak végre egy adatbázison, mielőtt a kért információt eljuttatná az ügyfélnek. Ez központi hálózati adminisztrációt tesz lehetővé, ami megkönnyíti a hálózati erőforrások felügyeletét.

Egy kiszolgálóprogramot futtató számítógép egyszerre több felhasználónak is nyújthat szolgáltatást. Ezentúl egy számítógép egyszerre többféle kiszolgálóprogramot is futtathat. Otthon vagy kisvállalatok esetén szükséges lehet, hogy egy számítógép egyaránt legyen fájlkiszolgáló, webkiszolgáló és levelező-kiszolgáló. Nagyvállalati környezetben az alkalmazottak külön-külön számítógépekhez férhetnek hozzá, amelyek egyike például egy e-mail-szerver. Ezt kizárólag levelek küldésére, fogadására és tárolására használják. Az alkalmazott számítógépén futó levelező ügyfélprogram üzenetet küld a kiszolgálónak, amelyben lekéri az olvasatlan leveleket. A kiszolgáló ezután válaszüzenetében elküldi a kért leveleket az ügyfélnek.

Egyetlen számítógép többféle ügyfélprogramot is tud futtatni. Minden igényelt szolgáltatáshoz külön ügyfélprogram szükséges. Ha egy gépen több ügyfélalkalmazás fut, a kliens egyszerre több kiszolgálóhoz is csatlakozhat.

Például egy felhasználó megnézheti az elektronikus levelezését és nézegethet egy weboldalt, miközben azonnali üzenetküldőn beszél és internetes rádiót hallgat.

A kliensszerver modell, a központosított hálózati adminisztráció segítségével, megkönnyíti a hálózati erőforrások felügyeletét. A hálózati adminisztrátor biztonsági mentéseket és védelmi intézkedéseket valósít meg. Ugyancsak hálózati adminisztrátor kezeli a felhasználói hozzáférést a hálózati erőforrásokhoz. A hálózat adatait központi fájlkiszolgálón tárolják. Központi nyomtatókiszolgáló kezeli a hálózat megosztott nyomtatóit. Csak a megfelelő jogokkal rendelkező felhasználók érhetik el a fájlokat és a megosztott nyomtatókat.



30. ábra: Az internet felépítése

Forrás: a szerző szerkesztése

A hálózat alkotóelemei

A hálózat alkotóelemei négy részből állnak:

1. üzenetek,
2. eszközök,
3. átviteli közegek,
4. szolgáltatások.

Üzenetek (messages)

Ha le szeretnénk egyszerűsíteni a hálózati kommunikációt, akkor az üzeneteket bitekre kódoljuk, majd az így kapott bináris számsorozatot továbbítjuk a hálózat bonyolult és összetett rendszerén keresztül a célállomáshoz. A célállomás a bináris kódsorozatot olvasható üzenet formátumban dekódolja, így ezzel létrejön a kommunikáció.

Eszközök (devices)

A hálózati eszközök alá tartoznak mindazon berendezések, amelyek a hálózati kommunikációt elősegítik olyan módon, hogy az üzeneteket az előírt szabályok alkalmazásával feldolgozzák és továbbítják a hálózat átviteli közegére. Működésükhöz külső áramforrás szükséges. Ezeket a berendezéseket aktív eszközöknek hívjuk.

Átviteli közegek (media)

A hálózatok passzív, vagyis külső áramforrás felhasználása nélküli, elemenként használt átviteli közegek, mindazok az előző fejezetben tárgyalt vezetékes és vezeték nélküli megoldások (analóg és digitális), amelyek a bináris kódsorozatot valamilyen fizikai jel formájában továbbítják a két pont között (például wifihálózatban a levegőfrekvencia). Ezek az átviteli közegek, valamint a kapcsolódásukat biztosító panelek, csatlakozók stb. képezik a hálózatok passzív elemeit.

Szolgáltatások (services)

A hálózati szolgáltatások azok a számítógépes szoftverek, amelyek a hálózaton keresztül kommunikációt kezdeményeznek egy távoli célállomással. Idetartozik számtalan szolgáltatás, amelyek egy meghatározott szabálygyűjtemény alkalmazásával kommunikálnak a hálózat többi végpontjával. A kommunikáció többnyire csak akkor valósulhat meg, ha mind a két fél betartja a szabványban előírtakat, amelyek az úgynevezett protokollok formájában valósulnak meg.

Gyakran használt portok és protokollok

TCP és UDP

A protokoll meghatározott szabályok készlete. Az internetprotokollok olyan szabálykészletek, amelyek a hálózaton lévő számítógépek közötti kommunikációt vezérlik. A protokoll-leírások meghatározzák a továbbított üzenetek formátumát. A postai hálózaton küldött levél szintén protokollokat használ, amelyek egy része például a kézbesítési cím szabványos helyét határozza meg a borítékon. Ha a címet rossz helyre írják, a levelet nem lehet kézbesíteni.

Az időzítés kritikus a hálózat megbízható működése szempontjából. A protokollok mindig meghatározzák, hogy mennyi időn belül kell megérkeznie az üzeneteknek, így a számítógépek nem várnak a végtelenségig egy esetleg elveszett üzenetre. Következésképpen a rendszerek egy vagy több időzítőt tartanak fenn az adatátvitel ideje alatt. Ezenfelül a protokollok meghatározott eljárásokat indítanak, ha a hálózat nem felel meg az időzítési előírásoknak.¹⁰⁰

A protokollok legfontosabb feladatai a következők:

- a hibák felismerése és kezelése;
- az adatok tömörítése;
- az adatok feldarabolásának és becsomagolásának meghatározása;
- az adatsomagok címezése;
- az adatsomagok küldésének és érkezésének szabályozása.

Az internethez kapcsolódó eszközök és állomások a TCP/IP-protokollkészlet segítségével kommunikálnak egymással. Az adatátvitelhez szükséges két leggyakoribb protokoll a TCP és az UDP.

Egy hálózat tervezése során előre el kell döntenünk, milyen protokollokat fogunk alkalmazni. Néhány protokoll gyártófüggő és csak bizonyos eszközökön működik, mások viszont nyílt szabványúak és többféle eszközön is használhatók.

¹⁰⁰ Szabó Bálint – Márfoldi Endre: *Számítógépes hálózatok*. Eger, Eszterházy Károly Főiskola, 2011.

TCP- és UDP-protokollok és portok

A TCP/IP-protokollkészlet engedélyezésével más protokollok is kommunikálhatnak a megfelelő portokon keresztül. Például a HTTP alapértelmezés szerint a 80-as portot használja. A port egy számszerű azonosító, amely meghatározott üzenetváltások nyomon követésére szolgál. Minden üzenet, amelyet egy állomás elküld, tartalmaz egy forrás- és egy célportot.

Az interneten vagy egy hálózaton az alkalmazások ezeknek a protokolloknak és portoknak a segítségével kommunikálnak. Némely szoftveralkalmazás olyan szolgáltatásokat nyújt, mint weboldalak tárolása, elektronikus levél küldése vagy fájlok átvitele. Ezeket egy vagy több kiszolgáló is biztosíthatja. Az ügyfelek a jól ismert portokat (*well-known ports*) használják az egyes szolgáltatásokhoz, azaz az ügyfélkérések ezeket a szolgáltatásokat egy adott célporttal azonosíthatják.

A hálózatok és az internet működésének megértéséhez tisztában kell lennünk a gyakran használt protokollokkal és a hozzájuk rendelt portokkal. Az ügyfelek ezeket a protokollokat használják távoli hálózati eszközök csatlakoztatásakor, weboldalak URL-címeinek IP-címmé alakításakor és adatállományok átvitelénél. Ahogy bővülnek az IT világában szerzett tapasztalataink, nyilván további protokollokkal is találkozunk majd, de azok nem olyan gyakoriak, mint az itt ismertetettek.¹⁰¹

Hálózati eszközök

Modemek

A világ különböző tájain élő emberek közötti több millió üzenetváltás a világhálón zajlik. A hálózat elemeinek szabványosítása lehetővé teszi a különböző gyártóktól származó eszközök együttműködését. Informatikai szakemberként fontos, hogy pontosan értsük a magán- és üzleti élet folyamatait támogató eszközök célját és működését.

A modem olyan elektronikus eszköz, amely internetcsatlakozást biztosít egy ISP-n keresztül. A digitális adatokat analóg jelekké alakítja, hogy azok a telefonvonalon keresztül továbbíthatók legyenek. Mivel az analóg jelek fokozatosan és folyamatosan változnak, így hullámként ábrázolhatók. A digitális jeleket

¹⁰¹ Vö. Tanenbaum–Wetherall (2013): i. m.

bináris adatként (bit) ábrázoljuk. A digitális jeleket a telefonvonalon történő átvitelhez hullámformává kell alakítani. Ezt a fogadó oldalon egy modem ismét bitekké alakítja, hogy a célállomás képes legyen értelmezni az adatokat.

A fogadó modem tehát az analóg jeleket a számítógép számára értelmezhető digitális adatokká alakítja vissza. Az analóg jelek digitálissá konvertálása, majd visszaalakítása az úgynevezett moduláció/demoduláció. A hibafelismerési és hibajavítási protokollok fejlődésével a telefonvonalakon jelentkező zaj és interferencia lecsökkent vagy teljesen megszűnt, így a modemalapú adatátvitel megbízhatósága is jelentősen megnőtt.

A belső modem az alaplap egy bővítőhelyébe illeszthető. Külső modem soros vagy USB-porton keresztül csatlakoztatható a számítógéphez. A modem megfelelő működéséhez illesztőprogramra és a portok beállítására van szükség.

A nyilvános telefonhálózatot használó számítógépes kommunikációt betárcsázós hálózati kapcsolatnak (*dialup networking* – DUN) nevezzük. A modemek a telefonvonal TONE üzemmódját használva kommunikálnak egymással. Ez azt jelenti, hogy a modemek képesek utánozni a telefon tárcsázási képességét. A betárcsázós hálózati kapcsolat pont-pont protokollt (*point-to-point protocol* – PPP) használ. A PPP két számítógép között telefonvonalon keresztül létrejött egyedi kapcsolatot.

Hubok

A hub megnöveli egy hálózat hatótávolságát azáltal, hogy az egyik portján beérkező adatokat regenerálja és az összes többi portján továbbítja. Egy hub jelismétlőként is működhet. A jelismétlő is kiterjeszti a hálózatot, hiszen a jelek regenerálásával megoldja a nagyobb távolságok esetében jelentkező adatvesztést. A hub csatlakoztatható más hálózati eszközhöz is, például kapcsolóhoz vagy forgalomirányítóhoz, összeköttetést teremtve ezzel a hálózat szegmensei között.

A kapcsolók hatékony működésének és alacsony árának köszönhetően a hubok használata manapság egyre ritkább. A hub nem szegmentálja a hálózati forgalmat, így csökkenti a hozzá csatlakozó eszközökön elérhető sáv szélességet. Ezen túlmenően, mivel a hubok nem tesznek különbséget az egyes adatcsomagok között, a szükségtelen hálózati forgalom is folyamatosan terheli az összes hozzá csatlakozó eszközt.

A hubok jellemzői:

- fizikai rétegbeli eszköz (biteket másol a portjai között);
- csillag topológiájú Ethernet-hálózatban használják;
- a bejövő jeleket felerősítést követően az összes portján továbbítja (*broadcast*);
- több egyidejű adásnál ütközés alakul ki, amely a hálózati forgalom pillanatnyi szüneteltetését vonja maga után (CSMA/CD);
- a sávszélesség eloszlik az elosztókra csatlakozott végpontok között.

Hidak és kapcsolók

Az állományokat a hálózaton történő továbbítás előtt kisebb darabokra, úgynevezett csomagokra tördelik. Ez a folyamat lehetővé teszi a hibaellenőrzést és a könnyebb újraküldést, ha a csomag elveszik vagy megsérül. A csomagok elejére és végére a továbbítás előtt címinformációk kerülnek. Az így kapott csomagot keretnek nevezzük.

A helyi hálózatokat gyakran kisebb részekre, úgynevezett szegmensekre osztják, hasonlóan ahhoz, ahogy egy céget részlegekre vagy egy iskolát osztályokra szoktak bontani. A szegmensek határainak kijelölésére hidakat használnak. A híd szűri a LAN-szegmensek hálózati forgalmát, és minden hozzá csatlakozó szegmens összes eszközét nyilvántartja. Egy keret fogadásakor megvizsgálja a célcímet, és ez alapján eldönti, hogy a keretet továbbítja egy másik szegmensbe vagy eldobja. Mivel a híd a kereteket a megfelelő szegmensen belül tartja, így hatékonyabbá teszi az adatátvitelt.

A kapcsolót többportos hídnak is nevezzük. A hídnak jellemzően két portja van, amely a hálózat két szegmensét köti össze. A kapcsoló számos porttal rendelkezhet attól függően, hogy hány hálózati szegmenst kell összekötnie. A kapcsoló lényegesen bonyolultabb eszköz, mint a híd.

Napjaink hálózataiban hub helyett kapcsolókat használnak. A hubhoz hasonlóan a kapcsoló esetén is az eszköz sebessége határozza meg a hálózat maximális sebességét. A kapcsoló szűri és szegmentálja a hálózati forgalmat azáltal, hogy az adatokat csak annak az eszköznek küldi, akinek címezték. Így nagyobb dedikált sávszélesség jut a hálózat egyes eszközeinek.

A kapcsolók kapcsolótáblát tartanak fenn. A kapcsolótábla tartalmazza a hálózaton előforduló összes MAC-címet, és hogy egy adott MAC-című eszköz melyik porton keresztül érhető el. A kapcsolótábla létrehozásához a kapcsoló megvizsgálja

minden beérkező keret forrás MAC-címét és a kapcsoló azon portját, ahol a keret beérkezett. Ezt követően épül fel a kapcsolótábla, amely a MAC-címeket a kimenő portokhoz rendeli. Amikor a kapcsolóba egy adott cél MAC-címmel egy keret érkezik, az eszköz a kapcsolótáblája alapján dönti el, hogy merre kell a keretet továbbítani. A keretet a kimenő porton a célállomáshoz továbbítja. Mivel a keretet egyetlen konkrét porton küldi ki, így a többi port forgalmát nem terheli.

Forgalomirányítók és vezeték nélküli hozzáférési pontok

Az internetszolgáltatóval (*internet service provider* – ISP) kötött szerződés előtt mérjük fel a rendelkezésre álló eszközöket, és ennek alapján válasszuk ki a szükséges berendezéseket! A szolgáltatók egyéni és üzleti felhasználók számára biztosítanak internet-hozzáférést. Az internetkapcsolatot, e-mail-postafiókot és webes felületet általában havi szolgáltatási díjért nyújtják. Néhány internet-szolgáltatónál lehetőség van eszközök bérlésére is. Ez sok esetben lényegesen kedvezőbb, mint ezek beszerzése, hiszen a szolgáltató támogatást biztosít az eszköz meghibásodása, cseréje vagy frissítése esetén is.

Vezeték nélküli hozzáférési pontok

A vezeték nélküli hozzáférési pontok lehetővé teszik a vezeték nélküli eszközök, mint például a laptopok és a táblagépek hálózathoz csatlakozását. A vezeték nélküli hozzáférési pont rádióhullámok segítségével kommunikál a vezeték nélküli eszközök hálózati kártyájával és más vezeték nélküli hozzáférési pontokkal. A hozzáférési pontok által lefedett terület mérete korlátozott. Nagyobb hálózatok esetén a megfelelő lefedettség érdekében több hozzáférési pontra van szükség. Míg a vezeték nélküli hozzáférési pont csak a hálózathoz való csatlakozást biztosítja, addig a vezeték nélküli forgalomirányítók további lehetőségeket is nyújtanak, mint például IP-cím-hozzárendelés.

Forgalomirányítók

A forgalomirányítók hálózatokat kötnek össze. Míg a kapcsolók MAC-címek alapján továbbítják a kereteket egy hálózaton belül, addig a forgalomirányítók

IP-cím alapján irányítják a csomagokat a hálózatok között. A forgalomirányító lehet egy speciális szoftverrel telepített számítógép vagy egy hálózati eszközöket gyártó cég céleszköze.

