2018
7–8.

BELÜGYI SZEMLE

A BELÜGYMINISZTÉRIUM SZAKMAI, TUDOMÁNYOS FOLYÓIRATA

66.
évfolyam

TARTALOM 2018/7–8.

SZERZŐK 2018/7–8.

BENEDEK ZOLTÁN Pécsi Rendőrkapitányság

BOGDÁNY GYULA rendőr alezredes, osztályvezető-helyettes,
Bács-Kiskun Megyei Rendőr-főkapitányság
bűnügyi osztály

DR. CZÁR ZSANETT rendőr főhadnagy, főnyomozó,
Csongrád Megyei Rendőr-főkapitányság

FAZEKAS ISTVÁN főelőadó,
Készenléti Rendőrség Nemzeti Nyomozó Iroda
kiberbűnözés elleni főosztály forenzikus osztály

HALÁSZ VIKTOR rendőr főhadnagy, főnyomozó,
Készenléti Rendőrség Nemzeti Nyomozó Iroda
kiberbűnözés elleni főosztály nyomozó osztály

HERÉDI ISTVÁN rendőr hadnagy, nyomozó
Készenléti Rendőrség Nemzeti Nyomozó Iroda
kiberbűnözés elleni főosztály

GAÁL TIBOR c. rendőr alezredes, kiemelt főnyomozó,
Szabolcs-Szatmár-Bereg Megyei
Rendőr-főkapitányság

DR. MÁTÉ ISTVÁN ZSOLT PHD igazságügyi informatikai szakértő,
Nemzeti Szakértői és Kutatóközpont

MRÁZ ZOLTÁN rendőr alezredes, kiemelt főnyomozó,
ORFK Bűnügyi Főigazgatóság bűnügyi főosztály
bűnügyi osztály

DR. NAGY PÉTER egyetemi tanársegéd,
Károli Gáspár Református Egyetem
Állam- és Jogtudományi Kar

DR. NAGY RICHÁRD rendőr alezredes, osztályvezető,
ORFK Bűnügyi Főigazgatóság bűnügyi főosztály
korrupció és gazdasági bűnözés elleni osztály

DR. NAGY TAMÁS rendőr főtörzsőrmester, nyomozó,
Nemzeti Nyomozó Iroda
kiberbűnözés elleni főosztály nyomozó osztály

DR. RÁDI NORBERT rendőr ezredes, bűnügyi rendőrfőkapitány-helyettes,
Csongrád Megyei Rendőr-főkapitányság

DR. SZONGOTH RICHÁRD c. rendőr alezredes, nemzetközi főreferens,
Készenléti Rendőrség Nemzeti Nyomozó Iroda

VETTER DÁNIEL rendőr hadnagy, mb. alosztályvezető,
Készenléti Rendőrség Nemzeti Nyomozó Iroda
kiberbűnözés elleni főosztály felderítő osztály

SUMMARY

Szongoth, Richárd – Vetter, Dániel
International law enforcement cooperation in the field of cybercrime [7–21]
The essay provides an overview of the potential and institutional structure of international law enforcement cooperation in the field of cybercrime.

Gaál, Tibor
The increasing role of digital evidence in criminal procedure [22–35]
The author provides an overview of what digital evidence is and how it is used in criminal procedures in Hungary.

Máté, István Zsolt
Investigating attacks on IT-systems: the role of digital evidence [36–54]
The author provides a comparative overview of the role of computer forensic specialists in criminal proceedings.

Fazekas, István
AI research in forensic sciences [55–65]
The author shows how the emergence of new forms of cybercrime is caused by the artificially created cognitive entities, the narrow knowledge-based AI penetration. With this technology leap, cybercrime is transformed into a qualitative change that means a previously unheard of threat.

Nagy, Tamás
BEC – the bank transfer related fraud [66–82]
The author provides an overview of Business E-mail Compromise and the typical features of this fraud.

Nagy, Richárd
Investigating cyber related crime against property [83–95]
The author provides an overview of law enforcement responses to challenges of investigating cyber related crime against property.

Mráz, Zoltán
The role of digital evidence in investigating property crimes [96–105]
Focusing on traveling burglars with the exploitation of the IT environment's data acquisition, the author provides an overview of how IT tools are used in investigations.

SUMMARY

Herédi, István
Open source data collection on the Internet [106–116]
The author provides an overview of how open source data collection on the Internet can be used in investigation.

Halász, Viktor
How Bitcoin work and how it can be seized in criminal procedures [117–146]
The author provides an overview of how cryptocurrencies are used by criminals, and how seizing and storing can be managed in criminal investigations.

Benedek, Zoltán
Digital data at the crime scene [147–160]
The author provides an overview of the development and potential of digital data in criminal investigation.

Rádi, Norbert – Czár, Zsanett
The lesson from the Csengele-case [161–167]
The authors provide an overview of the investigation of a recent homicide case in Csengele,Hungary.

Bogdány, Gyula
Disrupting serial crimes and criminal gangs [168–180]
The author provides an overview of how digital technology can be sued in law enforcement.

DOI: 10.38146/BSZ.2018.7-8.1

SZONGOTH RICHÁRD – VETTER DÁNIEL

Nemzetközi bűnügyi együttműködés a kiberbűnözés területén

A nemzetközi bűnügyi együttműködés napjaink igen dinamikusan változó területe, hiszen a szolgáltatások más országból való elérésének, az állampolgárok más országokba való mozgásának megkönnyítésével kapcsolatos vívmányokat a bűnelkövetők is figyelemmel kísérik, és ki is használják. Megfigyelhető a bűnözés szervezettségének növekedése, a bűnözés határon átnyúló jellege, amely olykor kiemelten nehéz feladat elé állítja a rendvédelmi szervek munkatársait.

A kiberbűnözés utóbbi időben tapasztalt felfutása és egyre szerteágazóbbá válása megkívánta a speciális rendőri egységek közötti kapcsolat szorosabbra fűzését, a beszerzett információk más országgal történő megosztását. A többéves számítógépes bűnözési nyomozati tapasztalattal, valamint a nemzetközi bűnügyi együttműködésben jártassággal bíró szerzőpáros célja annak bemutatása, hogy a kiberbűnözés területén milyen együttműködési lehetőségek találhatók, és azok milyen módon képesek támogatni a kiberbűnözés elleni küzdelmet, a hazai eljárásokat. Terjedelmi okok miatt a tanulmányban azon nemzetközi szervezetek, kapcsolattartási formák kifejtésére kerül sor, amelyekkel kapcsolatban kézzelfogható, rendszeresen visszatérő tapasztalatok állnak rendelkezésre.

Az Europol-együttműködés

Az Europol

Az Europol az Európai Unió bűnüldöző hatósága, amely segíti a tagállamok bűnüldöző hatóságainak munkáját. Az Europolnak nincs önálló nyomozati jogköre, de központi szerepet játszik az Európa biztonságával foglalkozó uniós és nemzeti szervek között, ennek keretében bűncselekményekkel kapcsolatos információs csatornaként működik, és egyike a legnagyobb bűnüldözési elemzési kapacitással felruházott szervezeteknek.

A hazai rendvédelmi szervek napi rendszerességgel küldenek és fogadnak bűnügyi információkat az Europol biztonságos információcserét kiszolgáló hálózatán (SIENA rendszer), így segítve a gyors és hatékony adatcserét a nemzetközi szervezett bűnözés elleni küzdelem terén. Az „Europol-csatorna”

leginkább az uniós tagállamokkal, az európai országokkal, illetve az operatív szerződéssel bíró harmadik tagállamokkal (például Amerika, Kanada, Ausztrália stb.) folytatott bűnügyi információcsere terén aktív.

Az EC3 és az elemzői projektek

Az Europol kiberbűnözéssel foglalkozó szervezeti egysége az European Cybercrime Centre[1] (EC3 – Európai Kiberbűnözés Elleni Központ), amely 2013-ban kezdte meg működését. A központban a kiberbűnözés három fő területéhez – kibertámadások, gyermekek szexuális kizsákmányolása és készpénz-helyettesítő fizetési eszközökkel kapcsolatos bűncselekmények – kötődő munka úgynevezett elemzői projektek *(analyst project)* keretében valósul meg. A projektek működéséhez szükséges információkat alapvetően a tagállamok szolgáltatják a nyomozásaik során felvetődő adatok és információk megosztásán keresztül, amely adatok összesítése és elemzése történik az elemzői projekt keretén belül.

A Készenléti Rendőrség Nemzeti Nyomozó Irodán keresztül hazánk tagja mindhárom kiberbűnözéssel foglalkozó elemzői projektnek, így az AP CYBORG-nak (kiberbűncselekményekkel foglalkozó elemzőprojekt), az AP TWINS-nek (gyermekek szexuális kizsákmányolásával foglalkozó elemzőprojekt) és az AP TERMINAL-nak (készpénz-helyettesítő fizetési eszközökkel történő visszaélésekkel foglalkozó elemzőprojekt). Az elemzői projektek[2] célja az adott bűnügyi szakterületen végzett folyamatos, naprakész és a nyomozásokat ténylegesen segítő adatcserék és elemzések. (Az elemzőprojektek segítségével megvalósuló munka szorosan kötődik a későbbiekben bemutatandó EMPACT feladatrendszerhez is.) Az elemzői projektek gyakorlatilag egy közös felületet kínálnak az adott bűnügyi területhez kötődő információcsere egy mederbe tereléséhez, illetve az Europol szakemberei által az információk tematikus elemzésére.

Az AP CYBORG célja az Európai Unió területén működő informatikai hálózatok, kritikus infrastruktúrák ellen irányuló kibertámadásokkal kapcsolatos nyomozások támogatása, különös tekintettel a profitorientált szervezett bűnözői csoportok elleni fellépésre. Ennek keretében a rosszindulatú számítógépes programok, zsarolóvírusok, hackertevékenység mellett az adatlopás, a személyiséglopás és az internetes csalások elleni fellépésben is szerepet játszik.

1 https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
2 https://www.europol.europa.eu/crime-areas-trends/europol-analysis-projects

A kibertámadások fogalmi körébe elsődlegesen a különböző kártékony programok – így a zsarolóvírusok, kémprogramok –, a túlterheléses, úgynevezett DoS-, DDoS-támadások, az adathalászatok, a szerverek adatbázisait érintő adatlopási tevékenységek vagy a weboldalak felületeit megváltoztató, úgynevezett deface támadások, továbbá a folyamatosan, elnyújtottan, célzottan és összehangoltan, egy előre kiválasztott konkrét célpont ellen végrehajtott, úgynevezett ATP- *(Advanced Peristent Threat)* támadások tartoznak. Az egység a klasszikus elemzői és koordinációs feladatai mellett speciális malware-, illetve virtuális valutákkal kapcsolatos elemzési tevékenységet is végez. Az előbbieken túl forenzikus tevékenysége keretében helyszíni adatmentésekben, adattárakban való ellenőrzésekben tud segítséget nyújtani a tagállamok együttműködő rendvédelmi szervezetei számára.

Az AP CYBORG, igazodva az internetes bűnözés folyamatosan változó körülményeihez, valamint a tagállamok részéről felvetődő igényekhez, a szervezetét, továbbá az általuk nyújtott támogatások, szolgáltatások körét igyekszik folyamatosan fejleszteni, azokat innovatív megoldásokkal ellátni, így az elemzői projektektől elvárt, a beküldött adatok más ügyben való egyezőségének megállapításán és az egyedi ügyek mélyebb, több módszerrel, eszközzel való elemzésén túl a következő kapacitások jellemzik.

A napjainkban egyre nagyobb nehézséget jelentő káros számítógépes programok, úgynevezett malware-ek és azok közül is az Európában a legnagyobb fenyegetést jelentő zsarolóvírusok elleni küzdelem vonatkozásában kiemelendő a kifejezetten a kártékony programok elemzésére létrehozott Európai malware-elemző rendszer *(European Malware Analyst System; EMAS),* amely jelentős segítséget tud nyújtani a tagállamok számára. A 2013 óta működő és folyamatosan fejlesztett, úgynevezett sandbox technológiára épülő rendszerbe a további vizsgálatok elvégzése érdekében a rendvédelmi szervek elektronikus úton feltölthetik az ügyekben felkutatott malware-mintázatokat, valamint az azokkal összefüggésben keletkezett adatokat, majd az egység az általa megállapítottakat részletes jelentésben küldi vissza az azt kérőnek. A készített jelentés választ adhat az adott kártékony program malware-családjáról, a kiforduló IP-címekről, az úgynevezett *command and control* szerverekről, valamint a kód lefutásáról.

Az utóbbi években egyre nagyobb népszerűségnek örvendő virtuális valuták a legális tevékenységeken túl a bűnözői körök által végrehajtott műveletekben is igen nagy szerepet játszanak, így a specializált kiberbűnözés elleni egységek is egyre érdeklődőbbé váltak a terület iránt. Az AP CYBORG az online elérhető adatbázisok és az elemzőszoftverek együttes alkalmazásával

hatékonyan képes támogatni a tagállami nyomozásokat. A részükre megküldött, virtuális fizetőeszközöket tartalmazó pénztárcák, úgynevezett *wallet*ek vizsgálata során elvégzik a hozzájuk kapcsolható, azzal összefüggésbe hozható további tárcák felderítését, valamint automatikusan ellenőrzést végeznek az Europol nyilvántartásában annak megállapítása érdekében, hogy az elemzésre megküldött egyedi azonosító nem szerepelt-e a korábbi eljárásokban. Az esetleges találatokról, valamint az elvégzett vizsgálatról jelentést készítenek, amelyet továbbítanak a megkereső félnek. Fontos megjegyezni, hogy a rendszerek segítségével összeállított anyagok a büntetőeljárások során bizonyítékként felhasználhatók, valamint a common law jogrendszer követelményeit figyelembe véve megállapításaikról az egység szakemberei szükség esetén az eljáró bíróság előtt is beszámolnak.

Az elemzői projekt feladatai évről évre bővülnek, ezt jól szemlélteti, hogy 2016-ban 4221 jelzést kellett feldolgozniuk, amelyből 107 egyezőségi, 32 operatív elemzői jelentést készítettek, továbbá 52 műveletben vettek részt, míg 2017-ben már 4254 feladatot dolgoztak fel, amelyből 108 egyezőségi, 52 operatív elemzői beszámolót készítettek, valamint 82 művelet támogatását látták el.

Az AP TWINS a gyermekek szexuális kizsákmányolásához és bántalmazásához kötődő valamennyi online és offline cselekmény elleni küzdelmet és bűnmegelőzési tevékenységet támogatja. Ez felöleli a gyermekek szexuális kizsákmányolását ábrázoló felvételek készítése, terjesztése, kereskedelme elleni fellépést, de a szorosan kapcsolódó úgynevezett *grooming* vagy beszervezési tevékenység, a szexuális zsarolás, az élőképes bántalmazás és az utazó szexuális bűnözők elleni küzdelmet is.

A projekten keresztül megvalósuló információcsere és az elemzések segítségével a tagállamok és az Europol a gyermekek szexuális kizsákmányolásáról készített felvételek klasszikus megosztási platformjai (például „Peer to Peer" fájlcserélés) mellett az újabb típusú platformok (például darknet piacterek, online chatszobák stb.) elleni fellépést is igyekszik hatékonyabbá tenni.

Az új típusú bűnelkövetési formák, mint a szexuális zsarolás és a beszervezés, olyan próbatételek elé állítják a rendvédelmi szerveket, amiket csak rendkívül gyors, rugalmas és áldozatközpontú nemzetközi együttműködéssel lehet teljesíteni. Akármelyik bűnelkövetési forma ellen küzdenek is a szakemberek, a legfontosabb cél mindig az áldozatok azonosítása és lehetséges megmentése, kimentése, ideális esetben a valós áldozattá válás megelőzése.