Egy vállalati hálózat esetén a forgalomirányító egyik portja a WAN-hoz, a többi pedig a vállalat helyi hálózatához csatlakozik. A forgalomirányító ilyenkor a helyi hálózat átjárója, vagyis a kijárat a többi hálózat felé.

Többfunkciós eszközök

A többfunkciós eszközök egyszerre több feladatot látnak el. Lényegesen kényelmesebb egyetlen eszköz megvásárlásával és telepítésével megvalósítani minden feladatot, mint minden egyes funkcióhoz külön eszközt vásárolni. Ez különösen igaz otthoni felhasználók esetében. Otthoni hálózat esetén a forgalomirányító csatlakoztatja a számítógépeket és hálózati eszközöket az internethez. A forgalomirányító ilyenkor átjáróként és kapcsolóként, a vezeték nélküli forgalomirányító pedig átjáróként, vezeték nélküli hozzáférési pontként és kapcsolóként is működik. A többfunkciós eszközök modemet is tartalmazhatnak.

Hálózati adattároló (NAS)

A hálózati adattároló (*network-attached storage* – NAS) egy vagy több merevlemezzel és egy Ethernet-csatlakozással rendelkezik, valamint beágyazott operációs rendszert használ a teljes funkcionalitású hálózati operációs rendszer helyett. Az adattároló a hálózatra csatlakozva biztosítja a felhasználók számára a fájlok, video- és audio-adatfolyamok hozzáférését és megosztását, valamint az adatok biztonsági mentését egy központi helyre. A több merevlemezt is támogató NAS-eszközök RAID-alapú adatvédelemre is képesek.

A hálózati adattárolók ügyfélszolgáltató elven működnek. Egy hardvereszköz, amelyet gyakran NAS-átjárónak is neveznek, biztosítja a kapcsolatot a NAS és a hálózati ügyfelek között. Az ügyfelek nem közvetlenül a tárolóeszközökhöz, hanem mindig a NAS-átjáróhoz csatlakoznak. A hálózati adattárolók nem igényelnek monitort, billentyűzetet vagy egeret.

A NAS-rendszerek adminisztrációja egyszerű. Gyakran tartalmaznak beépített funkciókat, mint például a lemezterület-kvóták, a biztonságos hitelesítés és a hibák észlelése esetén küldött automatikus e-mail-értesítések.

Az IP-telefonok

A VoIP (*voice over IP*, IP feletti hangátvitel) során a telefonhívások adathálózatokon és az interneten keresztül történnek. A hang analóg jelei digitális információkká alakítva IP-csomagokban továbbbitódnak. A VoIP egy már meglévő IP-hálózatot is használhat a nyilvános kapcsolt telefonhálózathoz (*public switched telephone network* – PSTN) való hozzáféréshez:

Az IP-telefonok megjelenésükben a hagyományos telefonokhoz hasonlítanak, csak a szabványos RJ-11 telefoncsatlakozó helyett RJ-45 Ethernet-csatlakozót használnak. Ezek a telefonok közvetlenül a hálózatra csatlakoznak, és az IP-kommunikációhoz szükséges összes hardver- és szoftverelemet tartalmazzák.

Ha IP-telefonnal csatlakozunk a hagyományos telefonhálózatra, akkor a hívást befolyásolhatja az internet-hozzáférés. Szolgáltatáskiesés esetén például nem tudunk telefonálni.

Különböző megoldások léteznek az IP feletti hangátvitelre:

- *IP-telefon*: eszköz, amely RJ-45 Ethernet-csatlakozóval vagy vezeték nélkül kapcsolódik egy IP-hálózathoz.
- *Analóg telefon adapter (analog telephone adapter – ATA)*: eszköz, amely a hagyományos analóg eszközöket, például telefonokat, faxokat vagy üzetrögzítőket csatlakoztatja egy IP-hálózathoz.
- *IP-telefon-szoftver*: alkalmazás, amely mikrofon, hangszórók és egy hangkártya segítségével képes egy IP-telefon funkcióit megvalósítani.

Hardveres tűzfal

A hardveres tűzfalak, mint például az integrált forgalomirányítók, a hálózat adatait és eszközeit védik az illetéktelen hozzáféréstől. A hardveres tűzfal egy olyan önálló egység, amely két vagy több hálózat között helyezkedik el. Az általa védett számítógépek erőforrásait nem használja, így nincs hatással a feldolgozási teljesítményükre.

A tűzfalakat a biztonsági alkalmazások kiegészítéseként célszerű használni. A tűzfal két vagy több hálózat között helyezkedik el és ellenőrzi a közöttük zajló forgalmat, valamint segíti a jogosulatlan hozzáférés elleni védelmet. A tűzfalak különböző módszerekkel határozzák meg, hogy mely forgalmat engedélyezik vagy tiltják egy hálózati szegmens felé.

A kiberbűncselekmények nyomozása – elméleti alapok

Bevezetés

Az elmúlt évtizedek technológiai újításai, illetve az ezek nyomán megjelenő elektronikus eszközök széles körű elterjedése digitális forradalomhoz vezetett, amely – közvetve vagy közvetlenül – mindennapi életünk szerves részévé tette a digitális eszközök használatát. Ez a folyamat egy sor olyan változást eredményezett, amelyek hatással voltak az alapvető társadalmi működésre és átalakították a gazdaság, az oktatás vagy akár a kultúra szegmensét. A digitalizáció emellett azonban nem várt következményekkel is járt, mivel számos olyan társadalmi anomáliát idézett elő, amelyek képesek negatív módon befolyásolni mindennapjainkat. Ezek egyike a technológiai alapú bűnözés megjelenése, amely tendenciáját, illetve a társadalomra gyakorolt hatását tekintve évről évre egyre komolyabb kihívások elé állítja a bűnüldöző szerveket.¹⁰²

Az OECD az 1980-as évek közepén már jelezte a bűncselekmények veszélyességét.¹⁰³ A számítógépes bűncselekmények fogalmáról, csoportosításáról már az 1980-as években születtek hazánkban tanulmányok.¹⁰⁴

Válaszul a számítástechnikai bűnözés okozta egyre jelentősebb fenyegetésekre az Európa Tanács 9 (89). sz. Ajánlásában¹⁰⁵ szerepelt egy minimális lista azokról a cselekményekről, amelyeket leginkább javasolt szankcionálni, továbbá a minimumlistát kiegészítő fakultatív lajstrom.

2001-ben megszületett a Számítástechnikai Bűnözésről szóló Egyezmény (a továbbiakban: Egyezmény),¹⁰⁶ amely a nemzetközi bűnüldöző szervek együttműködése mellett komoly hatást gyakorolt a terület hazai szabályozására is. Az Egyezmény a számítógépes bűncselekményekre vonatkozóan egy sor olyan

¹⁰² Simon (2017): i. m.

¹⁰³ OECD Computer – Related Criminality: *Analysis of Legal Police*. Paris, 1986. 28.

¹⁰⁴ Polt Péter: A számítógépes bűnözés. *Belügyi Szemle*, 21. (1983), 6. 60–64; Pusztai László: A számítógépes bűncselekmények nyomozása. *Belügyi Szemle*, 26. (1988), 3. 42–48; Nagy Zoltán András: Az informatika és a büntetőjog. *Magyar Jog*, 38. (1991), 1. 21–26.

¹⁰⁵ CoE Recommendation 1989, Council of Europe Recommendation No. R (89) 9 on Computer-related Crime (Az Európa Tanács Ajánlása a számítógépes környezetben elkövetett bűncselekményekre). Strasbourg, Legal Affairs. 1990.

¹⁰⁶ A törvénybe iktatott 2001-es „Budapest Egyezmény”.

megállapítást és rendelkezést tartalmazott, amelyek kihatottak a büntető anyagi- és eljárási kódexek kodifikációjára is. Az Egyezmény szövegét felhasználva új törvényi tényállások születtek, és olyan fogalmi meghatározások kerültek be a normaszövegekbe, amelyek részben orvosolták a hiányos vagy félreérthető meghatározásokból eredő – a korábban már említett jogalkotói és emiatt jogalkalmazói – bizonytalanságot.

A kiberbűnözés és a kiberbűncselekmények

A normatív szabályozás hiányossága többek között az is, hogy sem a kiberbűnözésnek, sem pedig a kiberbűncselekménynek nincs jogszabályban rögzített normatív fogalma, amely egyértelmű biztosítéka lenne annak, hogy az alapfogalmakat a tudományos és szakmai közeg általánosan és széles körben elfogadott konszenzus alapján, egységes meghatározásra épülve használja. Ugyan az utóbbi években többféle fogalmi megközelítés is született, ezek mégsem fedik le teljeskörűen a gyakorlatban is megjelenő deliktumokat, mivel – az információs rendszerek széles körű elterjedésének köszönhetően – a büntető törvénykönyvbe újonnan beemelt tényállások mellett a Btk. más fejezeteiben szabályozott bűncselekmények esetén is lehetővé vált az online térben történő elkövetés. Mivel e téren sem normatív, sem tudományos fogalom nem áll rendelkezésünkre, ezért csak szakmai szempontok szerint lehet meghatározni a tágabb fogalmi kategóriát. A kiberbűncselekmények körébe sorolható minden olyan jogellenes cselekmény, amely – közvetve vagy közvetlenül – fenyegetést jelent az információs rendszerekre, vagy az e rendszereken keresztül (adatok és információk formájában) megjelenő társadalmi és gazdasági folyamatokra.

A fogalom tisztázásához – e meghatározás mellett – fontos lehet az Egyezményben megjelenő kategorizálás is, amely azokra a tényezőkre épül, amelyeket a jogellenes cselekmény érint, vagy amelyek nélkül a cselekmény jogellenessége egyébként nem lenne megállapítható. Ezt a megközelítést alapul véve az első fejezetben (*Az internet mint nemzetközi tér*) említett deliktumok közül ehelyütt a leggyakoribb kiberbűncselekményeket emeljük ki:

- az információs rendszer vagy adat hozzáférését, sérthetetlenségét, illetve titkosságát sértő vagy veszélyeztető cselekmények;
- azok a cselekmények, amelyek elkövetéséhez információs rendszereket használnak fel (ilyen például az online térben elkövetett csalás);

- az elektronikus adatokhoz kapcsolódó jogellenes cselekmények (ilyen például a gyermekpornográfia is, amelynél az adat birtoklása önmagában is jogellenes); valamint
- a szerzői vagy szomszédos jogok sérelmével járó cselekmények.

Mivel napjainkra a kiberbűnözés a bűnelkövetés egy olyan jól körülhatárolt formájaként jelenik meg, ahol az elkövetők arra törekednek, hogy az információs és pénzügyi rendszereket tudatosan felhasználva (vagy manipulálva) kárt okozzanak, illetve anyagi haszonra tegyenek szert, egyértelmű, hogy a kiberbiztonsággal kapcsolatos hatósági feladatok szorosan összefüggnek a bűnüldöző szervek kiberbűncselekményekkel kapcsolatos hatósági tevékenységével.¹⁰⁷

A kiberbűncselekmények felderítésének gyakorlati szempontjai

A nyomozás alaki értelemben olyan – hatósági eszközökkel végzett – széles körű és célirányos tevékenység, amely során a nyomozó hatóság korábban megtörtént események utólagos rekonstruálására törekszik. Ennek kettős célja van: egyrészt a jogellenes cselekmény körülményeinek tisztázása, másrészt az elkövető kilétének megállapítása. A történeti tényállás felderítéséhez elengedhetetlen a cselekményhez kapcsolódó, valamint a terhelt büntetőjogi felelősségét megalapozó (személyi és tárgyi) bizonyítékok felderítése, összegyűjtése, valamint eredeti állapot szerinti biztosítása. Mivel a nyomozás formailag ugyan önálló, de tartalmilag a büntetőeljárás bírósági szakaszának előkészítésére szolgál, ezért a nyomozó hatóságnak a bizonyítékok összegyűjtése és biztosítása során arra is ügyelnie kell, hogy eleget tegyen a bizonyítás törvényességével szemben támasztott követelményeknek. A felderített bizonyítékok rögzítésének törvényessége, illetve – amennyiben feldolgozásuk szükséges – az abból nyert információk megkérdőjelezhetetlensége alapvető elvárás az eljárás bármely szakaszában.

A nyomozás során felmerülő bizonyítékok vonatkozásában fontos már a legelején tisztázni, hogy azok milyen szerepet játszanak az adott eljárásban, illetve a beszerzett bizonyítékok közül melyek azok, amelyekre a tényállást fel lehet építeni.

¹⁰⁷ Gyaraki Réka: *A számítógépes bűnözés nyomozásának problémája*. Doktori disszertáció. Pécs, PTE ÁJK Doktori Iskola, 2019b.

A számítógépes bűncselekmények elkövetése során keletkező bizonyítékokat – összhangban az elkövetés jellegével – két nagy csoportba lehet sorolni. Az első csoportba tartoznak azok a számítástechnikai eszközök, amelyek – közvetve vagy közvetlenül – a bűncselekményhez kapcsolódnak (például fizikai nyomhordozóként vagy elkövetési eszközként), a másik csoportba pedig a digitális térben keletkezett vagy ott tárolt (elektronikus) adatok tartoznak. A bizonyítékok ilyen jellegű megkülönböztetése elsősorban gyakorlati szempontból fontos, mivel az eljárási cselekmények tervezése során figyelembe kell venni azt is, hogy a felderíteni kívánt tényállásnak milyen elkövetési módozatai vannak.

A különbségtétel alapját az adja, hogy a számítógépes bűncselekmények egy része kifejezetten az információs rendszerhez, illetve az abban keletkező, kezelt vagy tárolt elektronikus adathoz kapcsolódik. A Büntetőeljárásról szóló 2017. évi XC. törvény (Be.) meghatározása szerint: információs rendszer az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezés vagy az egymással kapcsolatban lévő ilyen berendezések összessége [Be. 10. § (1) bekezdés 6. pont].

Más bűncselekmények esetén az információs rendszernek (vagy adatnak) csak köztes szerepe van, vagyis a bűncselekmény más módon (például számítógép felhasználása nélkül) is megvalósítható, azaz tradicionális bűncselekmények nyomai lelhetők fel számítástechnikai rendszerekben. Az, hogy a tényállás rekonstruálása elsősorban a digitális vagy fizikai térben található (keletkező) bizonyítékok alapján lehetséges, meghatározza a nyomozás egész menetét, különösen a nyomozó hatóság adatszerző tevékenységét, illetve az eljárás keretében alkalmazott (vagyont érintő) kényszerintézkedések körét (például kutatás, lefoglalás, elektronikus adat ideiglenes hozzáférhetetlenné tétele).

Az elektronikus adat nyomozásban betöltött szerepe

Az elmúlt évek általános tendenciája, hogy az elektronikus adatok büntetőeljárásban – bizonyítási eszközként – betöltött szerepe egyre inkább felértékelődik, mivel az esetek többségében rendelkezésre állnak olyan technikai eszközök vagy elektronikus adatok, amelyek a bizonyítás során felhasználhatók. A korábbi büntetőeljárási törvény nem határozta meg az elektronikus adat fogalmát, így annak beszerzését és felhasználását – a tárgyi bizonyítási eszközre épített párhuzam alapján – jellemzően a gyakorlat alakította. A technikai eszközök széles körű elterjedésével azonban egyre nagyobb igény mutatkozott az elektronikus

adat rendszeren belüli elhelyezésére és szabályozására. Az új büntetőeljárási törvény részben orvosolta ezt a hiányosságot és beemelte a bizonyítási eszközök rendszerébe az elektronikus adatot. A kodifikáció során a jogalkotó nem hozott létre új fogalmat az elektronikus adatra vonatkozóan, hanem – az elnevezés megváltoztatásával – beemelte a normaszövegbe a számítógépes adat Egyezményben rögzített meghatározását:

„Elektronikus adat a tények, információk vagy fogalmak minden olyan formában való megjelenése, amely információs rendszer általi feldolgozásra alkalmas, ideértve azon programot is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja.” [Be. 205. § (1) bekezdés].