A projekt kiemelt kezdeményezése az áldozatazonosítást elősegítő Áldozatazonosítási Munkacsoport *(Victim Identification Task Force)* kezdeménye-

zés, amelynek keretében a részt vevő tagországok szakemberei évente több alkalommal, hosszabb, akár többhetes időszakig együtt, összehangolva igyekeznek elemezni az ismeretlen áldozatokat ábrázoló képfelvételeket az Europol központjában.

Ki kell emelni továbbá, hogy az elemzői projekten keresztül érkeznek az amerikai NCMEC-jelentések (*National Center for Missing & Exploited Children;* Eltűnt és kizsákmányolt gyermekek nemzetközi központja). A szervezet kormányzati felhatalmazás alapján, konkrét állami feladatokat hajt végre az Egyesült Államokban a gyermekvédelem területén. A hazánkat érintő jelentések az amerikai szolgáltatók (Microsoft, Google, Facebook stb.) által észlelt magyarországi kötődésű gyermekek online szexuális kizsákmányolásával kapcsolatos információkat tartalmazzák. A Magyarországra érkező, évi kb. ezerötszáz-kétezer jelentés elsődleges elemzését a Készenléti Rendőrség Nemzeti Nyomozó Iroda kiberbűnözés elleni főosztálya végzi, a jelentések alapján évente több tíz büntetőeljárás megindítására is sor kerül.

Az AP TERMINAL a készpénz-helyettesítő fizetési eszközökkel kapcsolatos nyomozások támogatását szolgálja. A tradicionális elkövetési módszerek (például bankkártyamásolás) mellett az új típusú elkövetési módszerekre (például ATM-hackelés) is fókuszál. A készpénz-helyettesítő fizetési eszközökhöz kapcsolódó adatokra és tranzakciókra vonatkozó elemzői tevékenység mellett a projekt célja a széles körű bűnmegelőzési tevékenység is.

Még mindig népszerű elkövetési formák a klasszikus bankkártya-hamisításhoz kötődő bűncselekmények, mint a bankkártyaadatok megszerzését célzó, ATM- és POS-terminálok elleni cselekmények, valamint a hamis bankkártyák elkészítése és felhasználása.

Emellett azonban az internetes vásárlás lehetőségeinek elterjedésével egyenes arányban növekedett az online vásárláshoz szükséges bankkártyaadatok megszerzését célzó adathalász és más csalárd jellegű tevékenységek száma. A megszerzett bankkártyaadatoknak óriási, jellemzően a darknethez kötődő piaca van, így akár több tízezer illegálisan megszerzett bankkártyaadatot is lehet vásárolni az illegális piactereken.

Az EC3 legújabb szervezeti átalakulásaként említhető, hogy a korábbi kezdeményezések eredményeként az idei évtől megkezdi működését az Europol Darkweb Elleni Nyomozó Csoportja is, amely a kibertámadások, a gyermekek online szexuális kizsákmányolása, az online bankkártyás csalások, az emberkereskedelem és a hamisítások területén jártas szakemberekből, valamint a terrorelhárítás, a kábítószer- és a fegyverkereskedelem terén tapasztalt elemzőkből fog állni. A csoport a legnagyobb támogatást az évente

megrendezendő CyberPatrol elnevezésű, a darkneten elérhető illegális tartalmak és szolgáltatások célzott felderítését szolgáló EMPACT-műveletben fogja nyújtani. A csoport célja a darkneten üzemelő illegális piactereken megvalósuló, az említett bűnügyi területekhez kötődő rendvédelmi fellépés fokozása.

Európai kiberbűnözés elleni akciócsoport

Az elemzői projektekhez szorosan kapcsolódik az Europol-tagállamok kiberbűnözés elleni szakegységek vezetőit tömörítő, stratégiai tervezési, véleményezési és tanácsadási feladatokat ellátó Európai kiberbűnözés elleni akciócsoport *(European Cybercrime Task Force; EUCTF),* amelyben a Készenléti Rendőrség Nemzeti Nyomozó Iroda képviseli hazánkat. Az akciócsoport ülésein az önálló kezdeményezések mellett az elemzői projektek keretében keletkezett információk, feladatok megvitatása és a későbbiekben bemutatandó EMPACT-együttműködés támogatása is fontos szerepet játszik.

Europol számítástechnikai bűnözés elleni közös akció-munkacsoport

Szintén ki kell emelni a 2014 szeptemberében alakult, a kiberbűnözéssel kapcsolatos EMPACT-prioritások műveleti karjának is tekinthető számítástechnikai bűnözés elleni közös akció-munkacsoportot (J-CAT). Tagjai a tagállamok, valamint az Europollal operatív együttműködési megállapodást kötő országok rendvédelmi szervei által kifejezetten ebbe az egységbe delegált, kiberbűnözés területén jártas összekötő tisztjei, akik az EC3 szakmai iránymutatása mellett támogatják az országaik által folytatott, továbbá az országaikat érintő nyomozásokat, továbbá az Europol által legfontosabbként kezelt műveleteket. A korábban két évre alapított, majd két évvel meghosszabbított munkacsoport működése azóta állandó mandátumot kapott, valamint az abban részt vevő tagállamok mellett lehetőség van a munkacsoporthoz egy adott időszakra, kifejezetten egy adott ügy vagy ügyek megoldásának időtartamára csatlakozni. A munkacsoport felállítása óta először 2017 novemberében két hét időtartamra, négy nyomozás támogatására, EMPACT-finanszírozásból Románia delegált egy szakértőt, aki a J-CAT-tagokkal együttműködve hatékonyan tudta támogatni a folyamatban lévő eljárásokat.

A munkacsoport pozitívumai közé tartozik, hogy az egységbe delegált tagállami összekötők egymáshoz közeli irodákban látják el feladataikat, így az információk megosztása, valamint az informális csatornák kialakítása a

leghatékonyabban megoldható. Az egység 2015-ben nyolc, 2016-ban húsz, míg 2017-ben negyvenegy műveletet támogatott a napi szintű – a tagállami összekötő irodákat érintő és azokat az ebbe a csoportba delegált összekötő révén tehermentesítő – megkeresések, adatkérések, koordinációs feladatok elvégzése mellett, továbbá tavaly már két közös nyomozó csoportban is feladatokat vállalt.

Az Europol nemzeti összekötő irodák szerepe

Az Europol szervezetében a saját alkalmazásában lévő szakemberek, elemzők és egyéb munkakört ellátó szakértők mellett megtalálhatók a tagállamok és az Europollal operatív együttműködési megállapodást kötő országok összekötő irodái is, amelyek a feladatkörük alapján ellátják a nemzetközi bűnügyi együttműködésből rájuk delegált tevékenységeket, valamint képviselik hazájukat a különböző országok, szervezetek, intézmények előtt. Magyarország vonatkozásában az ORFK Nemzetközi Bűnügyi Együttműködési Központ szervezeti elemeként az Europol Magyar Összekötő Iroda végzi és felügyeli a rendőri együttműködés keretében megvalósuló információcseréket, a megkeresések kiküldését, azok – a hazai nyilvántartások ellenőrzését, szükség esetén az eljárást folytató egységekkel való egyeztetést követő – megválaszolását. Fontos fejlesztés, hogy a biztonságos adatcserét lehetővé tevő, úgynevezett SIENA-hálózat kiépítése után jelenleg – az Europol által működtetett Európai Biztonságos Hálózat alkalmazásainak felhasználásával megvalósuló együttműködés és információcsere rendjéről szóló 23/2016. (IX. 15.) BM–NGM együttes utasítás végrehajtásáról szóló 25/2017. (VIII. 17.) ORFK utasításnak megfelelően – a hazánkban SIENA-végponttal bíró szervezeti egységek közvetlenül bekapcsolódtak a nemzetközi információcserébe, így gyakran már a hazai nyomozók készítik és fordítják a megkereséseket, és továbbítják vázlatként az összekötő irodának, ahol annak ellenőrzését és az esetleges hibák javítása, javíttatása után küldik el a címzetteknek.

A 23/2016. (IX. 15.) BM–NGM együttes utasításban foglaltak alapján – a megkeresések és a válasziratok tartalmi és formai színvonala miatt – több egység is teljes jogosultságot kapott, így a kiberbűnözés esetében a Készenléti Rendőrség Nemzeti Nyomozó Iroda kiberbűnözés elleni főosztály végponti felhasználói közvetlenül, az összekötő iroda érintése nélkül képesek akár a társszervekkel együttműködést folytatni.

Az összekötő iroda tehát az egyszerűbb megítélésű, az adattárakban való ellenőrzést követően, többletinformáció nélkül megválaszolható, részükre

megküldött megkereséseket önállóan – a szakmai relevanciától függően, esetleg a kiberbűnözés elleni főosztályt később tájékoztatva – megválaszolják, míg az összetettebb vagy egy konkrét ügyre vonatkozó adatkéréseket a főosztálynak a további intézkedések megtétele céljából megküldik.

Az összekötő iroda a napi szintű SIENA-üzenetek kezelésén túl kapcsolatot tart az EC3 és a J-CAT munkatársaival, valamint szükség esetén – amennyiben a hazai eljárást folytató szerv akadályoztatva van, vagy az idő rövidsége indokolja – részt vesznek az Europol vagy más tagállam által szervezett műveleti találkozókon, amelyeken az előzetes egyeztetések alapján képviselik a hazai érdekeket, majd pedig annak végeztével tájékoztatják az eljáró szerveket. Az összekötő iroda által ellátott további tevékenységként említhető, hogy ha egy kiemelt jelentőségű ügyben azonnal szükséges az információ beszerzése, akkor személyesen, közvetlenül veszik fel a kapcsolatot más országok összekötőivel, ezzel segítve a bűnfelderítési célok hatékony megvalósulását.

Interpol

A jelenleg 192 tagországot soraiban tudó lyoni székhelyű Interpol a kiberbűnözés elleni küzdelemben főként a harmadik országokkal való nemzetközi bűnügyi együttműködésben nyújt segítséget hazánknak.

Az Interpol a már jól ismert adatkérésekkel, személy- és tárgykörözésekkel, kiadatásokkal, eljárási jogsegélyekkel kapcsolatos feladatainak ellátása mellett az utóbbi időben kiemelt figyelmet fordít a terrorelhárítás és a klasszikus szervezett bűnözés területein kívül a kiberbűnözés elleni küzdelemre. A célkitűzés súlyát és a feladat fontosságát jelzi, hogy a szervezet 2015-ben megnyitotta a szingapúri globális innovációs komplexumát, amelynek fő feladata a tudomány és technológia területén kiemelt szakértelemmel bíró szervezetekkel együttműködve a kiberbűnözés mértékének visszaszorítása, az alkalmazható technológiák kifejlesztése, megosztása, valamint a rendvédelmi szervek munkatársainak képzése.

Az Interpolnál több olyan, a bűnügyi munkát, illetve a bűnmegelőzést támogató projekt van, amelyek nagyban segítik a tagállamok munkáját. A gyermekek sérelmére elkövetett szexuális kizsákmányolás területén kiemelendő az Interpol gyermekek sérelmére elkövetett szexuális bűncselekmények nemzetközi képi adatbázisa *(International Child Sexual Exploitation)*. A 2009 márciusában létrehozott adatbázishoz 49 országnak van hozzáférése, köztük a Ké-

szenléti Rendőrség Nemzeti Nyomozó Irodán keresztül hazánknak is. Az adatbázis több százezer képfelvételt tartalmaz, köztük több mint tízezer már azonosított gyermek áldozattal kapcsolatos felvételt. Az adatbázis fő célja az abba feltöltött, ismeretlen áldozatokat ábrázoló felvételekkel kapcsolatos elemzési tevékenység támogatása, ezzel az áldozatazonosítások és -megmentések számának növelése. A rendszer segítségével hazánkban az elmúlt években több sikeres áldozatazonosítás és gyanúsítotti felelősségre vonás is történt.

Itt kell megemlíteni az Interpol *Worst of List* kezdeményezését, a szervezet által karbantartott és rendszeresen frissített linkgyűjteményt, adatbázist, amely a nyílt interneten keresztül elérhető, a gyermekek szexuális kizsákmányolását ábrázoló felvételeket tartalmazó linkekre vonatkozik. Az adatbázis segítségével már akár közvetlenül az internetszolgáltatókon keresztül is elérhetetlenné lehet tenni ezeket a linkeket az internet-előfizetők számára, csökkentve ezzel a képfelvételeken szereplő gyermekek minden egyes megtekintéssel megvalósuló ismételt áldozattá válását. Hazánkban jelenleg folyamatban van az adatbázis alkalmazásának jogszabályi hátterét megteremtő egyeztetés az érintett állami, civil és gazdasági szereplők közreműködésével.

Természetesen az „Interpol-csatorna” a legfontosabb olyan információcserét elősegítő csatorna, amelyen keresztül hazánk jellemzően a nem európai uniós országokkal szükséges rendvédelmi információcserét bonyolítja le. A csatorna alkalmas konkrét bűnügyi információk, személyi adatok megosztására, illetve a rendőri együttműködés keretein belül megvalósítható, konkrét nyomozásokhoz köthető kérések továbbítására is az Interpol által üzemeltetett I–24/7 globális rendőri kommunikációs csatornán keresztül. Az Interpol Magyar Nemzeti Iroda az ORFK Nemzetközi Bűnügyi Együttműködési Központ keretein belül működik.

24/7 kiberbűnözés elleni kapcsolattartási pontok

Az úgynevezett 24/7 kapcsolattartási pontok lényege, hogy a hálózatban részt vevő országok folyamatos, nonstop ügyeleti rendszert működtetnek a megkeresések fogadása és kiküldése érdekében. Magyarországot érintően három azonos célt szolgáló, de alapvetően különböző eredetű 24/7 kiberbűnözés elleni kapcsolattartási pontról beszélhetünk.

Az első a 2004. évi LXXIX. törvénnyel kihirdetett, az Európa Tanács Budapesten, 2001. november 23-án kelt számítástechnikai bűnözésről szóló egyezményéhez (budapesti egyezmény vagy cybercrime egyezmény) kapcsolódó, az

Európa Tanács szervezete által karbantartott, úgynevezett COE 24/7 hálózat. Ennek a hálózatnak az egyezményhez csatlakozó államok a tagjai, jelenleg összesen 52 ország. Az európai országok között jellemzően ez a leggyakrabban alkalmazott sürgősségi csatorna.

A második a G7 együttműködési fórumhoz kapcsolódó, az Egyesült Államok igazságügyi minisztériuma által karbantartott úgynevezett G7 24/7 hálózat. Ennek 71 ország a tagja. A nem európai országok között jellemzően ez a leggyakrabban alkalmazott sürgősségi csatorna.

A harmadik lehetséges csatornaként természetesen meg kell említeni az Interpol-együttműködéshez köthető, az Interpol által üzemletetett úgynevezett I–24/7 globális rendőri kommunikációs csatornát. Ennek a hálózatnak az Interpol-tagországok a tagjai, több mint 190 állam.

Magyarország képviseletében az ORFK Nemzetközi Bűnügyi Együttműködési Központ a kijelölt 24/7-es kapcsolattartási pont valamennyi hálózatban, de a Készenléti Rendőrség Nemzeti Nyomozó Iroda kiberbűnözés elleni főosztálya is meg van jelölve valamennyi hálózatban mint kijelölt szakmai kapcsolattartási pont.

A 24/7 hálózatokon keresztül jellemzően olyan, a rendvédelmi együttműködéshez köthető megkeresések érkeznek, mint az elektronikus adatok megőrzésére vonatkozó kérelem, későbbi igazságügyi jogsegélykérelemhez kötődő kérdések, kérések, de akár késedelmet nem tűrő más, kiberbűnözéshez kötődő információk átadása is megvalósulhat, vagy halasztást nem tűrő, azonnali intézkedések végrehajtására vonatkozó kérések is érkezhetnek.