A fogalom normatív meghatározása szakmai szempontból jelentős előrelépést hozott, ugyanakkor az elektronikus adat bizonyításban betöltött szerepe továbbra is tisztázatlan maradt. A törvény az elektronikus adatot – főszabályként – a tárgyi bizonyítási eszközzel együtt, annak egy sajátos formájaként határozza meg [Be. 205. § (2) bekezdés], ami önmagában is ellentmondásos. A gyakorlatban az elektronikus adat kezelése nem okoz különösebb problémát, mivel a törvény, illetve annak végrehajtási rendelete, a 100/2018. (VI. 8.) Korm. rendelet (Nyer.) a nyomozás és az előkészítő eljárás egyes szabályairól számos garanciális rendelkezést tartalmaz az adat eljárás során történő kezelése kapcsán (ilyen például a szaktanácsadó igénybevétele). Ennek ellenére a normaszövegben nem sikerült feloldani azt az ellentmondást, amely a digitális és fizikai bizonyítékok (tárgyi bizonyítási eszközök) között feszül, miszerint az elektronikus adat anyagi jellemzőkkel csak a fizikai adathordozó részeként rendelkezik, birtokba vétele (különösen a lefoglalása) pedig ennek megfelelően csak korlátozottabb formában lehetséges.

A nyomozás elrendelését követően a nyomozó hatóság a – feljelentés tartalma vagy saját felderítő tevékenysége alapján – rendelkezésre álló adatokat felhasználva mérlegeli, hogy az adott eljárás szempontjából mi tekinthető bizonyítéknak, és e bizonyítékokat milyen formában és technikai eszközökkel, továbbá milyen eljárási cselekmény keretében lehet beszerezni. Vitathatatlan tény, hogy a számítógépes bűncselekmények nyomozása többnyire elképzelhetetlen a cselekményhez kapcsolódó elektronikus adatok összegyűjtése nélkül. Az elektronikus adat a tényállás rekonstruálásának elengedhetetlen eszköze, olyan digitális nyom, amely – hasonlóan a fizikai nyomokhoz – a tényállás megismerésének,

együttal a nyomozás sikerének kulcsa. A bizonyítékok begyűjtése kapcsán tehát azt is mérlegelni kell, hogy az eljárás szempontjából releváns elektronikus adat:

- milyen jellegű és terjedelmű,
- hol található és kinek a birtokában van (vagy ki tárolja),
- a hatóság általi hozzáférésnek vannak-e akadályai (például földrajzi),
- a vizsgálat csak a helyszínen lehetséges-e vagy akár utólagosan is.

A történeti tényállás tisztázása érdekében különösen az alábbi elektronikus adatok (lefoglalást követően: digitális bizonyíték) beszerzése lehet indokolt:

- számítástechnikai és telekommunikációs eszközök adattartalma,
- adathordozók (például optikai lemezek, merevlemezek, memóriakártyák) adattartalma,
- felhőalapú szolgáltatásban tárolt adatok,
- kriptovaluták,
- elektronikus levelezés, illetve egyéb kommunikációs adatok (például alkalmazáson belüli beszélgetések),
- kép- és videófájlok, hangfelvételek,
- alkalmazáson belüli felhasználói és regisztrációs adatok,
- elektronikusan tárolt pénzügyi vagy előfizetői adatok,
- mobilkommunikációs adatok,
- ATM-ek, biztonsági kamerák és térfigyelő kamerák felvételei,
- metaadatok.

Az elektronikus adatok jellegét és bizonyításban betöltött szerepét (szükségesség), valamint a fenti körülményeket figyelembe véve meghatározhatjuk azt a tényleges intézkedést, amely úgy biztosítja az adatok beszerzését, hogy nem okoz a szükségesnél nagyobb érdeksérelmet (arányosság). Az adatok beszerzésére ennek megfelelően sor kerülhet: önálló rögzítéssel, adatkérés útján, valamint kényszerintézkedés keretében.

Önálló adatrögzítés

Az elektronikus adatok nyomozó hatóság általi önálló rögzítése abban az esetben lehet indokolt, ha:

- a) a beszerezni kívánt elektronikus adatok nyilvánosak, vagyis a folyamat bárki számára nyíltan elérhető adattartalom (például weblap felépítése) pillanatnyi állapotának rögzítését jelenti, vagy
- b) a nyomozó hatóság az eljárás sértettjének birtokában (vagy kezelésében) lévő adattartalmat rögzít, feltéve, hogy ehhez az érintett kifejezetten hozzájárul (kényszer alkalmazása nem indokolt), és a rögzítés nem jár az elektronikus adatok sérelmével.

Mivel a Be. 51. § (1) bekezdés *b)* pontja alapján a sértett jogosult az eljárás során bizonyítékot előterjeszteni, illetve a sikeres felderítésben egyébként is érdekelt, ezért az így beszerzett bizonyíték megfelelő bizonyító erővel rendelkezik.

Az elektronikus adatok önálló rögzítéséről célszerű minden esetben feljegyzést készíteni, amelyben fel kell tüntetni a rögzítés helyét, idejét, módját, a rögzítést végző személyt (vagy személyeket), illetve azt, hogy a folyamat milyen típusú és terjedelmű adatállományt érintett.

Adatkérés

A büntetőeljárási törvény alapján a nyomozó hatóság bármely szervtől, jogi személytől vagy jogi személyiséggel nem rendelkező szervezettől adatszolgáltatást kérhet. [Be. 261. § (1) bekezdés.] Az adatkérés (ideértve a feltételes adatkérést is) vonatkozhat olyan elektronikus adat szolgáltatására is, amely a cselekménnyel összefüggésbe hozható, és az adatkezelő (vagy az adatok birtokosa) más közigazgatási szerv vagy olyan szervezet (például gazdasági társaság), amely az eljárásban nem érdekelt.

Ha a cselekmény jellege vagy a feltárt személyes körülmények (például a feltételezett elkövető az adatkéréssel érintett szerv munkavállalója) indokolják, célszerű az elektronikus adatokat lefoglalás útján beszerezni, mivel a hatóság által dokumentált kényszerintézkedés az adatok változatatlanságát erősíti.

Amennyiben az adatok teljes körű és eredeti állapot szerinti beszerzése így is lehetséges, akkor – az arányosság elvét figyelembe véve – nem indokolt kényszerintézkedés alkalmazása. Célszerű továbbá adatkérést alkalmazni a külföldön bejegyzett és magyarországi érdekeltséggel (vagy fiókteleppel) nem rendelkező szolgáltatók esetén is, mivel ezekre nem terjed ki a magyar joghatóság (például tárhelyszolgáltatók).

A külföldön bejegyzett cégek és egyéb jogi személyek nem kötelesek a magyar büntetőeljárási szabályok alapján kibocsátott adatkérést teljesíteni, ezért az adatszolgáltatás megtagadása esetén a 24/7-es kapcsolati pontokon keresztül vagy nemzetközi bűnügyi jogsegély alapján lehet az adatok rögzítését biztosítani.

Lefoglalás

A bizonyítékok felderítése és beszerzése alapvetően illeszkedik abba a folyamatba, amely során a nyomozó hatóság megpróbál egyfajta valósághű tényállást rekonstruálni. Abban az esetben, ha az elektronikus adatok (vagy más bizonyítékok) beszerzése egyéb módon nem lehetséges, vagy a körülmények alapján kényszer alkalmazása válhat szükségessé, a hatóság lefoglalás útján biztosítja a bizonyítékok megőrzését. A lefoglalás jellemzően más eljárási (kényszer) cselekményhez (kutatás, motozás) kapcsolódik, kivételesen viszont – ha a bizonyítékok felhasználhatóságát és eredetiségét ez nem veszélyezteti – önállóan is sor kerülhet rá.

A nyomozás sikere érdekében a hatóságnak mérlegelnie kell, hogy az adott eljárás szempontjából mi tekinthető bizonyítéknak, és e bizonyítékokat milyen formában és technikai eszközökkel, illetve milyen eljárási cselekmény keretében lehet beszerezni.

A felsorolt lehetőségek közül a lefoglalás végrehajtása a legösszetettebb, mivel ebben az esetben az adatok beszerzésének nemcsak időbeli, hanem – a kényszerintézkedés jellegénél fogva – személyi akadályai is lehetnek. Mivel a lefoglalás esetén a kényszerintézkedéssel érintett személy jellemzően nem érdekelt a nyomozás sikerében (nem áll érdekében az, hogy a hatóság bizonyítékokat szerezzen be), ezért a végrehajtást lehetőség szerint alaposan elő kell készíteni.

A kutatás, motozás és lefoglalás szerepe a nyomozásban

A kutatás szabályai – kisebb változtatásokkal – azonosak a korábbi eljárási törvényben szereplő házkutatás szabályaival, vagyis az eljárási cselekmény célja – a büntetőeljárás eredményes lefolytatása érdekében – a lakás, az egyéb helyiség, a bekerített hely vagy a jármű átkutatása. A Be. ide vonatkozó rendelkezése alapján a kutatás elrendelésére akkor kerülhet sor, ha megalapozottan feltehető, hogy az:

- bűncselekmény elkövetőjének elfogására,
- bűncselekmény nyomainak felderítésére,
- bizonyítási eszköz megtalálására,
- elkobozható, illetve vagyonelkobzás alá eső dolog megtalálására vagy
- információs rendszer, illetve adathordozó átvizsgálására vezet. [Be. 302. § (2) bekezdés]

Mivel a törvény nem határozza meg egyértelműen, hogy a kutatás elrendelése mikor tekinthető megalapozottnak, ezt a gyakorlatban a rendelkezésre álló adatok alapján kell eldönteni. A korábbi szabályozáshoz képest fontos előrelépést jelent, hogy a törvény az információs rendszer, illetve adathordozó átvizsgálása esetén is lehetővé teszi a kutatás elrendelését. Ugyanez a bizonyítás szempontjából inkább folyamatnak, mintsem eredménynek tekinthető, a nyomozás hatékonysága szempontjából mégis fontos, mivel a digitális bizonyítékok megtalálását eredményezheti.

A kutatáshoz hasonlóan a motozás is bizonyítási eszköz, valamint elkobozható vagy vagyonelkobzás alá eső dolog felkutatására irányul, ez azonban nem ingatlan vagy jármű, hanem meghatározott személy (jellemzően terhelt) átkutatását jelenti. Ez magában foglalja a motozás alá vont személy ruházatának és testének átvizsgálását, amely során az adott személynél található dolog is átvizsgálható. Ugyan az utóbbi rendelkezés nem egyértelmű, bizonyos körülmények között (például tettenérés esetén) ez akár a felderítés során is megalapozhatja a motozás szükségességét, ha a motozás alá vont személynél olyan dolog található, amelynek bizonyítási eszközként való értékelése valószínűsíthető (például mobiltelefon, pendrive stb.).

A kutatás és a motozás elrendelése határozattal történik, amelyet a nyomozó hatóság is kibocsáthat, fontos azonban kiemelni, hogy ha a közjegyzői vagy ügyvédi irodában tartandó kutatás közjegyzői vagy ügyvédi tevékenységgel összefüggő védett adat megismerésére irányul, a kutatást csak bíróság rendelheti el. A kutatást és a motozást a törvény azonos fejezetben szabályozza, aminek oka az, hogy e kényszercselekmények elrendelése kapcsán a nyomozó hatóság diszkrecionális jogkörrel rendelkezik, másrészt nem feltétlenül jár együtt egyik sem a tulajdonjog korlátozásával. A kutatás és a motozás gyakorlati szempontból tehát – amennyiben az eljárás célja nem a vagyonelkobzás alá eső vagyron biztosítása – annak megállapítására irányul, hogy van-e a terhelt vagy más személy birtokában bizonyítási eszköz vagy elkobozható dolog.

A lefoglalás jelentheti meghatározott dolog, információs rendszer, az ilyen rendszerben tárolt adatokat tartalmazó adathordozó vagy elektronikus adat lefoglalását is, amely – a lefoglalt dolog jellegétől és a lefoglalás módjától függően – a lefoglalás tárgya feletti birtok- vagy tulajdonjogot korlátozza. A lefoglalást lehetőség szerint a lefoglalt dolog birtokba vételével kell végrehajtani, kivételesen viszont az érintett őrizetében hagyásával is végrehajtható. Elektronikus adatok esetén ez abban az esetben lehet indokolt, ha a lefoglalás aránytalan adminisztratív terhet jelentene (például az adattartalom mérete miatt), az érintettnek az elektronikus adatok használatához fűződő érdeke miatt, vagy más fontos okból, ha az adatok megváltoztatásának veszélye egyébként nem áll fenn.

A lefoglalás elrendelése határozattal történik, amelyet a nyomozó hatóság az eljárási cselekmény megkezdése előtt bocsát ki, kivételes esetben – halaszthatatlan eljárási cselekmény esetén – a határozat meghozatala utólag történik. A lefoglalható dolgok körét a Be. kategorikusan meghatározza, ezek az alábbiak [Be. 315. § (2) bekezdése alapján]:

- ingó dolog,
- számlapénz,
- elektronikus pénz [Hpt 1. § 16. pont] (ideértve például az egyéni Transferwise- vagy Revolut-számlákon kezelt pénzt is),
- elektronikus adat.

A lefoglalás – a végrehajtás módját tekintve – megvalósulhat:

- birtokba vétellel,
- a megőrzés más módon történő biztosításával,
- az érintett őrizetében hagyással vagy
- az elektronikus adat esetében pedig
- az elektronikus adatról történő másolat készítésével,
- az elektronikus adat áthelyezésével,
- az elektronikus adatot tartalmazó információs rendszer vagy adathordozó teljes tartalmáról történő másolat készítésével,
- az elektronikus adatot tartalmazó információs rendszer vagy adathordozó lefoglalásával, vagy
- jogszabályban meghatározott más módon (például kriptovaluták esetén számláról történő átvezetéssel).

A fenti felsorolás nemcsak azokat a konkrét lehetőségeket jelöli, amelyek az elektronikus adat lefoglalása kapcsán rendelkezésre állnak, hanem – az arányosság

követelményét alapul véve – egyfajta sorrendiséget is kifejez. Az eljárási cselekmény során figyelembe kell venni az arányosság követelményét, amely ebben az esetben kettős követelményként jelenik meg. A lefoglalást lehetőleg azokra az elektronikus adatokra kell végrehajtani, amelyek a bizonyítás szempontjából szükségesek, továbbá a kényszerintézkedés információs rendszerre vagy adat-hordozóra csak akkor terjedhet ki, ha:

- az elkobozható, illetve vagyone elkobzás 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.

A lefoglalás külön rendelkezései között jelenik meg a fizetésre használt elektronikus adat, illetve az elektronikus adatként létező irat lefoglalása.

Az elektronikus adatként létező irat lefoglalása az irat lefoglalására vonatkozó szabályok szerint lehetséges.

Ezek közül a fizetésre használt elektronikus adat lefoglalását érdemes kiemelni, amelyet olyan művelettel (átváltás, átvezetés, átutalás) is végre lehet hajtani, amely az érintettnek az elektronikus adat által kifejezett vagyoni érték feletti rendelkezési lehetőségét akadályozza meg.