Gyakorlati példaként említhető meg a Készenléti Rendőrség Nemzeti Nyomozó Iroda kiberbűnözés elleni főosztályán folyamatban lévő nyomozás, amelynek keretében egy európai tagország területén található szerveren tárolt adatok soron kívüli megőrzésére, majd lefoglalására volt szükség annak érdekében, hogy ha a szabadlábon lévő, még el nem fogott elkövetők a szerver tartalmát esetleg távolról törölnék, az a későbbiekben rendelkezésre álljon. Az adatok megmaradása érdekében a COE 24/7 hálózaton keresztül megkeresés kiküldésére került sor az adott országba, amelynek a rendőri szervei néhány órán belül lehetővé tették a külföldi tárhelyszolgáltatón keresztül az adatok megőrzését, ezeket később európai nyomozási parancs megküldésével foglalták le.

Az EMPACT feladatrendszer

Hazánk az Készenléti Rendőrség Nemzeti Nyomozó Irodán, illetve a Nemzeti Adó- és Vámhivatalon keresztül tevékenyen részt vesz az Europol támogatása mellett folyamatban lévő EMPACT-munkában (*European Multidisciplinary Platform Against Criminal Threats;* Európai multidiszciplináris platform a bűnügyi fenyegetettség ellen). Az EMPACT egy olyan ad hoc menedzsmentkörnyezet, amely azért fejleszt ki egyes cselekvéseket, hogy elősegítse az előre meghatározott közös bűnügyi célok elérését.[3] A tagállamok, az EU ügynökségei és intézményei, a harmadik államok, valamint az állami és magánszervezetek olyan strukturált multidiszciplináris együttműködési platformja, amely a sürgősként meghatározott súlyos és szervezett nemzetközi bűncselekmények ellen küzd.

A munka lényegében az Európai Unió égisze alatt, a nemzetközi szervezett bűnözés elleni hatékony fellépés érdekében kialakított feladatrendszer, amelynek keretében több, különböző prioritást (például emberkereskedelem, szintetikus drogok, illegális bevándorlás, kiberbűnözés stb.) érintően végeznek közös munkát a kijelölt EMPACT nemzeti szakértők az Europol segítségével. A különböző bűnügyi területeken végzendő, összeurópai rendvédelmi tevékenység érdekében évente úgynevezett operatív akcióterveket *(Operational Action Plan; OAP)* hoznak létre, amelyek összehangolják az adott területen végrehajtandó feladatokat.

A feladatok rendkívül sokfélék lehetnek. A leggyakoribbak az összehangolt, közös akciók, akciónapok, végrehajtások megszervezése, amely valamennyi részt vevő tagországtól konkrét operatív felderítések és/vagy nyomozások lefolytatását, összehangolt házkutatások, elfogások végrehajtását várja. Emellett természetesen akár közös képzések és konferenciák megszervezése, bűnmegelőzési kampányok lefolytatása, kutatások kezdeményezése, civil partnerekkel történő együttműködések kialakítása is a feladatrendszer része lehet.

A rendőrséget érintő valamennyi prioritás területén a Készenléti Rendőrség Nemzeti Nyomozó Iroda képviseli Magyarországot. A kiberbűnözéshez kötődően a gyermekek szexuális bántalmazása/kizsákmányolása (child sexual exploitation/abuse EMPACT CYBER – CSA/CSE), az információs rendszerek elleni támadások (EMPACT CYBER AAIS; attacks against information systems), illetve készpénz-helyettesítő fizetési eszközökkel való visszaélés

---

3 Hegyaljai Mátyás: Az EMPACT mint rendészeti válasz az európai bűnözésre. In: Gaál Gyula – Hautzinger Zoltán (szerk.): Tanulmányok a „Biztonsági kockázatok – rendészeti válaszok” című tudományos konferenciáról. Pécs, 2014, 127–134. o. [Pécsi Határőr Tudományos Közlemények XV.]

(EMPACT Non-cash payment) munkacsoportokban folyik az összehangolt munka. Csak hogy érzékeltessük a munka jelentőségét és hasznosságát, néhány példa az egyes szakterületek által végrehajtott közös feladatokról az elmúlt évekből.

Kiváló példa a konkrét műveleti munka és a bűnmegelőzés összekapcsolására az EMPACT CYBER AAIS együttműködés keretében végrehajtott egyik közös akció, amelynek célja a közepesen felkészült, információs rendszerek elleni támadásokat végrehajtó, alapvetően fiatalabb bűnelkövetők felderítésére és elfogására irányuló nyomozások lefolytatása és az elkövetők elszámoltatása mellett egy olyan bűnmegelőzési kampány indítása volt, amely az informatikában jártas fiatalokat célozta.

Az akció keretében több olyan, jellemzően fiatalkorú vagy fiatal felnőtt elkövető beazonosítása és elfogása történt meg, akik weblapok elleni túlterheléses, vagy különböző, adatlopásokat megvalósító támadásokat hajtottak végre.

Az akcióhoz kapcsolódó, *Cyber Crime vs. Cyber Security: What will you choose?* (Kiberbűnözés vagy kiberbiztonság: Mit választasz?) elnevezésű kampány[4] arra biztatta a fiatalokat, hogy a kiberbűnözői életmód helyett a civil szférában, informatikai vállalatoknál vagy akár a kiberbűnözés ellen küzdő rendvédelmi szerveknél kamatoztassák a számítástechnikai tudásukat.

Az EMPACT Non-cash payment együttműködés keretében minden évben az éves feladatrendszer része, az úgynevezett Globális repülőtéri akciónapok *(Global Airport Action Days)* elnevezésű operatív akciósorozat, amelynek célja a lopott bankkártyaadatok felhasználásával vásárolt repülőjegyekkel kapcsolatos visszaélések elleni összehangolt fellépés. A 2017-ben[5] tizedik alkalommal megrendezett akcióban 61 ország – köztük hazánk – és 63 légitársaság vett részt, 226 repülőteret érintve világszerte. Az akciónak köszönhetően 298 gyanús tranzakció feltárására került sor, és 195 személyt számoltattak el. Az akciósorozat az európai tagországok egymás közötti együttműködése mellett remek példa a harmadik országokkal történő együttműködésre is.

A gyermekek online szexuális kizsákmányolása és bántalmazása elleni EMPACT-összefogás keretén belül talán a legtöbb a bűnmegelőzési jellegű feladat. Tisztán bűnmegelőzési jellegű, ám a témából fakadóan igen érzékeny területet érintő közös kampány volt a *Say No!* (Mondj nemet!) kampány,

4 https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/cyber-crime-vs-cyber-security-what-will-you-choose

5 https://www.europol.europa.eu/newsroom/news/195-individuals-detained-result-of-global-crack-down-airline-ticket-fraud

amelynek célja az online szexuális zsarolásokra történő figyelemfelhívás, illetve az áldozattá válás megelőzésének lehetőségei. A kampány keretében egy részletes ismertető anyag[6] elkészítése mellett grafikákkal és a részt vevő tagországok nyelvére – így magyarra is – lefordított kisfilmmel[7] igyekeztek a részt vevő rendvédelmi egységek felhívni a figyelmet a szexuális zsarolás veszélyeire.

Bilaterális együttműködések

A kétoldalú együttműködések a nemzetközi bűnügyi kooperáció igen jelentős szeletei, amelynek költségeit szükség esetén az Europol részben fedezi. Az ügynökség épületébe szervezett műveleti találkozók megtartásához szükséges utazási költségek lehívására két mód áll rendelkezésre, a kisebb összegű támogatások, illetve a nagyobb összegű támogatások rendszere. A legalább két tagállam részvételével megtartandó munkamegbeszélés költségeinek viselése kapcsán benyújtott kisebb összegű támogatások rendszerébe eső pályázat engedélyezése akár két hét alatt is megtörténhet, így a bűnmegelőzési, bűnfelderítési érdekek még inkább biztosíthatóvá válnak.

A kétoldalú együttműködést támogatja továbbá az Eurojust is, amely nagy súlyt fektet a kiemelt kibertámadások során rövid időn belül összeállítható JIT-megállapodás mintáinak megszerkesztésére. Megfigyelhető, hogy a rendelkezésre álló pénzügyi keret évről évre növekszik, valamint hogy 2017-ben az Eurojust összesen kétszáz JIT-et támogatott, amelyek közül 87 aláírására tavaly került sor.

A kiberbűnözés országhatárokon átnyúló jellege, valamint az elkövetői csoportok vegyes összetétele miatt a számítógépes bűnözés elleni egységek és így a Készenléti Rendőrség Nemzeti Nyomozó Iroda kiberbűnözés elleni főosztály napi munkavégzésében is hangsúlyos szerepet kap a más országok bűnüldöző hatóságaival való együttműködés, a megszerzett információk megosztása. Különösen intenzív és hatékony a főosztály együttműködése az Egyesült Államok szövetségi rendvédelmi szerveivel, így a Szövetségi Nyomozóirodával *(Federal Bureau of Investigation)* és a Belbiztonsági Nyomozó Irodával *(Homeland Security Investigation),* illetve a Német Szövetségi Bűnügyi Hivatallal *(Bundeskriminalamt).*

---

6 https://www.europol.europa.eu/publications-documents/online-sexual-coercion-and-extortion-form-of-crime-affecting-children-law-enforcement-perspective

7 https://www.youtube.com/watch?v=ufTgIJ2zKTE&feature=youtu.be

Pozitív példaként említhető, hogy hatóságunk az Egyesült Államok bevándorlási és vámhivatal belbiztonsági nyomozóegységének *(United States Immigration and Customs Enforcement Homeland Security Investigations)* bűnügyi jelzése alapján nyomozást rendelt el gyermekpornográfia bűntett gyanúja miatt, mivel a társszerv jelzése, illetve a nyomozás során beszerzett adatok szerint megalapozott gyanú merült fel arra, hogy az elkövetők egy olyan weboldalt üzemeltettek, amelyen keresztül az oda regisztráló, főleg külföldi személyek tömegesen osztottak meg tizennyolc évesnél fiatalabb személyekről készült, a nemiséget súlyosan szeméremsértő nyíltsággal ábrázoló fénykép- és videófelvételeket.

Az Egyesült Államok bevándorlási és vámhivatal bécsi regionális képviseletével *(United States Immigration and Customs Enforcement Regional Attaché Vienna, Austria),* illetve a belbiztonsági nyomozóegység charlestoni irodájával *(Homeland Security Investigations Charleston, South Carolina)* folytatott kiterjedt bűnügyi együttműködés következtében hatóságunk házkutatást tartott az elkövetők lakásaiban, majd az eljárás eredményes lefolytatása nyomán a két személy tekintetében az illetékes ügyészség vádemelési javaslatot tett gyermekpornográfia bűntettének elkövetése miatt.

További pozitív példa az Amerikai Egyesült Államok és Magyarország között elsőként megkötött közös nyomozó csoport felállításáról szóló megállapodás, amelynek célja egy a darkneten elérhető, főként kábítószereket és illegálisan megszerzett személyazonosító adatokat kínáló oldalt kiszolgáló szerverrel, valamint annak adminisztrátorával kapcsolatos minden lehetséges adat beszerzése, továbbá az érintett eszközökön tárolt adatok lefoglalása volt. A bevezetett nyomozati cselekmények után a Szövetségi Nyomozóiroda munkatársainak részvételével házkutatás keretében sor került az érintett szerveren tárolt adatok lefoglalására, majd az amerikai fél a nyomozása során korábban beszerzett adatok alapul vételével megkezdhette a kiszolgáló szerveren tárolt információk elemzését, vizsgálatát.

A bemutatott nemzetközi együttműködési lehetőségek alapján látható, hogy a rendvédelmi szervek elsőrendűként tekintenek a kiberbűnözés területére, valamint hogy egy adott ügy megoldása során a beszerezni kívánt adatok és más ország rendvédelmi szerveivel való közvetlen együttműködés szükségessége alapján mérlegelni kell az alkalmazható kommunikációs csatornákat, majd megválasztani az alkalmazandót.

Végezetül fontos megemlíteni az együttműködés normatív hátterét. A kiberbűnözés területén folytatott nemzetközi együttműködés jogszabályi alapjait a bűnüldöző szervek nemzetközi együttműködéséről szóló 2002. évi

LIV. törvény teremti meg, amelynek célja, hogy – a felderítés hatékonyságának növelése érdekében – szabályozza a magyar bűnüldöző szerveknek a bűnmegelőzés és a bűnüldözés során külföldi hatóságokkal folytatott együttműködését.

Az Európai Unió tagállamaival folytatott együttműködés területén kiemelt jelentőségű továbbá az Európai Unió tagállamaival folytatott bűnügyi együttműködésről szóló 2012. évi CLXXX. törvény, amelynek célja az uniós tagországok közötti együttműködés gyorsítása és egyszerűsítése.

Természetesen a büntetőeljárások során a nemzetközi bűnügyi jogsegélyről szóló 1996. évi XXXVIII. törvény rendelkezéseit is figyelembe kell venni az eljárási jogsegélyek kérése és végrehajtása során.

DOI: 10.38146/BSZ.2018.7-8.2

GAÁL TIBOR

A digitális bizonyítékok jelentőségének növekedése a büntetőeljárásokban

A technológia emberre, illetve társadalomra gyakorolt hatása folyamatosan tetten érhető mindennapi életünkben. Tehát nem az a kérdés, hat-e ránk, hanem az, hogy hogyan. A XX. század közepétől fokozott érdeklődés mutatkozik a társadalomtudományok részéről ennek vizsgálatára. A legismertebb tudományos műhely a Torontói Egyetemen jött létre és Torontói Iskola néven vált ismertté. Jelesebb képviselői *Harold Innis, Marshall McLuhan, Joshua Meyrowitz, Neil Postman* és még folytathatnánk a sort. Közülük Innis volt az első, aki felhívta a figyelmet a technika társadalomra gyakorolt hatásaira[1]. A hatás mibenléte még nem tisztázott ugyan, de az mindenképpen megállapítható, hogy a technológia és azon belül a digitális/elektronikus szolgáltatások és eszközök használata mélyen beivódott a mindennapjainkba.

Elfogadva tehát a hatás tényét kimondhatjuk, hogy ennek nyomai megtalálhatók akkor is, amikor büntetőeljárást folytatunk, szinte függetlenül az eljárást kiváltó cselekmény típusától. Ez azt jelenti, hogy a büntetőeljárást végző nyomozók olyan digitális/elektronikus nyomokra bukkanhatnak munkájuk során, amiknek a felhasználásával, helyes értelmezésével az adott ügy megoldásához juthatnak el. Azonban ez a folyamat nem olyan egyszerű, s ez egyben új ismeretek, készségek, képességek elsajátítását, s nem utolsósorban – a digitális/elektronikus nyomok bizonyítékként történő felhasználását biztosító – új eljárások alkalmazását igényli a nyomozó hatóságok tagjai és a nyomozó hatósággal együttműködő szakértők és szaktanácsadók részéről is.

1 A Torontói Iskola egyik előzményeként vagy szellemi forrásaként tekinthetünk *Hajnal István*ra (1892–1956). A Széchenyi-díjas magyar történész, egyetemi tanár, az MTA tagja, a történelemtudományok doktora írástörténeti és technikatörténeti munkáiban a technikai változásokat a történelem egyik fontos alakítójának tekintette. Továbbá http://okt.ektf.hu/data/nadasia/file/tananyag/informaciotortenelem/29_04/432_harold _innis.html

A digitális bizonyíték fogalma

Hazai jogszabályi háttér

Ahhoz, hogy a digitális nyomból hogyan válik digitális bizonyíték, pontosan ismernünk kell a digitális bizonyíték fogalmát. Azonban a jogszabályaink nem definiálják pontosan, mit értünk digitális bizonyítékon. Tehát más módon kell meghatározni a fogalmát.

Nézzük először, hogy a magyar jogban hogyan definiáljuk a bizonyíték fogalmát! A büntetőeljárásról szóló 1998. évi XIX. törvény a bizonyítás általános szabályai között határozza meg a bizonyítás eszközeit.