A kutatás és lefoglalás előkészítése

Ahogy arról már korábban is szó volt, a nyomozás eljárási cselekmények célirányos, tervszerűen végrehajtott láncolata. A tervszerűség végigkíséri a nyomozás egészét, általános értelemben ez biztosítja az eljárás folytonosságát, de megjelenik egyes eljárási cselekmények végrehajtása kapcsán is. Minél szofisztikáltabb egy bűncselekmény, annál nagyobb kihívást jelent a tényállás utólagos rekonstruálása, ami szükségessé teszi a tudatos tervezést, különösen a kihallgatásokat és a kényszerintézkedéseket megelőzően. Mivel a kibercselekmények felderítésének sikerét szinte valamennyi esetben a cselekményhez kapcsolódó elektronikus adatok és tárgyi bizonyítási eszközök beszerzése jelenti, ezért a kutatás előkészítése minden eljárásban indokolt. Ennek azért van jelentősége, mivel a megfelelően előkészített és tervszerűen végrehajtott eljárási kutatás – a bizonyítási eszközök beszerzését megkönnyítve – nagyban hozzájárul az eljárás sikeréhez. A végrehajtási tervet vagy kutatási tervet úgy kell elkészíteni, hogy a kutatás és a lefoglalás megfeleljen a legfontosabb eljárási szempontoknak:

- észszerű időn belül befejezhető legyen;
- lehetőleg ne kelljen megszakítani (kivételes esetben rövid ideig);
- ne kelljen megismételni;
- az eljárási cselekményen jelen lévők megfelelő módon követhessék az eljárási cselekmény végrehajtását, eljárási jogaikat gyakorolhassák;
- biztosítva legyen az eljárási cselekmény és a jelen lévő személyek külső befolyástól való mentessége.

A törvényességi garanciák mellett a végrehajtási tervnek tartalmaznia kell mindazokat az információkat, amelyek a nyomozás alapján rendelkezésre állnak, így különösen:

- az eljárási cselekmény helyét, idejét, tervezett ütemezését és célját;
- a részt vevő hatósági személyek számát, nevét és feladatát;
- a vizsgált cselekmény minősítését (törvényi tényállás);
- a rendelkezésre álló adatok alapján rekonstruált történeti tényállást;
- azokat az információkat, amelyek az eljárási cselekmény szükségességét megalapozzák (például korábban beszerzett bizonyítékok);
- a cselekmény végrehajtása során jelen lévők (kényszerintézkedéssel érintett személyek) személyes és bünygyi nyilvántartási adatai;
- a feltételezett elkövetőről készített adatgyűjtés eredményét (személyes adatok, bünygyi nyilvántartási adatok, löfgyver-nyilvántartás adatai, képzettség/végzettség, foglalkozás, családi és baráti kapcsolatok stb.);
- a keresett bizonyítási eszközök körét (általános vagy meghatározott jelleggel);
- a lefoglalás módját, eszközeit;
- a tervezett további eljárási cselekményeket vagy kényszerintézkedéseket (például előállítás, kihallgatás, őrizetbe vétel).

A kutatási tervben érdemes külön kitérni arra, hogy a kutatás helyszínén lehet-e bizonyítási eszközökre számítani, és ha igen, azok elsődlegesen tárgyi bizonyítási eszközök, elektronikus adatok, vagy mindezek együttesen. A vizsgált bűncselekmény jellege mellett az elkövetés módszere is fontos támpontja a kényszerintézkedésnek, különösen, ha van olyan azonosított technikai eszköz (például számítógép), amely az elkövetésben szerepet játszott. Az elkövetés jellege (elkövetési tárgy) alapján a tárgyi bizonyítási eszközök és az elektronikus adatok bizonyítékként betöltött szerepe az alábbiak szerint csoportosítható:

- Amennyiben az elkövetés tárgya a számítógép vagy annak valamilyen alkatrésze vagy tartozéka (például lopás vagy rongálás esetén), az elektronikus adatok bizonyítási szerepe legfeljebb esetleges (dogmatikai értelemben az ilyen cselekmények nem tekinthetők számítógépes bűncselekményeknek), a bizonyítás szempontjából a tárgyi bizonyítási eszközök szerepe lesz elsődleges.
- Ha az elkövetés tárgya az információs rendszer, illetve az abban tárolt adat vagy program, klasszikus számítógépes bűncselekményről beszélhetünk, vagyis kiemelt szerepet kapnak az elektronikus adatok a bizonyításban. Figyelembe véve azt, hogy a Btk. 423. § (5) bekezdésében foglaltak alapján adatnak minősül az a program is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja.
- Amennyiben a technikai eszköz (például számítógép, mobiltelefon) vagy maga az információs rendszer (online felület) olyan bűncselekmény elkövetését teszi lehetővé, amely enélkül is megvalósítható (például csalás, gyermekpornográfia), az elkövetéssel összefüggésben keletkező (vagy ahhoz felhasznált) adatok mellett a technikai eszközök is bizonyító erővel bírnak.

A digitális bizonyítékok felkutatása a fizikai térben kezdődik, vagyis a hatóság először azt vizsgálja, hogy milyen tárgyi bizonyítási eszközök találhatók a helyszínen. A kutatás során leggyakrabban az alábbi eszközökkel találkozhatunk:

Számítógép: az elektronikus adatok szempontjából a legáltalánosabb és legelterjedtebb technikai eszköz, amely – az asztali számítógéptől a laptopig – egy sor olyan adatot és információt tartalmazhat, amely a felhasználóra, a felhasználó digitális szokásaira és online tevékenységére, valamint a számítógéppel végrehajtott konkrét cselekményre vonatkozik (idesorolható a felhasználói tevékenységet rögzítő periféria is, mint például nyomtató). A számítógéphez kapcsolódó perifériák lefoglalása és vizsgálata alapvetően csak akkor indokolt, ha azok olyan fizikai nyomot hordoznak (például elkövető ujjnyomata), amely a bizonyítás szempontjából nélkülözhetetlen.

Mobiltelefon: a mobiltelefon olyan telekommunikációs eszköz, amely jellemzően egyetlen személy használatában van, és – általános szerepe mellett – rendelkezik mindazokkal a funkciókkal, amelyekkel a számítógép is, vagyis olyan személyes adatokat tartalmazhat, amelyeknek a bizonyítás során – különösen az elkövető kilétének megállapításában vagy tevékenységének felderítésében – kiemelt szerepük van.

Tartós adathordozó: a tartós adathordozók köre – összhangban az Európai Unió 2011/83/EU irányelvével – a háttértárak mellett (például CD-k, DVD-k, pendrive, memóriakártyák, merevlemezek stb.) kiterjed a papírra és az elektronikus levelekre is, amelyek – vizuális vagy digitális formában – az adattárolás és a kommunikáció alapvető eszközei.

A fizikai környezet átvizsgálását követően – amennyiben a helyszín jellege és a körülmények ezt lehetővé teszik – meg kell vizsgálni, hogy vannak-e a helyszínen olyan tárgyi bizonyítási eszközök, amelyek tartalma az ügy szempontjából releváns lehet. A fizikai térben található bizonyítékokkal ellentétben az elektronikus adatokat nem elegendő megtalálni, azt is fel kell tární, hogy azok milyen forrásból származnak, vagy milyen bizonyítékláncolatba illeszkednek. A nyombiztosításhoz hasonlóan az elektronikus adatok kapcsán is fontos szerepe van a folyamatos dokumentálás mellett (fénykép, videó- vagy hangfelvétel) az adatok megfelelő rögzítésének. Ennek célszerű olyan formáját (adatok mentése/másolása, adathordozó vagy technikai eszköz lefoglalása) választani, amely biztosítja az adatok hiteles, eredeti és módosításoktól mentes rögzítését, továbbá azt, hogy azok az eljárás későbbi szakaszában is (például a szakértő vagy szaktanácsadó által) feldolgozhatók maradjanak.

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 büntető-eljárásban 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 krimináltaktikai 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 egybeesnek – 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

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 formái 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 eljárást 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 foglалható le, ha az elkobozható, illetve vagyoneklobzás 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 vagyoneklobzás 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 szereztek (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 változatlanosságát – 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 bite 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 adatösszeség. 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 végezhesen a felhasználó. A felcsatolás folyamata 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 büntető-eljárás 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 adatösszeség 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 meghaladóan 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 szakismertekkel, 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 legtöbbszor 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 szerveret 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 megjegyezni arról, hogy az eszköz valóban kikapcsolt állapotban van, vagy csak úgy tűnik. A gyártók körében energiatakarékosági 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 üzemkészs, 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 végezhetőek.

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, csatlakozási 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 kijelentkezeti 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 kiemelő 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 úgy 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.

Vákát

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 keregett 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 érdeksérellemmel 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.

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 kevésbé 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 nyomomonkövethető). 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 merevlemez. 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 videokártya, 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 törvényt szöveg 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 kiszerezni 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: egyrésztől annak igazolásából, hogy a dolog már a lefoglaláskor is azokkal a tulajdonságokkal rendelkezett, amelyekkel bármikor később az eljárás során; másrésztől 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 $25 \times 40 \times 60$ 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 $25 \times 40 \times 60$ 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. Ugyan-ezen 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 merevlemez 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 felválni 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 merevlemezben 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 tehetette 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 visszakérül 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 helyezjük 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 megóvjá, a csomagot pedig úgy kell lezárni, hogy az a csomagolóanyag vagy a zár sérülése nélkül ne legyen felnyitható. A csomagolás burkolatán (illetőleg bűnjelcímken) 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 követhető 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 természetesen 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. Egyrészt az azért fontos ez, hogy jobban megérthető legyen, melyek azok a hátrányok, amelyek az új szemléletmóddal kiküszöbölhetők, másrészt 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 következtelenségekhez, 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, kézzel fogható 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 szükségtelemmé nem válik. Az adat tárolása pedig gyakorlatilag csak egy esetben válhat szükségtelemmé: 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 tartsa magában 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 semmisítendőek 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 fálnak 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 merevlemez 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 bűnjelként 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 változatlanlanságát, 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 adatsomag 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 változatlanlanságát vagy a változtatás nyomonkövethetőségét. Az adatok változatlanlanságának 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 karaktersorra redukáljuk, amely így már könnyedén rögzíthető a jegyzőkönyvön.

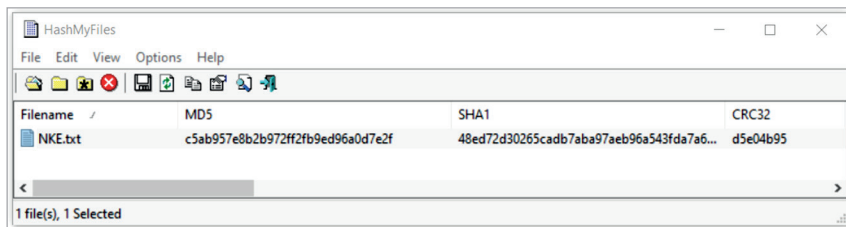
A karaktersor hosszúsága előre meghatározott, az nem függ az adatok jellegétől vagy méretétől; a függvény minden esetben addig „dolgozik”, míg a megfelelő mértékig le nem egyszerűsíti az eredeti adattartalmat. Az így kapott karaktersor – a hashkulcs – természetesen nem fejthető vissza, a folyamat csak 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 fájlnev is csupán metaadat, és nem tekinthető a fájl adattartalmának.

Több fájl lefoglalása esetén (tekintve, hogy az egyszerűsége 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 változatlanágát. 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 egyrésről nem egyértelmű a lefoglalás módja, másrésről 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 adatsomag 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:

<u>Bűnjeljegyzék</u>				
A Büntető Törvénykönyvről szóló 2012. évi C. törvény 339. § (1) bekezdésébe ütköző és <u>aszerint</u> minősülő garázdaság vétségének gyanúja miatt ismeretlen tettes ellen indított bűnügyben lefoglalt tárgyról.				
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 fényképfelvétel tartalmazó adatállomány (MD5 HASH: Ea891660c76f2a7178b2d191f9f082b4)	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 hordozóját (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 chat-beszélgetés);
- 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 tartalmazzak 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 kelletnél 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 változatlanlenségét 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 szerveket. 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

Az igazságügyi informatikai szakértő feladatai

Bevezetés

Az igazságügyi informatikai szakértő feladata a tudomány és a műszaki fejlődés eredményeinek felhasználásával az adott ügyben felmerülő szakkérdés eldöntése (2016. évi XXIX. törvény az igazságügyi szakértőkről [Szaktv.] 3. §), amely az igazságügyi szakértői nyilvántartásban bejegyzett szakterületei [9/2006. (II.27.) IM rendelet] valamelyikébe esik:

- informatikai berendezések, számítógépek, perifériák és helyi hálózatok (hardver),
- informatikai biztonság,
- informatikai rendszerek tervezése, szervezése,
- stúdiótechnika, multimédia területtel összefüggő informatikai tevékenység,
- számítástechnikai adatbázis, adatstruktúrák,
- szoftverek.

A szakértő a feladatot kirendelés alapján [Be. 189. § (1)] végzi. A szakértői vizsgálat tartalma szempontjából a kirendelő határozat központi eleme a szakértőhöz intézett kérdések vagy feladatok meghatározása, illetve a kirendelés indokolása. A kérdések és feladatok esetén a kirendelő az ügy szempontjából értékes adattípusok, információk vagy körülmények kinyerésére, azonosítására vonatkozóan rendelkezik, míg a kirendelés indokolásánál valamennyi lényeges körülményt megadja a szakértő részére, amely a vizsgálat elvégzéséhez szükséges. A kérdések és feladatok, valamint az indokolásban szerepeltetendő körülmények részleteit az egyes vizsgálat típusoknál tárgyaljuk részletesen.

A szakértő a kirendelő határozat alapján elkészített igazságügyi informatikai szakértői véleményben foglalja össze a vizsgált informatikai szakkérdésre vonatkozó megállapításait. Amennyiben a kirendelő eldöntendő kérdéseket tett fel, úgy az ezekre vonatkozó válasz a szakértői vélemény szövegében található, abban az esetben, ha valamely körülményre, állapotra vonatkozó kérdések szerepeltek a kirendelésben, úgy az ezekre vonatkozó adatok jellemzően a szakértői vélemény elektronikus/digitális mellékletén található. Az eldöntendő kérdésre adott válaszok közvetlenül felhasználhatók, míg a körülményre, állapotra vonatkozó további elemzést és értékelést tehetnek szükségessé, különösen nagy mennyiségű forrásadat esetén.

Az igazságügyi informatikai szakértő munkája a szakértői vélemény átadásakor részben lezárul, abban az esetben, ha a szakértői vélemény tartalma valamilyen körülmény [Be. 197. § (1)] miatt nem értelmezhető, úgy a szakértői vélemény kiegészítése kérhető.

A fenti tevékenység elvégzése az igazságügyi informatikai szakértő részéről több elkülönült tevékenységből áll, amelyek informatikai szakmai részleteiről és a büntetőeljárással összefüggő kapcsolatairól a következő alfejezetekben esik szó. A további szövegben a magyar nyelvű terminológia mellett – az angol nyelvű szakirodalom későbbi könnyebb használata érdekében – megadjuk az angol szakkifejezéseket is.

Az elektronikus adatok forrásai

Az elektronikus adatok önmagukban nem állnak rendelkezésre, azokat valamilyen információs rendszer tartalmazza (tárolórendszer hordozza). Az információs rendszerek technológiai nézőpontból tekinthetők tisztán hardver- vagy tisztán szoftverrendszernek. A gyakorlatban általában a két komponenst különböző mértékben tartalmazó komplex rendszerekkel találkozhatunk, amelyek közül a leggyakoribbak az alábbiak.¹⁰⁸

Számítógépek, különösen:

- kiszolgáló számítógép (*server*),
- asztali számítógép (*desktop computer*),
- hordozható számítógép (*laptop, notebook computer*),
- táblaszámítógép (*tablet*).

Tárolóeszközök, különösen:

- memóriakártyák,
- USB-kulcsok,
- külső csatlakoztatású tárák (*external HDD, SSD*),
- hálózatra csatolt tárák (*network attached storage*).

¹⁰⁸ Ashley Brinson – Abigail Robinson – Marcus Rogers: *A cyber forensics ontology: Creating a new approach to studying cyber forensics*. *Digital Investigation*, (2006), 3. 37–43.

Kis mérettartományú digitális eszközök, különösen:

- mobiltelefonok (*featurephone*),
- okostelefonok (*smartphone*),
- egyéb kommunikációs és kiegészítő eszközök (SIM-, memóriakártya).

Nagy mérettartományú digitális közrendszer, különösen:

- számítógépfűrt (*computer cluster*),
- számítási rácsok (*computer grid*),
- felhőszolgáltatások (*cloudcomputing*)
- infrastruktúra-szolgáltatás (IaaS),
 - platformszolgáltatás (PaaS),
 - szoftverszolgáltatás (SaaS).

Egyéb eszközök, különösen:

- játékgépek (PlayStation, Xbox stb.),
- tartalomrögzítők (DVR),
- mágnesszalagos archiválórendszerek.

Az elektronikus adatokból megismerhető információk típusai

Az egyes adathordozókról kinyert elektronikus adatok információtartalma esetről esetre változó, azonban az egyes adathordozó-típusokon megtalálható információk fajtái az adott eszköz használati módjainak ismerete és tapasztalati adatok alapján előre jelezhetők. A szakértői vizsgálat alá vont adathordozók legnagyobb mennyiségét kitevő mobilkommunikációs eszközök és a tárolók (együttesen a vizsgált eszközök több mint 80%-át teszik ki) vonatkozásában a jellemző információ típusok az alábbiak.¹⁰⁹

Univerzális integrált áramköri kártya:

- nemzetközi mobilelőfizető-azonosító – (*international mobile subscriber identity* – IMSI) – maximálisan 15 számjegyből áll
 - országcód (*mobile country code* – MCC), 3 számjegy
 - hálózatkód (*mobile network code* – MNC), 2 vagy 3 számjegy
 - előfizető azonosító (*mobile subscriber identification number* – MSIN)
- gyorstárcsázás hívószámai (*abbreviated dialing numbers* – ADN),

¹⁰⁹ Ehogan Casey: *Digital evidence and computer crime*. Amsterdam, Elsevier, 2011. 37.

- legutóbb tárcsázott hívószámok (*last numbers dialed* – LND),
- egyszerű szöveges üzenetek (*short message service* – SMS),
- egyszerű multimédia-üzenetek (*enhanced messaging service* – EMS),
- bejövő hívások adatai (*EF incoming call information* – EF ICI),
- kimenő hívások adatai (*EF outcoming call information* – EF OCI).

Funkcionális mobiltelefon (*featurephone*):

- telefonkönyv-bejegyzések,
- híváslisták,
- naptárbejegyzések,
- jegyzetek,
- digitális fényképek,
- digitális hangfelvételek,
- digitális videófelvevételek,
- egyéb készülékspecifikus adatok.

Okostelefon (*smartphone*):

- telefonkönyv-bejegyzések,
- híváslisták,
- naptárbejegyzések,
- jegyzetek,
- digitális fényképek,
- digitális hangfelvételek,
- digitális videófelvevételek,
- internethasználattal kapcsolatos adatok,
 - böngészési előzmények,
 - elektronikus levelezés,
 - azonnali üzenetküldő programok használatával kapcsolatos adatok,
 - letöltött fájlok és dokumentumok,
- GPS-adatok,
- vásárlási adatok,
- pénzügyi adatok,
- egyéb készülék- és/vagy szolgáltatásspecifikus adatok,
- telepített alkalmazások által tárolt egyedi formátumú adatok.

Táblagépek:

- okostelefonokkal azonos adatkörök,
- számítógép-specifikus adatok.

Memóriakártya:

- funkcionális mobiltelefonokkal azonos adatkörök,
- okostelefonokkal azonos adatkörök,
- számítógép-specifikus adatok.

Merevlemezis adattárolók:

- beépített adattárolók,
 - felhasználói adatok, különösen
 - internethasználat adatai,
 - kommunikációs adatok (levelezés, azonnali üzenetküldés stb.),
 - mobiltelefonok biztonsági mentései,
 - működtető rendszer adatai, különösen
 - telepítés ideje,
 - felhasználók adatai,
 - telepített alkalmazások adatai,
 - fájlrendszer adatai,
 - a rendszer hardver- és szoftverkomponenseinek adatai,
 - a rendszer használati eseményeinek adatai,
- külső csatlakozású adattárolók, különösen
 - archivált adatok (dokumentumok, digitális képek, videók, hangfelvételek),
 - mobiltelefonok biztonsági mentései,
- nagy tárolókapacitású hálózati adattárolók (SAN, NAS), különösen
 - archivált adatok (dokumentumok, digitális képek, videók, hangfelvételek),
 - napi használat adatai (dokumentumok, elektronikus levelezés, digitális képek, videók, hangfelvételek).

Szilárdtest adattárolók:

- felhasználói adatok, különösen
 - internethasználat adatai,
 - kommunikációs adatok (levelezés, azonnali üzenetküldés stb.),
- működtető rendszer adatai, különösen
 - telepítés ideje,

- felhasználók adatai,
- telepített alkalmazások adatai,
- fájlrendszer adatai,
- a rendszer hardver- és szoftverkomponenseinek adatai,
- a rendszer használati eseményeinek adatai.

Memóriakártyák, USB-kulcsok:

- mobiltelefonok működési adatai,
- mobiltelefonok biztonsági mentései,
- felhasználói adatok (különösen digitális fényképek, videók, hangfelvételek, dokumentumok).

Optikai adathordozók:

- telepítőkészletek,
- archivált felhasználói adatok (különösen digitális fényképek, videók, hangfelvételek, dokumentumok).

A kibernetikai és szakértői munka kapcsolata

A tématerülettel foglalkozó szakirodalom és nemzetközi szabványok: az alcím-ben írt kapcsolatot két fő nézőpontból tárgyalják, egyrészt a munkafolyamatok osztályozása, másrészt a tevékenységek meghatározása révén.

A fő munkafolyamatok azok, amelyekben a kibernetikai és a szakértői önállóan vagy együtt vesz részt, de mindenképpen egymás munkáját befolyásolva. A munkafolyamatok tipikusan sorfolytonosan követik egymást, míg a folyamaton belüli tevékenységek egymással egy időben is végezhetők.

Készenlét

A készenlét (*readiness*) elsősorban azokat a szervezeten (a nyomozó hatóság és a szakértői intézmény) belüli tevékenységeket foglalja össze, amelyek a következő szakaszokban beszerzendő bizonyítási eszközök – különösen az elektronikus adatok (*potential digital evidence*, *digital evidence*) – felhasználhatóságával, a költséghatékony és folyamatos működéssel, valamint az információbiztonsággal kapcsolatosak.

Ezek közül kiemelendő a kibernetizáció és szakértők rendszeres képzése és továbbképzése, a korábbi esetek feldolgozása és tipizálása, az egységes módszertanok, eszközkészletek használatának bevezetése és az egyes tevékenységi csoportokat végző egységek közötti eszköz- és információforgalmi kapcsolatok kialakítása és fenntartása. Ennek érdekében két alaptévékenységet kell végrehajtani, a tervezést és a felkészülést.

Tervezés

A tervezés (*plan*) fázisában kerül sor a vizsgálati folyamat során alkalmazandó módszerek és eljárások kidolgozására és meghatározására az alábbi területeken:

- elektronikus adatok lehetséges tárolóeszközeinek azonosítása,
- összegyűjtése,
- megóvása a külső behatásoktól,
- elektronikus adat kinyerése, megszerzése (amennyiben szükséges),
- elektronikus adatok lehetséges tárolóeszközeinek szállítása,
- tárolása.

Ekkor kell megtervezni a részt vevő személyek felkészültségi szintjének mérését és az ismeretek, készségek szinten tartásának lejárásait is.

Felkészülés

A felkészülés (*prepare*) során be kell gyakorolni a felhasználandó eszközök – különösen a hardver- és szoftverkomponensek – készségszintű használatát oly módon, hogy azok alkalmazása a kijelölt módszerekkel és eljárásokkal együttesen történjen.

- A potenciálisan elektronikus adatot vagy ahhoz kapcsolódó kiegészítő információkat tartalmazó digitális eszközök és analóg információhordozók felismerésének, összegyűjtésének, megóvásának, szállításának és tárolásának begyakorlása, különös tekintettel a rejtett funkcionalitású eszközökre és a kiemelt darabszámban előforduló (mobilkommunikációs és tároló-) eszközökre vonatkozóan.
- Alapvető és eszköz- (hardver- és szoftver-) specifikus ismeretek begyakorlása és számonkérése.

Folyamatindítás

A vizsgálandó esemény bekövetkezése, pontosabban annak észlelése megnyitja (*initialization*) a vizsgálati eljárás aktív szakaszát.

Észlelés

Az észleléskor (*incident detection*) kerül sor az eseménnyel érintett információs rendszer elsődleges azonosítására. Az észlelés tipikus forrásai a következők:

- az adott rendszert megfigyelő, üzemeltető személyek bejelentése,
- behatolásérzékelő rendszer (*intrusion detection system* – IDS) jelzése,
- behatolásmegelőző rendszer (*intrusion prevention system* – IPS) jelzése,
- naplóelemző rendszerek (*log-analysing system*) riasztási adatai,
- változáskövető rendszerek (*change tracking system*) riasztási adatai,
- egyéb.

Az észlelést követően a bejelentési adatok alapján közvetlenül meg kell határozni az esemény elsődleges tartalmát egy osztályozási (besorolási) folyamat révén. Ennek során azonosítani kell az esemény típusát – például különleges személyes adatokkal történő visszaélés, gyermekpornográfia, költségvetési csalás stb. –, amely alapján a vizsgálat várható iránya (például milyen típusú eszközökön valószínűsíthető az adott cselekményhez kapcsolódó elektronikus adat jelenléte). Az osztályba sorolást oly módon kell elvégezni, hogy az ne változtassa meg a feltételezhetően elektronikus adatot tartalmazó információs rendszer állapotát, vagyis a vizsgálat ezen szakaszában a cselekménnyel érintett információs rendszereken elemző szoftver még nem futtatható (megváltoztatná a rendszer állapotát).¹¹⁰

Reagálás

Az észlelést követően a reagálás (*respond*) során a rendelkezésre álló adatok és az elvégzett osztályba sorolás információi alapján meg kell kezdeni a feltételezhetően releváns elektronikus adatokat tartalmazó eszközök felmérését,

¹¹⁰ ISO/IEC 27043:2015, 14–15.

azonosítását, az esetleges kockázatok elhárítását vagy csökkentését. Ennek keretében kerülhet sor egy adott eszköz számítógépes hálózatról történő leválasztására vagy a kapcsolat fenntartására:

- amennyiben a releváns elektronikus adat feltételezhetően a helyi információs rendszeren található, úgy a számítógépes hálózati kapcsolat megszüntetendő a távoli hozzáférésből adódó adatmódosulás megakadályozása érdekében;
- ugyanakkor ha a releváns elektronikus adat feltételezhetően a távoli információs rendszeren található (például távoli asztali kapcsolat, bejelentkezett állapotú felhőszolgáltatás stb.), úgy a kapcsolat nem szakítható meg, illetve azonnal meg kell kezdeni a feltételezhetően releváns elektronikus adatok megszerzését.

Az egyes műveletek végrehajtása során különös figyelmet kell fordítani az elektronikus adatok, illetve az azokat tartalmazó eszközök sértetlensége megőrzésének. Ennek érdekében mérlegelni kell az élő rendszerekkel kapcsolatos tevékenységeket, úgymint a működő információs rendszer leállítása, adatok megnyitása szerkesztésre stb.¹¹¹

Megszerzési folyamatok

Az észlelést és reagálást követően kerülhet sor a potenciálisan releváns elektronikus adatok megszerzésére (*acquisitive process*), amely az elektronikus adatok hordozóinak felismerésétől és azonosításától kezdődően az elektronikus adatok megszerzéséig tart, s magában foglalja a hordozóeszközök összegyűjtését és megőrzését is. A továbbiakban – terjedelmi okokból – a leggyakoribb eszköztípusokra vonatkozó eljárásokat tekintjük át.¹¹²

Felismerés és azonosítás

Az elektronikus adatokat tartalmazó eszközök általában – különösen a nagy mérettartományba eső berendezések esetén – jól azonosíthatók, elhelyezkedésük

¹¹¹ ISO/IEC 27043:2015, 15.

¹¹² ISO/IEC 27043:2015, 15.

a használat általános módjából adódóan előre jelezhető. A méret, a használati hely és a működési jellemzők alapján az egyes eszköztípusok felismerése és azonosítása (*identify*) az alábbiak szerint történik:

Számítógépek

Az általánosan használt asztali (álló vagy fekvő kivitelben) számítógépek a $60 \times 30 \times 60$ cm és $32 \times 10 \times 32$ cm (magasság $\times$ szélesség $\times$ hosszúság) mérettartományba esnek, tömegük jellemzően 1–15 kg közé esik, színük korábban világosszürke, napjainkban inkább fekete, alakjuk általában téglatest.

Egyes készülékek azonban jelentősen eltérhetnek a fenti általános értékektől, így a szélsőségesen kis mérettartományú (*ultra small formfactor* – USFF) eszközök mérete $18 \times 6 \times 18$ cm is lehet, illetve az egy áramköri lapból álló eszközök (például Raspberry Pi) akár 6×3 cm méretű és 7 gramm tömegű formában is megjelenhetnek. A kisebb méretű eszközök potenciális adattartalma a lehetséges tárolóeszközök kis fizikai mérete miatt közel azonos lehet a „normál” méretű számítógépek adattartalmával.

A különleges kialakítású számítógéptípusoknál – mint az All-in-One PC-é és az iMac számítógépek – a számítógép vezérlő- és tárolóegységei a kijelzővel azonos modulban helyezkednek el, így megjelenésük alapján könnyen össze-teszethetők egy önálló kijelzővel. Méretük (a képernyő átlóját figyelembe véve) általában 23–27 hüvelyk (58–68 cm) közötti.

Az átlagnál nagyobb méretű és tömegű eszközök jellemzően a játékgépek (*gamer computer*) és a kiszolgáló gépek (*server computer*) közül kerülnek ki. A nagyobb számítási teljesítmény mellett ezekben az eszközökben több tároló is elhelyezkedhet, illetve a kiszolgáló számítógépek esetén távoli kapcsolódások is gyakoriak. Míg a gamer számítógépek megjelenése gyakran extravagáns (a formát és a színt is beleértve), addig a server számítógépek tipikusan *tower* (torony), *blade* (keskeny álló kivitel) vagy *rackmount* (keskeny fekvő kivitel) elrendezésűek.

A hordozható számítógépek vezérlő- és tárolóegységei és a kijelző (az all-in-one eszközökhöz hasonlóan) egybeépített, ezeknél azonban két különálló modulként (amelyeket esetenként külön is lehet választani) kerülnek kivitelezésre. Méretüket a képátló nagyságával szemléltetve az eszközkategória a 7 hüvelyktől (netbook, 2in1 tablet) a 10,6 és 16,4 hüvelyk közötti (minilaptop, laptop, notebook) eszközökön át az akár 18,4 hüvelykes képátlójú multimédia vagy gamer

laptopokig terjed. Vastagságuk az 10 mm-től az 52 mm-ig terjed, az előbbieket az ultravékony eszközök közül, míg az utóbbiak az ütésálló kivitelű készülékek közül kerülnek ki.

A számítógépek többnyire – a kiszolgálógép kivételével – személyhez kapcsolódó berendezések, ezért az elhelyezkedésük is ennek megfelelő. Gyakori a fali vagy padlóba süllyesztett elektromos csatlakozók közelében történő elhelyezés, valamint a vezetékes számítógépes hálózati kapcsolat is. Ez utóbbi nyomvonalának végigkövetése (kábelek vagy kábelcsatornák) lehetővé teszi a nem tipikus helyen elhelyezett eszközök azonosítását is. A kiszolgálógépek fizikai elhelyezkedése (helyben) általában kis méretű, hűtött, zárt helyiségben történik, vagy távoli helyszínen (adatközpont, fizikai- vagy virtuálisserver-bérlet, felhőinfrastruktúra-szolgáltatás stb.).