A bizonyítás eszközei a 76. § (1) bekezdésében szerepelnek: *„A bizonyítás eszközei a tanúvallomás, a szakvélemény,* a tárgyi bizonyítási eszköz, *az okirat és a terhelt vallomása.”*

A tárgyi bizonyítási eszközről a jogszabály 115. § (1) és (2) bekezdése a következőket rögzíti: *„115. § (1) Tárgyi bizonyítási eszköz minden olyan tárgy (dolog), amely a bizonyítandó tény bizonyítására alkalmas, így különösen az, amely a bűncselekmény elkövetésének vagy a bűncselekmény elkövetésével összefüggésben az elkövető nyomait hordozza, vagy a bűncselekmény elkövetése útján jött létre, amelyet a bűncselekmény elkövetéséhez eszközül használtak, vagy amelyre a bűncselekményt elkövették.*

(2) E törvény alkalmazásában tárgyi bizonyítási eszköz az irat, a rajz és minden olyan tárgy, amely műszaki, vegyi vagy más eljárással adatokat rögzít. Ahol e törvény iratról rendelkezik, ezen az adatot rögzítő tárgyat is érteni kell.”

A jogszabály szövege nem utal közvetlenül a digitális bizonyítékra, azonban minden olyan tárgy, amely *„… műszaki, vegyi vagy más eljárással adatokat rögzít…”,* a digitális bizonyíték meghatározásának közvetett definíciója lehet. A hangsúly az adatrögzítésen van.

A jogszabály a 149. § (1) bekezdésében megnevezi az „információs rendszer”-t, bár annak tartalmát nem definiálja.

„A házkutatás a ház, lakás, egyéb helyiség, az azokhoz tartozó bekerített hely vagy a jármű átkutatása, továbbá az ott elhelyezett információs rendszer vagy ilyen rendszerben tárolt adatokat tartalmazó adathordozó átvizsgálása az eljárás eredményessége érdekében.”

A 149. §-ban az adattárolási funkcióra helyeződik a hangsúly. Ez visszautal a tárgyi bizonyítási eszköznél írtakra, amely szerint az adatok rögzítése vagy rögzítettsége döntő motívum az ilyen jellegű bizonyítéktípus esetében.

A jogszabály azonban azt is kifejti, hogy a büntetőeljárásban csak olyan adatforrás, illetve törvényes adatforrás és adat képezhet bizonyítékot, amely büntetőjogilag releváns tényre vonatkozik.

Összegezve tehát elmondható, hogy a magyar szabályozás önállóan nem definiálja a digitális bizonyíték fogalmát, mindamellett biztos támpontként nevesíti az adatrögzítés mozzanatát, külön megemlítve az információs rendszert mint az adatrögzítési aktus eszközét.

Az új Be. a bizonyítás eszközeit a 165. §-ban sorolja fel.

„165. § A bizonyítás eszközei:

a) a tanúvallomás,

b) a terhelt vallomása,

c) a szakvélemény,

d) a pártfogó felügyelői vélemény,

e) a tárgyi bizonyítási eszköz, ideértve az iratot és az okiratot is, és

f) az elektronikus adat.”

Az f) pontban nevesített elektronikus adat pontosítását a jogszabály 205. §-ában találhatjuk meg.

„205. § (1) 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.

(2) Ahol e törvény tárgyi bizonyítási eszközt említ, azon e törvény eltérő rendelkezése hiányában az elektronikus adatot is érteni kell.”

Az új büntetőeljárási törvény egyes digitális bizonyítékként használható adatok beszerzését már ügyészi engedélyhez köti. Ilyen például az elektronikus hírközlési szolgáltatóktól származó adat [262. § (1) bekezdés c) pont]. Ezzel a jogalkotó érzékelteti, hogy ez egy olyan digitálisbizonyíték-forrás, amely szenzitív adatokat tartalmaz.

Kitekintés az Amerikai Egyesült Államok jogszabályi hátterére

Hasonlóan a magyar joghoz a szövetségi szabályozás csak általános kereteket fogalmaz meg[2].

2 https://www.rulesofevidence.org/article-i/rule-101/

„101. szabály – hatókör; meghatározások

(6) egy hivatkozás bármilyen írásos anyagra, vagy más hordozóra, beleértve az elektronikusan tárolt információt is.”[3]

Észrevehető, hogy a hangsúly az adatrögzítésre helyeződik, függetlenül attól, hogy azt milyen közvetítő eszközön tárolták. A szöveg csak utalást tesz az elektronikus tárolási formára, de a digitális bizonyíték kifejezést nem találjuk meg a jogszabály szövegében.

Az Amerikai Egyesült Államokban 1998-ban alakult meg a digitális bizonyítékokkal foglalkozó tudományos csoport *(Scientific Working Group on Digital Evidence; SWGDE)*. A csoport munkájának eredménye egy olyan szabványosítási folyamat, amely lehetővé teszi a digitális bizonyítékok egységes kezelését. A tudományos csoport szerint a digitális bizonyíték nem más, mint bizonyító erejű információk, amelyeket bináris formában tároltak, vagy továbbítottak[4].

Ebben a definícióban a hangsúlyt a bináris formában tárolt adatra helyezték. Nincs szó az adat tárolására szolgáló adathordozóról.

Azonban a szervezet nem feledkezik meg arról, hogy a digitális adat más, mint a legtöbb tárgyi bizonyíték, azaz legtöbbször nem kézzelfogható tárgyként van jelen, amelyet a nyomozó hatóság egyszerűen lefoglal, vagy egyéb korlátozó intézkedéssel gondoskodik eredeti állapotának megőrzéséről. A teljesség igénye nélkül elmondhatjuk, hogy a digitális bizonyíték korlátlan számban többszörözhető, méghozzá úgy, hogy közben nem változik a minősége. A digitális bizonyíték nem mindig található meg egyetlen fizikai helyen (például felhőalapú szolgáltatások). Az is előfordulhat, hogy a digitális bizonyíték nem egyben van, hanem darabokból állítható össze (például a merevlemezeken található kötetek egymástól elkülönülő könyvtáraiban tárolt részdokumentumok egymáshoz illesztésével). Ezek alapján a tudományos csoport más fogalmak bevezetését is indokoltnak tartotta, ilyen az eredeti digitális bizonyíték, a többszörözött digitális bizonyíték, vagy a másolat fogalma.

Egyéb amerikai szakirodalomban a digitális bizonyítékok másfajta jellegzetességére is felhívják a figyelmet. Ezek az osztályra és egyénre vonatkozó *(class characteristics, individual characteristics)* jellegzetességek[5]. Értelemszerűen az osztályjellemzők az információk csoportját vagy csoportjait, míg

3 Rule 101 – Scope; Definitions (6) a referencetoanykind of written material or any other medium includes electronically stored information.

4 Scientific Working Groupson Digital Evidence and Imaging Technology: SWGDE and SWGIT Digital & Multimedia Evidence Glossary. version: 2.7, SWGDE/SWGIT https://www.swgde.org/documents

5 Eoghan Casey: Digital Evidence and Computer Crime. Elsevier, Amsterdam, 2011

az egyénre vonatkozók magára az egyedre vonatkozó jellemzőket teszik a büntetőeljárásban definiálhatóvá. Utóbbi megközelítés rendszerszintű (adat és annak hordozója), míg az előbbi kizárólag adatorientált megközelítést mutat.

Utóbbi megközelítést példával szemléltetve egy papírra írógéppel készített dokumentum esetében a betűképzés módja az osztályjellemzőket (milyen írógéppel készült), míg annak a betűképzés során keletkezett hibái az írógép egyedi jellegzetességére utalhatnak (melyik írógéppel készült).

Ha ugyanez a dokumentum például Word szövegszerkesztővel készült dokumentumként áll rendelkezésre, akkor a dokumentumból kiolvasható, hogy milyen verziójú Worddel készült a dokumentum (osztályjelleg). Ha a dokumentumban egy olyan időpontra történik hivatkozás, amikor a dokumentum készítéséhez használt verzió még nem állt rendelkezésre (egyedi jelleg), akkor a dokumentum valódiságával kapcsolatban kétely ébredhet bennünk.