A számítógépek egyedi azonosítása a gyári számmal (*serial number*) történik, ennek hiányában az operációs rendszer licenckódja (amennyiben van ilyen) is használható. A gyártófüggetlen eszközök esetében leíró típusú azonosító alkalmazható, amely egy egyedi sorszámot és az adott helyszínt, helyiség és eszköz megnevezését tartalmazza.¹¹³

Tárolóeszközök

A tárolók a kis méretskálájú eszközök közé tartoznak fizikai méretük alapján. Az eszközökön tárolható elektronikus adatok tekintetében azonban rendkívül széles spektrumot mutatnak.

Méret és adattartalom tekintetében a SIM-kártyák a legkisebb tárolók közé tartoznak, amelyek nano (12,3 × 8,8 mm), micro (15 × 12 mm) és standard (25 × 15 mm) kivitelben és 128–256 KB adattároló kapacitással érhetők el. Önállóan kevésbé fordulnak elő, általában valamilyen mobilkommunikációra képes eszközbe behelyezve vagy abban végleges módon rögzítve lelhetők fel, különösen mobiltelefonokban, táblaszámítógépekben, laptopokban. A SIM-kártyák felismerésekor a hozzáférési adatok (mint PIN-kódok és PUK-kódok) megszerzésére is kísérletet kell tenni a bankkártyaméretű (54 × 85,6 mm) kódkártyák vagy a potenciális kódokat tartalmazó jegyzetek felkutatásával. A SIM-kártyák egyedi azonosítása az ICCID (*integrated circuit card identifier*, integrált

¹¹³ Gárdonyi Gergely – Anti Csaba László: *Krimináltechnikai kézikönyv*. Budapest, Semmelweis, 2020. 229–238.

áramköri kártyaazonosító) által történik, amelynek számsorozata a kártya felületén olvasható, illetve elektronikusan kiolvasható az eszközről.

A memóriakártyák a tárolókapacitás tekintetében mutatnak széles spektrumot: míg a 2000. év előtti gyártású kártyák leggyakoribb tárolókapacitása 2–128 MB közé esett, addig napjainkban a 16–32–128 GB kapacitású tárolók az elterjedtek. Méretük a PCMCIA-kártyák $85,6 \times 54$ mm-es méretétől a microSD-kártyák 15×11 mm-es méretéig terjed általában. A kártyatípusok közül napjainkban a *secure digital card* (SD card) tartozik a legelterjedtebbek közé, standard (32×24 mm), mini ($21,5 \times 20$ mm) és a korábban már említett mikro méret kivételben. A memóriakártyák általában eltávolítható tárolók, de egyes esetekben (például drónokban) a végleges (ragasztott) rögzítés is előfordul. A mikroméretű tárolók alkalmasak rejtett funkciójú (például óráként, tollként, kulcstartóként azonosítható) eszközökben történő elhelyezésre, ezért felismerésük esetenként rendkívüli körülményt igényel.

A nagy kapacitású külső tárolók (*external drive*) az adatok archiválására és hordozására is alkalmas eszközök. Alaphelyzetben a tárolók tokozása (védőburkolata) a beépített tároló méretét követi, így 3,5 hüvelykes – asztali számítógépekben alkalmazott – tárolók $146,99 \times 101,85$ mm-e, a 2,5 hüvelykes – hordozható számítógépekben alkalmazott – tárolók $100 \times 69,85$ mm-es méretéhez közelítenek. Az asztali kivitelű tárolók kevésbé, míg a hordozható és ütésálló eszközök erősebben robusztus kivitelűek.

Asztali kivitelű és hálózatra csatolt tárolók (*network attached storage* – NAS) esetén több merevelemet (leginkább 3,5 hüvelykes méretű) is elhelyezkedhet a tokozásban vagy eszközházban, így annak mérete is ehhez alkalmazkodik.

A tárolók rendszerint egyedi gyártási számmal rendelkeznek, így megkülönböztetésükhöz ez használható, vagy ennek hiányában a számítógépeknél ismertetett egyedi azonosítási módszer szerint lehet eljárni.¹¹⁴

Mobilkommunikációs eszközök és táblagépek

A hagyományos és okostelefonok mellett itt tárgyaljuk a táblaszámítógépek felismerését és azonosítását is, elsősorban a nagy mértékű eszköz és funkcionális hasonlóság miatt.

¹¹⁴ Vö. Gárdonyi – Anti (2020): i. m. 229–238.

A készülékek mérete a mini ($68 \times 28 \times 12$ mm – L8Star BM10) mérettől a normál funkcionális méreten ($104 \times 44 \times 16,3$ mm – Samsung B100) és a normál okostelefon-méreten át ($146,2 \times 70,9 \times 8,3$ mm – Samsung Galaxy A1) a tabletek ($254 \times 167 \times 6,1$ mm – Sony Xperia Z4 Tablet LTE) mérettartományáig terjed. Az eszközök felismerését nehezítheti a szokásos készülékkülalaktól történő jelentős eltérés (cigarettdoboz, toll vagy műanyag figura kivitelű eszközök), amely esetén az adott területen végzett elektromágneses hullámelemzéssel (élő mobilwifi, Bluetooth-kapcsolatok) lehetséges a bekapcsolt működő eszközök azonosítása. Kikapcsolt készülékek esetén a ferromágneses detektorok alkalmazása ajánlott.

A mobilkommunikációs eszközök gyakran tartalmaznak kivethető másodlagos tárat (memóriakártya), illetve SIM-kártyát. Ezek kezelésekor és azonosításakor minden esetben rögzíteni kell az eszközök kapcsolatát (mely készülékben volt eredetileg a tároló vagy a SIM).

A mobilkommunikációs eszközök egyedi gyári azonosítóval rendelkeznek, amely a készülékház külső burkolatán, illetve a készülékház belső felületén elhelyezett címkén olvasható. Eltávolított azonosító esetén az adat elektronikus kiolvasható vagy a számítógépeknél ismertetett egyedi azonosítási módszer szerint lehet elérni.

Egyéb eszközök

A fentiekől eltérő eszközök felismerésekor és azonosításuk esetén a korábban ismertetett általános eljárásokat kell alkalmazni, figyelembe véve az adott eszköztípus sajátosságait is. Így például drón azonosítása esetén a kivethető memóriakártyát a tárolóknál bemutatott módon kell kezelni, míg a digitális videórögzítők esetén a számítógépeknél írtak alkalmazandók.

A hardveres kriptopénztárcák (általában pendrive-hoz hasonló kialakítású eszközök) azonosítása során meg kell kísérelni a hozzáférést biztosító PIN-kódok és a fizetési tranzakciók érvényesítéséhez szükséges privát kulcsok (alfanumerikus karakterláncok) beszerzését is.

Amennyiben az elektronikus adatok hordozója nem jelen lévő fizikai eszköz, hanem távoli szolgáltatás (például felhőtárhely, elektronikus levelezési fiók stb.), úgy az elektronikus adatok forrásának egyedi azonosításához a szolgáltatás elnevezése és a hozzáférés felhasználó azonosítója szolgálhat (például Gmail: valaki@gmail.com).

Összegyűjtés

Az összegyűjtés (*collect*) során azokat a fizikai tárgyakat, amelyek potenciálisan elektronikus adatokat tartalmazhatnak, az eredeti helyükről ellenőrzött környezetbe, majd további vizsgálatra szállítják. Ennek során részletesen dokumentálni kell az eszköz eredeti helyét, annak kapcsolatait más eszközökkel (például eltávolítható másodlagos táruk), valamint ekkor kell beszerezni az egyes eszközökön található elektronikus adatokhoz történő hozzáférést lehetővé tevő adatokat és kiegészítő eszközöket is, amelyek tipikusan a következők lehetnek:

- felhasználói azonosítók (bejelentkezési név, e-mail-cím),
- jelszavak, képernyőlezárási minták, hozzáférési kódok,
- elektromos tápellátás kábelei és adapterei,
- adatátviteli kábelek (telefonkészülékek esetén),
- egyéb kapcsolódó információkat tartalmazó hordozók és kiegészítő eszközök.

Az összegyűjtés során (beleértve a szállítási fázist is) az adott eszköz és az azon potenciálisan megtalálható elektronikus adat integritásának megőrzése érdekében a megővásra vonatkozó eljárások betartása szükséges.

Megóvás

Az elektronikus adatok és az azokat hordozó tárgyak (eszközök, berendezések) megóvása (*preserve*) során kiemelt figyelmet kell fordítani az alábbi veszélyforrások elhárítására.

A mechanikai sérülések az egyes berendezések és eszközök egymáshoz ütése, leesése, vibrációja, vagy más mechanikai hatások során keletkeznek, amelyek ellen a készülékek elsődleges védőtokozása (például számítógépház, telefon elő- és hátlapja stb.) nyújt védelmet. Azok az eszközök, amelyek az elektronikus adat kiolvasásához szükséges mozgó alkatrészt is tartalmaznak (különösen a merevlemezek), a fizikai károsodás másodlagos hatásai (például író-olvasó fej sérülése, adatfelület sérülése) miatt károsodhatnak. A komplex eszközök (például mobiltelefon, okostelefon, tablet) kijelzőjének sérülése az adattartalom kinyerését nehezítheti, vagy az ezzel kapcsolatos költségeket növelheti.

A mechanikai sérülések elkerülése gondos csomagolással (buborékfóliás, légpárnás térkitöltők alkalmazása) és megfelelő rögzítéssel oldható meg.

Az elektromágneses terek elsősorban a mágneses tárolási elvű adathordozókat érintik (merevlemezes tárák, mágnesszalagos egységek) oly módon, hogy a tárolóterület egyes részein megváltoztathatják az információ rögzítésére szolgáló mágneses jelölők tulajdonságait, és ezzel megnövelhetik a hibás adatbitek számát, amely bizonyos mérték felett már nem korrigálható a beépített hibajavító megoldásokkal. Az elektromágneses terek ellen elsődleges távoltartással, amennyiben ilyen térben történő eszközelhelyezés vagy mozgatás történik, úgy Faraday-tasakkal vagy a Faraday-kalitka elvét megvalósító csomagolóanyaggal védekezhetünk.

A készülék irányából származó jelátvitelt (mobilkommunikáció, wifi- vagy Bluetooth-kapcsolat) az adott eszköz „repülőgép üzemmódba” (*airplane mode*) történő kapcsolásával érhetjük el, amennyiben az adott berendezés nincs lezárt állapotban. Lezárt (például jelkóddal védett) eszköz esetén a leárnyékolás (például Faraday-tasak, fémfóliás csomagolás stb.) megvédheti a készüléket a távolról (például mobilkommunikáción keresztül történő) módosítástól, ugyanakkor az árnyékolásból eredő jelvesztés miatt a készülék magasabb teljesítmény alkalmazásával próbálhatja meg felvenni a kapcsolatot a mobilkommunikációs hálózattal. A magasabb teljesítmény következménye az akkumulátor lemerülése, illetve túlmelegedése lehet, ezért az ismertetett esetben a folyamatos tápellátás (például power bank) mellett a készülék hűtéséről (például jégakku alkalmazásával) is gondoskodni kell. Mindezen tevékenységek végrehajtása akkor szükséges, ha a készülék kikapcsolása valamilyen okból nem lehetséges, vagy nem célszerű (jelkódos védelem vagy kikapcsolás utáni zárolás).

A statikus elektromosság elsősorban az elektronikus elvű adattárák (SSD, pendrive, memóriakártya), illetve az integrált vezérlőelektronikával szerelt eszközök (például merevlemezes tárolók) esetében okozhat károkat az adathoz történő hozzáférés útvonalának megszakítása vagy az adat egyéb módon történő elérhetetlenné tétele révén. A veszély csökkenthető az eszközök és csomagolásuk földelése segítségével.

Az extrém környezeti hőmérséklet, a por és a nedvesség elleni védekezést elsődlegesen a felsorolt hatások elkerülésével, másodlagosan megfelelő ellenintézkedéssel (aktív vagy passzív hűtés) és csomagolással (védőfólia) kell megoldani.

Megszerzés

Az elektronikus adatok megszerzése (*acquire*) elsődlegesen a szakértői laboratóriumban történik a statikus elemzés részben írtak szerint. Szükség esetén az elektronikus adatok megszerzésére az eszköz megtalálásának eredeti helyszínén is sor kerülhet az élő rendszer elemzése részben írtak szerint.

Az elektronikus adatok megszerzése az erre a célra megfelelő szakismertekkel és gyakorlattal rendelkező és arra feljogosított személy feladata, aki lehet szakértő, szakkonzultáns vagy a nyomozó hatóság szakképzett munkatársa is.

Az elektronikus adatok vizsgálati modelljei

Az elektronikus adatok vizsgálata alapvetően két megközelítést jelent: a statikus elemzés során a korábban megszerzett vizsgálati tárgy, bűnjel elemzése szakértői laboratóriumban, míg az élő rendszer elemzése során a vizsgálati tárgy elsődleges azonosítása (felismerése) a valóságos vagy virtuális helyszínen történik, amelyet közvetlenül követ az elektronikus adatok megszerzése, majd azok elemzése (akár a helyszínen, akár szakértői laboratóriumban).

Statikus elemzés

Az elnevezés arra utal, hogy a vizsgálat az eredeti környezetéből kiemelt, kikapcsolt állapotú eszköz (mint az elektronikus adatot hordozó tárgy) vizsgálatára vonatkozik.

Azonosítás

A szakértői munka a megfelelően azonosított, károsító hatásoktól megvédett és a vizsgálat helyszínére – szakértői laboratórium – szállított vizsgálati tárgy, bűnjel ismételt azonosításával indul, amelynek alapidokumentuma a szakértői vizsgálatot elrendelő irat (határozat) és a szakértő részére rendelkezésre bocsátott egyéb iratok, adatok. Elsőként a vizsgálati tárgyak, bűnjelek mennyiségi ellenőrzését kell elvégezni az átvételi iratok adatai alapján. Ekkor kell meggyőződni arról is, hogy az egyes eszközök tartalmazznak-e további, elektronikus adat

önálló tárolására alkalmas egységeket – mint mobiltelefon esetén a SIM-kártya és memóriakártya –, illetve az egységként átadott berendezések – mint asztali számítógép, laptop stb. – esetén ekkor kell megállapítani az adott eszközben található adattárolók mennyiségét és típusát is. A minőségi azonosítás során – az átvételi iratok alapján – ellenőrizni és szükség esetén korrigálni kell az átvett eszközök, berendezések gyártmány-, típus- és egyéb minőségi adatait (mint mobiltelefon esetén az IMEI-azonosító, sorozatszám stb.). A véglegesített adatokat – az esetleges eltérésekre történő figyelemfelhívással együtt – fel kell tüntetni a vizsgálat eredményét tartalmazó szakértői véleményben.¹¹⁵

Vizsgálat előkészítése

A statikus elemzés – lehetőség szerint – az elektronikus adat másolatán történik, ezért a szakértői vizsgálat előkészítése a feltehetően elektronikus adatot tartalmazó eredeti vizsgálati tárgy, bűnjel tartalmának bitazonos másolásával kezdődik. A másoláshoz az erre a célra rendszeresített célhardver (*forensic duplicator*, forenzikus adatmásoló berendezés), illetve célhardver és célszoftver (*forensic writeblocker*, forenzikus írásvédő és *forensic imager*, forenzikus lemezképkészítő alkalmazás) eszközökkel történik.

Amennyiben műszaki vagy üzemeltetési okból a statikus vizsgálat nem lehetséges, úgy a vizsgálatot az élő rendszerek vizsgálati eljárása szerint kell lefolytatni.

Abban az esetben, ha nincs mód bitazonos másolat készítésére, úgy a statikus elemzés – az írásvédelem biztosítása mellett – elvégezhető az elektronikus adat eredeti tárolóján is. Egyes esetekben, ha az adatokhoz történő hardverközeli hozzáférés nem lehetséges valamilyen okból, úgy az adatokat az eredeti (natív) fájlrendszer felhasználásával történő másolás módszerével kell megszerezni, és a további szakértői vizsgálatot az így kinyert adatokon kell elvégezni.

¹¹⁵ Máté István Zsolt: *Az igazságügyi informatikai szakértő a büntetőeljárásban*. PhD-dolgozat. Pécs, Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola, 2018. 130.

Vizsgálat

A statikus elemzés során a bitazonos másolatból az adatok helyreállítása – törölt adatok visszaállítása (*data recovery*), adatok összeállítása fájl töredékekből (*file carving*) –, csoportosítása és értelmezése történik. Mind a csoportosítás, mind az értelmezés történhet szoftveres eljárással, szoftveres eljárással emberi közreműködéssel, illetve kizárólag emberi közreműködéssel. Az adatcsoportosítás általános területei a következők:

- releváns fájl típusok (dokumentumok, táblázatok, adatbázisok, képek, mozgóképek, hangok stb.) kigyűjtése;
- adatok időbeli elhatárolása (*timeline*);
- metaadatok alapján történő kiválogatás (létrehozó eszköz, jogosultság stb.);
- képi tartalom azonosítása és elhatárolása, különösen az alábbi tartalmakra vonatkozóan:
 - pénz,
 - dokumentum,
 - kábítószer,
 - szexuális tartalom,
 - önkényuralmi jelképek,
 - fegyverek;
- mozgóképi tartalom azonosítása és elhatárolása a képi tartalomnál írtak szerint.

Az adatértelmezés különösen a következő műveleteket jelenti:

- optikai karakterfelismerés szöveget tartalmazó képi adatokon,
- kulcsszavas keresés szöveges tartalomban,
- az adott fájl típus betöltése olvasó (*reader*) vagy megtekintő (*viewer*) alkalmazásba,
- napló- (*log*-) állomány betöltése naplóelemző (*log analyzer*) alkalmazásba,
- egyéb állományspecifikus műveletek.

Élő rendszer elemzése

Az élő rendszer elemzése (*live analysis*) során nincs lehetőség bitazonos másolat készítésére, mivel

- egyedi hardver nem teszi lehetővé a tároló eltávolítását;
- különleges csatolófelület (*interface*) miatt nem csatlakoztatható a másolóeszközhöz;
- használatban lévő, kiemelt fontosságú eszköz tartalmazza az adatot (orvosi berendezés, komplex, nem megbontható szerkezetű informatikai rendszer stb.);
- egyéb akadályozó tényezők miatt.

A fenti esetekben előzetes helyzetfelmérés alapján (tehát nem az adott helyszínen ad hoc módon) kockázatelemzéssel kell meghatározni az adatmegszerzés kivitelezhetőségét, a megszerzési prioritásokat és kockázatokat, különösen az alábbi szempontok figyelembevétele mellett:

- az élő (bekapcsolt) rendszerekről történő adatmegszerzés megváltoztatja a rendszer állapotát, amely a rendszer instabilitását is okozhatja;
- titkosított tárolóeszközök esetén a rendszer kikapcsolása megakadályozhatja az adatokhoz történő hozzáférést, ezért a titkosítás jelenlétét megfelelő eszközzel ellenőrizni kell;
- az élő rendszerek külső kapcsolatai (vezetékes vagy vezeték nélküli számítógépes hálózati kapcsolat) vagy távoli vezérlés jelenléte befolyásolhatja az adatmegszerzés folyamatát.¹¹⁶

A felsorolt kockázatok értékelését és az egyes adatforrások azonosítását (statisztikus vizsgálattal azonos eljárás szerint) követően meg kell határozni az adatok megszerzésének sorrendjét, amelyet az adatok változékonysága (*order of volatility*) határoz meg az alábbiak szerint (amennyiben az adott ügy szempontjából az releváns):

- processzorregiszter és gyorsítótár-tartalmak,
- számítógépes hálózati útvonalválasztó útvonaltáblája,
- címfeloldási protokoll (ARP) gyorsítótára (az IP-címek és a fizikai címek megfeleltethető táblázata),
- feladat-végrehajtási tábla (*processtable*),
- operációs rendszer rendszermag-statisztika és rendszermagmodulok tartalma (*kernel statistics and modules*),
- operatív tár tartalma (*main memory*),
- ideiglenes fájlrendszer tartalma (*temporary file systems*),

¹¹⁶ ISO/IEC 27037:2012, 25–27.

- másodlagos memória tartalma (*secondary memory*),
- útvonalválasztó eszközök beállításai (*router configuration*),
- számítógépes hálózati összeköttetés-rendszer (*network topology*),
- további adatok.¹¹⁷

Az adatmegszerzés során a fentiek mellett folyamatosan gondoskodni kell a kérdéses rendszer tápellátásának biztosításáról oly módon, hogy azt sem technikai, sem emberi esemény, illetve beavatkozás ne zavarhassa meg.

A helyszínen végzett adatmegszerzés során figyelembe kell venni a vizsgálati tárgyak tárolókapacitásait és adatátviteli sebességét. Ezek az adatok általában csak a vizsgálat helyszínén, a vizsgálat megkezdését közvetlenül követően szerezhetők be, így a helyszíni vizsgálat időtartama ezen adatok és az ismert általános adatátviteli sebességek alapján becsülhető. Az élő rendszer vizsgálataánál használt leggyakoribb csatlakozótípusok és átviteli sebességek az egyes készülékek esetén a következők:

- Az USB 1.x – a fehér színkóddal jelölt 4 érintkezős csatlakozó csupán 1,5 MB/s maximális átviteli sebességre képes, előfordulása 2001 előtt gyártott eszközökön lehetséges, helyszíni adatmentésre nem alkalmas (1 DVD-nyi adatot körülbelül 1 óra alatt képes továbbítani).
- Az USB 2.x fekete színkóddal jelölt 4 érintkezős csatlakozó 60 MB/s maximális átviteli sebességre képes, előfordulása 2001 után gyártott eszközökön lehetséges, helyszíni adatmentésre korlátozottan alkalmas (1 DVD-nyi adatot körülbelül 1 perc alatt képes továbbítani).
- Az USB 3.x kék színkóddal jelölt 9 érintkezős csatlakozó 6251 280 MB/s maximális átviteli sebességre képes, előfordulása 2011 után gyártott eszközökön lehetséges, helyszíni adatmentésre alkalmas (1 DVD-nyi adatot körülbelül 4-8 másodperc alatt képes továbbítani).
- FireWire 400-800-1600-3200 [IEEE 1394 /1394b]: a 4-6-9 érintkezős csatlakozók 49 – 393 MB/s maximális átviteli sebességre képesek, előfordulásuk a nagyobb teljesítményű, elsősorban multimédiás célokra is szolgáló eszközökön gyakoribb, helyszíni adatmentésre alkalmas (1 DVD-nyi adatot körülbelül 12–96 másodperc alatt képes továbbítani).
- eSATA300/600: a 7 érintkezős csatlakozó 300–600 MB/s maximális átviteli sebességre képes, előfordulása 2004 után gyártott eszközökön

¹¹⁷ Matthew Braid: *Collecting electronic evidence after a system compromise*. Brisbane, AusCERT, 2001. 13.

lehetséges, helyszíni adatmentésre alkalmas (1 DVD-nyi adatot körülbelül 8–16 másodperc alatt képes továbbítani).

- Thunderbolt 1/2/3: a 20 érintkezős csatlakozó 1,25–2,5 5 GB/s maximális átviteli sebességre képes, előfordulása 2011 után gyártott eszközökön lehetséges, helyszíni adatmentésre alkalmas (1 DVD-nyi adatot körülbelül 1–4 másodperc alatt képes továbbítani).

Amennyiben az adatokat helyi vagy nagy távolságú számítógépes hálózati kapcsolaton keresztül szükséges megszerezni, úgy az alábbi átviteli paraméterekkel kell kalkulálni:

- FastEthernet (100BASE-X) szabványú helyi hálózatok esetén 12,5 MB/s maximális átviteli sebességre lehet számítani ideális körülmények között (ha az adott hálózati szakaszon nincs egyéb adatforgalom, 1 DVD-nyi adatot körülbelül 6 perc alatt képes továbbítani).
- GigabitEthernet (1000BASE-X) szabványú helyi hálózatok esetén 125 MB/s maximális átviteli sebességre lehet számítani ideális körülmények között (ha az adott hálózati szakaszon nincs egyéb adatforgalom, 1 DVD-nyi adatot körülbelül 38 másodperc alatt képes továbbítani).

A fentiekre figyelemmel az élő rendszerből történő adatkinyerés időtartamát a megszerzendő adatok mennyisége (tárolási mérete) és az adatátvitel elméleti sebességének hányadosa adja. Az így kapott elsődleges elméleti megszerzési időt növelhetik az egyéb befolyásoló körülmények, úgymint párhuzamos adatforgalom, több adatforrásból azonos kimeneti csatornán történő adatkinyerés. Az elméleti adatmegszerzési idő kalkulációját követően mérlegelni kell annak veszélyét, hogy az adatátvitel megszakadhat-e. Ennek okai lehetnek:

- távoli hozzáférés a helyi eszközhöz,
- távoli rendszer lekapcsolása,
- távoli és helyi rendszer közötti adatkapcsolat megszakítása,
- helyi áramellátás kimaradása,
- eszközterhelésből adódó körülmények (például túlmelegedés).

Az élő rendszer vizsgálata esetén megszerzett adatok további vizsgálata a statikus vizsgálati eljárásnál ismertetett módon történik szakértői laboratóriumban.

Szakértői vélemény és annak felhasználása

Az elektronikus adatok kinyerését követően elkészülő igazságügyi informatikai szakértői vélemény tartalmazza mindazon körülmények leírását, amelyek a vizsgálat szempontjából releváns, így jellegzetes tartalmi elemei közé tartozik a jogszabályban előírtak közül különösen

- a vizsgálat módszerének általános leírása vagy hivatkozás a módszert leíró dokumentumra;
- a felhasznált eszközök felsorolása (hardver- és szoftvereszközök);
- a felhasznált szakirodalom és egyéb hivatkozások megadása;
- az egyes eszközök vizsgálatának leírása;
- a kinyert elektronikus adatok bemutatása nyomtatott és digitális formában.

A szakértői vélemény szövegében a szakértő számára feltett kérdésekre adott válaszok és az azokat alátámasztó, jellegzetesen a digitális mellékleten megtalálható elektronikus adatok a leghangsúlyosabbak, ezek értelmezése és felhasználása a kirendelő hatóság erre kijelölt munkatársának feladata.

A szakértői válaszok és különösen a digitális mellékleten megtalálható elektronikus adatok kezeléséhez felhasználói szintű informatikai ismeret szükséges, ami azt jelenti, hogy az erre kijelölt személynek a következőket kell végrehajtania:

- számítógép általános kezelése,
- szoftverek (fájlkezelő programok, irodai programok) kezelése,
- adathordozók (külső táruk, USB-kulcsok, optikai adathordozók stb.) kezelése,
- általánosan ismert fájltypusok kezelése (.pdf, .doc, .jpg stb.),
- kommunikációs alkalmazások (azonnali üzenetküldő programok, levelezőprogramok) kezelése,
- számítógépes hálózati ismeretek (böngészőprogramok, felhőszolgáltatások használata).

A felsorolt ismeretek és készségek révén a szakértői véleményben bemutatott elektronikus adatok információtartalma felhasználhatóvá válik az adott eljárásban.

Felhasznált irodalom

Szakkönyvek, tanulmányok

- 2G / 3G / 4G – Is it all about the speed. *Mikroe*, 2016. május 27. Online: www.mikroe.com/blog/2g-3g-4g-speed
- Balog Zsolt: *LTE feletti beszédátvitel monitorozási módszerei a maghálózatban*. TDK-dolgozat. Budapest, Budapesti Műszaki és Gazdaságtudományi Egyetem Villamosmérnöki és Informatikai Kar Távközlési és Médiainformatikai Tanszék, 2016. Online: <https://tdk.bme.hu/vik/downloadpaper/lte-feletti-beszedatvitel-volte-monitorozasi>
- Bartlett, Jamie: *The dark net*. London, Windmill Books, 2015.
- Béres Roland: *Mobilhálózatok energiatakarékos üzemeltetése*. TDK-dolgozat. Budapest, Budapesti Műszaki és Gazdaságtudományi Egyetem Villamosmérnöki és Informatikai Kar Távközlési és Médiainformatikai Tanszék, 2012. Online: <https://tdk.bme.hu/VIK/DownloadPaper/FMC-Fixmobil-konvergalt-hozzaferesi>
- Boda József – Dobák Imre (szerk.): *A nemzetbiztonság technikai kihívásai a 21. században*. Budapest, NKE Szolgáltató Nonprofit Kft, 2015.
- Boda József (főszerk.): *Rendészettudományi szaklexikon*. Budapest, Ludovika Egyetemi Kiadó, 2019.
- Bodlaki Ákos – Csernay Andor – Mátyás Péter – Muha Lajos – Papp György – Vadász Dezső: *Informatikai rendszerek biztonsági követelményei*. Budapest, Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága (MeH ITB), 12. számú ajánlása. 1996.
- Braid, Matthew: *Collecting electronic evidence after a system compromise*. Brisbane, AusCERT, 2001.
- Brinson, Ashley – Abigail Robinson – Marcus Rogers: A cyber forensics ontology: Creating a new approach to studying cyber forensics. *Digital Investigation*, (2006), 3. 37–43. Online: <https://doi.org/10.1016/j.diin.2006.06.008>
- Campanella, Nick: The beginner's guide to virtual PBX. *Getvoip*, 2017. szeptember 08. Online: <https://getvoip.com/blog/2017/09/08/what-is-virtual-pbx/>
- Casey, Ehogan: *Digital evidence and computer crime*. Amsterdam, Elsevier, 2011.
- Dérné Hopoczky Janka: *Univerzális joghatóság pro és kontra. Jogi tanulmányok*, 14. (2010), 2. 339–354. Online: http://epa.niif.hu/02600/02687/00002/pdf/EPA02687_jogi_tanulmanyok_2010_02_339-354.pdf
- Eszes István: *Digitális gazdaság. Az e-kereskedelem marketinges szemmel*. Budapest, Nemzeti Tankönyvkiadó, 2012. 61–126.

- Gárdonyi Gergely – Anti Csaba László: *Krimináltechnikai kézikönyv*. Budapest, Semmelweis, 2020.
- Gazdag Tibor – Kovács Zoltán: Felhő alapú új pénzügyi tranzakciós lehetőségek és azok veszélyei. *Nemzetbiztonsági Szemle*, 2. (2014), 2. 36–57. Online: http://epa.oszk.hu/02500/02538/00003/pdf/EPA02538_nemzetbiztonsagi_szemle_2014_02_036-057.pdf
- Gyaraki Réka: A kiberbűncselekmények megjelenése és helyzete napjainkban. In Mezei Kitti (szerk.): *A bűnügyi tudományok és az informatika*. Budapest – Pécs, Pécsi Tudományegyetem Állam- és Jogtudományi Kar – MTA Társadalomtudományi Kutatóközpont, 2019a. 83–101.
- Gyaraki Réka: *A számítógépes bűnözés nyomozásának problémája*. Doktori disszertáció. Pécs, PTE ÁJK Doktori Iskola, 2019b.
- Haardt, Martin: *CA topology based on 3-sector-cell system*. 2008. Online: www.researchgate.net/figure/CA-topology-based-on-3-sector-cell-system_fig2_220056898
- Haig Zsolt: Az információbiztonság komplex értelmezése. Robothadviselés 6. Tudományos Szakmai Konferencia 2006. november 22. *Hadmérnök*. Különszám. Online: www.hadmernok.hu/kulonszamok/robothadviseles6/haig_rw6.pdf
- Halász Viktor: *Kriptovaluták a bűnüldözésben – új kihívások és lehetséges válaszok*. Diplomamunka. NKE NETK, 2018.
- Henderson, Lance: *Tor and the dark art of anonymity*. Amazon Media EU, 2016. 13–98.
- Horvai Ferenc: Ötven éve a világűrben. *Meteor*, 37. (2007), 10. 12.
- Internet Radicalization. U.S. Government, Department of Defense, U.S. Naval Postgraduate School. 2017. 7–63.
- Jolliff, Jeremiah: *Islamic extremism and cybercrime*. Leipzig, Amazon, 2017.
- Kartit, Zaid – Hamza Kamal Idrissi – Mohamed El marraki – Kartit Ali: *Network Issues in cloud computing and countermeasures*. 2014. Online: www.researchgate.net/publication/290445671_Network_Issues_in_cloud_computing_and_countermeasures
- Kiss Tibor: Agresszió szerepe az internetes tartalom-bűncselekmények oksági mechanizmusában. In: Zséges Barbara (szerk.): *Kriminológiai közlemények 77*. Budapest, Magyar Kriminológiai Társaság, 2017. 257–270.
- Kovács Zoltán: *Az infokommunikációs rendszerek nemzetbiztonsági kihívásai*. Doktori értekezés. Budapest, Nemzeti Közszerzői Egyetem, 2015. Online: http://m.ludita.uni-nke.hu/repozitorium/handle/11410/10868nke.hu/xmlui/bitstream/handle/123456789/12346/kovacs_zoltan_doktori_ertekezes.pdf?sequence=15
- Kurose, James F. – Keith Ross: *Számítógép-hálózatok működése. Alkalmazásorientált megközelítés*. Budapest, Panem, 2009.

- Lambert Miklós: Bináris prefixumok. *Műszerügyi és Méréstechnikai Közlemények*, 37. (2001), 67. Online: www.muszeroldal.hu/MMK/nr67/lambert.html
- Lazakidou, Athina A. – Konstantinos M. Siassiakos: *Handbook of research on distributed medical informatics and e-health*. Hershey – New York, Medical Information Science Reference, 2009. Online: <https://doi.org/10.4018/978-1-60566-002-8>
- Lichtblau, Erich: *The nazis next door: how America became a safe haven for Hitler's men*. Boston – New York, Houghton Mifflin Harcourt, 2014.
- Máté István Zsolt: *Az igazságügyi informatikai szakértő a büntetőeljáráásban*. PhD-dolgozat. Pécs, Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola, 2018.
- Mealer, Michael: *Internet Radicalization: Actual Threat or Phantom Menace*. US Government, Department of Defense, Naval Postgraduate School, Monterey, 2012. 7–63.
- Meyers, Mike: *PC hardver és karbantartása*. Budapest, Panem, 2004.
- Mezei Kitti – Dornfeld László: Az online gyermekpornográfia elleni küzdelem aktuális kérdései. *Infokommunikáció és Jog*, 14. (2017), 68. 32–37.
- Mezei Kitti – Nagy Zoltán András: A zsarolóvírus és a botnet, mint napjaink két legveszélyesebb számítógépes vírusa. In Gaál Gyula – Hautzinger Zoltán (szerk.): *Szent Lászlótól a modern kori rendészettudományig*. Pécs, Pécsi Határőr Tudományos Közlemények, 19. (2017). 163–168. Online: http://real.mtak.hu/102318/1/nagy_mezei.pdf
- Mezei Kitti: A kriptovaluták büntető anyagi és eljárásjogi kihívásai. *Pro Futuro*, 9. (2019b), 1. 79–98. Online: <https://doi.org/10.26521/Profuturo/1/2019/3906>
- Mezei Kitti: A szervezett bűnözés az interneten. In Mezei Kitti (szerk.): *A bűnügyi tudományok és az informatika*. Budapest – Pécs, Pécsi Tudományegyetem Állam- és Jogtudományi Kar – MTA Társadalomtudományi Kutatóközpont, 2019a. 125–147.
- Miskolczi Barna – Szathmáry Zoltán: *Büntetőjogi kérdések az információ korában*. Budapest, HVG–ORAC, 2018.
- Molnár György: Az IKT-val támogatott tanulási környezet követelményei és fejlesztési lehetőségei. 2008. Online: www.mszt.iif.hu/documents/szsz0803-molnar.pdf
- Mouly, Michel – Marie-Bernadette Pautet: *The GSM system for mobile communications*. Telecom Publishing, 1992.
- Muha Lajos: *A Magyar Köztársaság kritikus információs infrastruktúráinak védelme*. PhD-értekezés. Budapest, ZMNE, 2007. Online: <http://ludita.uni-nke.hu/repozitorium/handle/11410/9894>
- Muha Lajos: Fogalmak és definíciók. In Muha Lajos (szerk.): *Az informatikai biztonság kézikönyve*. Budapest, Verlag Dashöfer Szakkiadó, 2004.

- Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana. *Bolyai Szemle*, 17. (2008), 4. 137–156.
- Muha Lajos – Krasznay Csaba: *Az elektronikus információs rendszerek biztonságának menedzselése*. Budapest, Nemzeti Közszerológati Egyetem, 2018. Online: http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/11173/Az%20elektronikus%20inform%C3%A1ci%C3%B3s%20rendszerek%20biztons%C3%A1g%C3%A1nak%20menedzsel%C3%A9se_2018.pdf?sequence=1&isAllowed=y
- Munk Sándor: Információbiztonság vs. informatikai biztonság. Robothadviselés 7. Tudományos Szakmai Konferencia 2007. november 27. *Hadmérnök*, Különszám. Online: www.hadmernok.hu/kulonszamok/robothadviseles7/munk_rw7.pdf
- Nagy Ferenc: Az európai büntetőjog fejlődési irányairól és jogállami alapjáról. *Acta Universitatis Szegediensis Acta, Juridica Et Politica, Tomus LXI*. Szeged, 2002.
- Nagy Zoltán András: A számítástechnikai rendszer és adatok elleni új bűncselekmények. *Belügyi Szemle*, 40. (2002), 11–12. 27–41.
- Nagy Zoltán András: Az informatika és a büntetőjog. *Magyar Jog*, 38. (1991), 1. 21–26.
- Nemzeti Adatvédelmi és Információszabadság Hatóság: *NAIH Adatvédelmi Értelmező Szótár*. (é. n.). Online: www.naih.hu/adatvedelmi-szotar.html
- Pásztor András: *QoS támogatás vizsgálata LTE alapú femtocellák ütemezési kérdéseiben*. TDK-dolgozat. Budapest, Budapesti Műszaki és Gazdaságtudományi Egyetem Villamosmérnöki és Informatikai Kar Híradástechnikai Tanszék, 2012. Online: <https://tdk.bme.hu/VIK/DownloadPaper/QoS-tamogat-as-vizsgalata-LTE-alapu-femtocellak>
- Pletl Szilveszter – Kincses Zoltán: Supervisory control and data acquisition. SCADA. PLC és SCADA rendszerek. 2014. Online: http://eta.bibl.u-szeged.hu/900/1/2011_0104-szte_5_plc_es_scada.pdf
- Pokol Béla: *Politikaelmélet: Társadalomtudományi trilógia III*. Budapest, Századvég, 2004. Online: www.ssoar.info/ssoar/bitstream/handle/document/10430/ssoar-2006-pokol-politikaelmelet_tarsadalomtudomanyi_trilogia_iii.pdf?sequence=1
- Polt Péter: A számítógépes bűnözés. *Belügyi Szemle*, 21. (1983), 6. 60–64.
- Pusztai László: A számítógépes bűncselekmények nyomozása. *Belügyi Szemle*, 26. (1988), 3. 42–48.
- Sallai, Gyula: Defining infocommunications and related terms. *Acta Polytechnica Hungarica*, 9. (2012), 6. 5–15. Online: www.uni-obuda.hu/journal/Sallai_38.pdf
- Sangdao, Chokchai: *Mobile phone evolution. Part 3*. Mahanakorn University of Technology, 2014. október 10. 31. Online: www.mut.ac.th/research-detail-37
- Senker, Cath: *Cybercrime and the darknet*. London, Arcturus Publishing Ltd., 2017.

- Simon Béla: A bűnüldözés előtt álló digitális kihívások. *Magyar Rendészet*, 17. (2017), 5. 83–104. Online: <https://folyoirat.ludovika.hu/index.php/magyrend/article/view/1777/1076>
- Simon Béla: A kriptovaluták és a kapcsolódó rendészeti kihívások. In Mezei Kitti (szerk.): *A bűnügyi tudományok és az informatika*. Budapest – Pécs, PTE ÁJK – MTA Társadalomtudományi Kutatóközpont, 2019. 169–186.
- Szabó Bálint – Márfoldi Endre: *Számítógépes hálózatok*. Eger, Eszterházy Károly Főiskola, 2011.
- Szabó Csaba: A 3D nyomtatási technológiával előállított tűzfegyverek biztonságpolitikai kihívásainak vizsgálata a fegyverrendészet aspektusából I–II. *Nemzetbiztonsági Szemle*, 5. (2017), 4. 91–124. Online: http://epa.oszk.hu/02500/02538/00021/pdf/EPA02538_nemzetbiztonsagi_szemle_2017_04_091-109.pdf; http://epa.oszk.hu/02500/02538/00021/pdf/EPA02538_nemzetbiztonsagi_szemle_2017_04_110-124.pdf
- Szücs Péter: Technológiai fejlődés és hatása napjaink titkosszolgálataira. In Tanenbaum, Andrew – David Wetherall: *Számítógép-hálózatok*. Budapest, Panem Könyvek. Taramix Kft., 2013. Online: <https://gyires.inf.unideb.hu/GyBITT/30/index.html>. 2013.
- Ürmösné Simon Gabriella: Miben segítik a nyelvi ujjnyomok a nyomozást? *Magyar Rendészet*, 19. (2019), 1. 65–75. Online: <http://doi.org/10.32577/mr.2019.1.4>
- Vega-Rodriguez, Miguel A. – José M. Chaves-González: Multiobjective frequency assignment problem. *MSTAR::UNEX*, 2020. Online: http://mstar.unex.es/index.php?option=com_content&view=article&id=59&Itemid=55
- Ward, Bob: *From nazis to NASA: the life of Wernher Von Braun*. London, Sutton Publ., 2006. Online: http://epa.oszk.hu/03000/03054/00350/pdf/EPA03054_meteor_2007_10_10-12.pdf

Jogforrások

- 11/2003. (V.8) IM-BM-PM együttes rendelet A lefoglalás és a büntetőeljárás során lefoglalt dolgok kezelésének, nyilvántartásának, előzetes értékesítésének és megsemmisítésének szabályairól, valamint az elkobzás végrehajtásáról
2013. évi L. törvény az állami és önkormányzati szervek elektronikus információ biztonságáról
- A Büntető Törvénykönyvről szóló 2012. évi C. törvény (Btk.)
- A Büntetőeljárásról szóló 2017. évi XC. törvény (Be.)
- A hitelintézetekről és pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII. törvény (Hpt.)

Az igazságügyi szakértőkről szóló 2016. évi XXIX. törvény
 Az igazságügyi szakértői szakterületekről, valamint az azokhoz kapcsolódó képzési és egyéb szakmai feltételekről szóló 9/2006. (II. 27.) IM rendelet
 A nyomozás és az előkészítő eljárás részletes szabályairól szóló 100/2018. (VI. 8.) Korm. rendelet (Nyer.)
 Budapesti egyezmény (2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről)
 CoERecommendation 1989, Council of Europe Recommendation No. R (89) 9 on Computer-related Crime – Az Európa Tanács Ajánlása a számítógépes környezetben elkövetett bűncselekményekre
 Eurojustreport (2003). Online: <http://eurojust.europa.eu/doclibrary/corporate/eurojust%20Annual%20Reports/Annual%20Report%202003/Annual-Report-2003-EN.pdf>
 62 – 64.
 Security within the North Atlantic Treaty Organisation (NATO) – C-M(2002)49

Internetes források

Bureau International des Expositions. Online: www.bic-paris.org/site/en/1876-philadelphia
 Cisco Certified Expert. Network Design. PBX sand the PSTN. Online: www.ccexpert.us/network-design/pbxes-and-the-pstn.html
 Data SecurityLifecycle 2.0. Online: <https://securosis.com/blog/data-security-lifecycle-2.0>
 Denet India. Top Benefits of IP PBX. 2019.12.21. Online: <https://medium.com/@dcnetindia.com/top-benefits-of-ip-pbx-ffd99b4c2c99>
 Gartner Glossary: Network management center. Online: www.gartner.com/en/information-technology/glossary/nmc-network-management-center
 GSM Functionalities. YateBTS Wiki. Online: https://wiki.yatebts.com/index.php/GSM_Functionalities
 Gsm oktatási anyag. Online: www.muszeroldal.hu/measurenotes/gsm.pdf
 Gsm Network Architecture. Online: www.electronics-notes.com/articles/connectivity/2g-gsm/network-architecture.php
 India calling (s. a.). 5G networks may be in place by 2020. Elérhető: www.aashah.com/event/news-23/
 ISO/IEC 27037:2012 Information technology — Security techniques — Guide lines for identification, collection, acquisition, and preservation of digital evidence. Geneva, International Organization for Standardization. Online: www.iso.org/standard/44381.html

ISO/IEC 27043:2015 Information technology — Security techniques — Incident investigation principles and processes. Geneva, International Organization for Standardization. Online: www.iso.org/standard/44407.html

ISO/IEC 7813:2006 Information technology — Identification cards — Financial transaction card. Online: www.iso.org/standard/43317.html

JUNIPER: 3GPP WLAN Interworking Reference Model. Online: www.juniper.net/documentation/software/aaa_802/imsaaa11/sw-imsaaa-admin/html/Introduction3.html.

Nemzeti Infokommunikációs Stratégia 2014–2020. Online: www.kormany.hu/download/a/f7/30000/NIS_v%C3%A9gleges.pdf

NMHH *Vezetékes gyorsjelentés*. Online: http://nmhh.hu/cikk/209508/Vezetekes_gyorsjelentes__2019_november

Ozeki: *Company PBX-Voip*. Online: www.voip-sip-sdk.com/p_246-company-pbx-voip.html

Rich: *Data Security Lifecycle 2.0. Securosis. Blog*. 2011. szeptember 6. Online: <https://securosis.com/blog/data-security-lifecycle-2.0>

Szellemi Tulajdon Nemzeti Hivatala: *Puskás Tivadar* (1844–1893). Online: www.sztnh.gov.hu/hu/magyar-feltalalok-es-talalmanyaik/puskas-tivadar

The Ultimate Hosted Cloud PBX Solution. Online: <https://thevoicesolutions.com/cloud-pbx/>

Vertel Corporation: *Telecommunications management network (TMN)*. Online: www.hit.bme.hu/~jakab/edu/litr/TMN/tmn.pdf.

<http://el-gibbor.synthasite.com/my-assignments-2.php>

<https://how2do.org/how-to-update-the-pc-bios-uefi/>

https://hu.wikipedia.org/wiki/Alaplap#/media/F%C3%A1jl:VIA_Mini-ITX_Form_Factor_Comparison.jpg

www.3glteinfo.com/ims-volte-architecture/

www.drivereasy.com/knowledge/how-to-enter-bios-on-windows-10-windows-7/

www.indiamart.com/proddetail/laptop-motherboard-repairs-14273562288.html

www.researchgate.net/figure/Separation-of-responsibilities-in-cloud-models_fig4_290445671

Vákát

A számítástechnika nyújtotta előnyöket mindennapi életünkben szinte észre sem vesszük, természetesnek tartjuk. A számítógép egyszerre van jelen a munkánkban, és teret hódít otthonainkban is. A technika, technológia vívmányaival a bűnelkövetések eszköztára is bővült. Ma már nemcsak a kibertérbeli támadásokban, hanem a valós térben elkövetett, tradicionális bűncselekményekben is szerepet kapnak.

A számítástechnikai rendszerekben kezelt elektronikus adatok a bűncselekmények bizonyítékai, amelyek megszerzése, megváltoztathatatlanságuk biztosítása új eszközöket, új módszereket igényel. Ez azt jelenti a jogalkalmazók számára, hogy meg kell ismerkedniük az új típusú bűncselekményekkel, azok eszközeivel, az elektronikus adatok bizonyítékként való felhasználásával.

A több szerző által jegyzett kötetünk a kiber- és az informatikai nyomozók képzéséhez készült, de a téma iránt érdeklődők számára is hasznos ismereteket nyújt.



9 789635 316434