További példát tekintve egy adott hírközlési szolgáltató által hűségidővel eladott mobiltelefon a szolgáltató hálózatához van kötve (tehát nem hálózatfüggetlen), és hordozza annak összes tulajdonságait (osztálytulajdonság). Amikor egy szolgáltatást vesz igénybe a szolgáltató hálózatán, és kap például egy IP-címet, akkor már egyedi jellemzőket is hordoz, amelyek csak erre az egyetlen mobiltelefonra jellemzők (egyedi tulajdonság).

Casey a digitális bizonyítékokat három csoportba sorolja: számítógéprendszerek (szerverek, asztali és hordozható számítógépek és azok tartozékai), kommunikációs rendszerek (vezetékes telefon, wireless rendszerek, számítógépes hálózatok, internet stb.) és beágyazott számítógépes rendszerek (például GPS, mobiltelefon, videófelvevő stb.). Ezek a csoportok a gyakorlati tapasztalatokhoz jóval közelebb állnak, mint a digitális bizonyítékokkal foglalkozó tudományos csoport szervezet definíciói.

Összegezve elmondható, hogy a magyar jogszabályi háttér szinte megegyezik az amerikaival. Azonban a digitális bizonyíték kezelése, elemzése, vizsgálata tárgyában szinte semmilyen ajánlásunk, szabványunk nincs. Ez az idézi elő, hogy mind a nyomozó hatóságok, mind a szakértők, szaktanácsadók, vagy elemző-értékelők nehezen azonosítják, kezelik, vizsgálják, elemzik, értékelik a digitális bizonyítékokat. Ha megteszik azt – mivel különböző módszerekkel vizsgálódnak –, azok eredménye nehezen összehasonlítható. Az is elmondható, hogy a hatóságok alkalmazottai nem minden esetben vannak felkészülve a digitális bizonyítékok eljárásban történő felhasználására, illetve adott esetben megfelelő eszközeik sincsenek azok kezeléséhez.

A bűnjeltől a digitális bizonyítékig jutás folyamata

Természetesen a nyomozó hatóságok szakértőket és szaktanácsadókat, illetve szervezeten belül elemző-értékelőket vehetnek igénybe a digitális bizonyíték(ok) büntetőeljárásban történő sikeres felhasználásának érdekében. Azonban ehhez az említett szereplők sokkal szorosabb munkájára van szükség. A gyakorlatban jelenleg ez úgy zajlik, hogy a büntetőeljárásban azonosított lehetséges digitális bizonyítékot egy szakértő kirendelésével másolják le úgy, hogy annak eredetivel megegyezése bizonyítható legyen. Majd egy újabb szakértő (lehet a mentést elvégző is) kirendelésével, vagy egy elemző-értékelő felkérésével megkezdődhet az adatok elemzése, végezetül pedig következik az adatok értékelése. Az értékelés után döntés születik arról, hogy a lehetséges digitális bizonyíték törvényes digitális bizonyíték lehet-e. Ezt a döntést értelemszerűen a nyomozó hatóság, ügyészség, bíróság illetékese hozza meg.

Vizsgáljuk meg ezt a folyamatot lépésről lépésre! A büntetőeljárás során tehát a nyomozó hatóság munkáját az igazságügyi informatikai szakértő – ha tényállás megállapításához szakkérdés eldöntése szükséges (a Be. és a szakértői törvény alapján) –, vagy szaktanácsadó – a bizonyítási eszközök felkutatásának támogatása céljából (a Be. alapján) – segítheti.

Jellemzően tehát az informatikai szakértő vagy szaktanácsadó, esetleg elemző-értékelő – mint a nyomozó hatóság tagja, akinek speciális ismeretei vannak – a digitális bizonyítékok felkutatása, azonosítása során jut első körben szerephez, például házkutatáskor. A lefoglalás szabályairól szóló 11/2003. (V. 8.) IM–BM–PM együttes rendelet alapján a nyomozó hatóság lefoglalja azt a dolgot, *„… amely az eljárás során a bizonyítás eszközéül szolgál...”* A „dolog” azonosítása, kiválasztása a legnehezebb feladat, különösen azért, mert a releváns eszköz, nyom azonosítása egy összetett környezetben nem egyszerű feladat. A jogszabály imént idézett részében definiált bűnjel válik majd a bizonyítás során legtöbbször tárgyi bizonyítási eszközzé, digitális bizonyítékká.

A digitális bizonyítékok kezelésének alapelvei

A szakértőnek tehát bináris adatokat kell keresnie egy tárolón, vagy bináris adatok átvitelének folyamatát kell megfigyelnie, rögzítenie. Jellemzően az

adatra fókuszálunk, de annak tárgyi megjelenését is keressük (például merevlemez, vagy hálózati kapcsolóeszköz[6]).

A digitális bizonyíték felkutatása és azonosítása

A bináris formában tárolt vagy továbbított adatok digitális eszközökön való megjelenése nagy változatosságot mutat (például a gépkocsi nyitásához használt, indítókulcsba szerelt RF-ID chip, személygépkocsi fedélzeti számítógépe, vagy internetszolgáltató kiszolgáló szervere stb.). A példaként felsoroltak nemcsak megjelenésükben, de egyéb jellemzőikben is lényegesen eltérhetnek egymástól. Így ezek csoportosítása többféleképpen is elvégezhető lenne.

A már említett Casey által javasolt digitálisbizonyíték-csoportok, vagy a *Brinson és társai* által javasolt osztályozások[7] sem igazán nyújtanak segítséget a nyomozó hatóság munkatársai vagy a szakértők számára.

Valamilyen tagolást mégis alkalmazni kellene. Amennyiben visszatérünk a definíciókhoz, és a gyakorlati szempontokat figyelembe véve próbáljuk a tagolást elvégezni, akkor online és offline eszközökről beszélhetünk. Az online eszköz olyan, amely más eszközökkel kapcsolatban áll(hat). A kapcsolatai révén az aktuális adattartalma módosul(hat). Mivel az offline eszközök nem állnak más eszközökkel kapcsolatban, így az adattartalmuk statikusnak tekinthető. A *Matthew Braid*-féle csoportosítás a következőkben foglalható össze[8]:

1. processzor regiszter és gyorsítótár-tartalmak *(Registers and Cache);*
2. számítógépes hálózatiútvonal-választó útvonaltáblája *(Routing Tables);*
3. címfeloldási protokoll gyorsítótára *(Arp Cache)* (az IP-címek és a fizikai címek megfeleltető táblázata);
4. a feladatok végrehajtási táblázata *(Process Table);*
5. operációs rendszer rendszermag-statisztika és rendszermag-modulok tartalma *(Kernel Statistics and Modules);*
6. operatív tár tartalma *(Main Memory);*

---

6 LAN switch, WAN router, bridge, set-top-box, IPTV vevőegység, gépjármű fedélzeti számítógép, SIM-kártyák stb.

7 Nagy mérettartományba eső eszközök; kis mérettartományba eső eszközök; számítógépek, mint asztali számítógépek, laptopok, kiszolgáló gépek és táblaszámítógépek; tárolóeszközök, mint elektronikus tárak, digitális zenelejátszók, külső merevlemezek; bizonytalan besorolású eszközök, mint játékgépek, felvevőeszközök.

8 Matthew Braid: Collecting Electronic Evidence After a System Compromise. AusCERT, Brisbane, 2001

7. ideiglenes fájlrendszer tartalma *(Temporary File Systems);*
8. másodlagos memória tartalma *(Secondary Memory);*
9. útvonalválasztó eszközök beállításai *(Router Configuration);*
10. számítógépes hálózati topológia *(Network Topology).*

Braid javaslata szerint a bizonyítékok felkutatásának és azonosításának a sorrendje mindig az aktuális helyszínre vagy esetre vonatkozó egyedi változékonysági sorrenden kell hogy alapuljon. A kritikus eszközök vagy rendszerek kerüljenek előre, míg a kevéssé változékonyak, azaz kevéssé kritikus eszközök a végére.

A gyakorlatban leggyakrabban a következő eszközök lefoglalására kerül sor: kiszolgálógép (szerver), asztali gép, laptop, HDD, pendrive, DVD, memóriakártya, SIM-kártya, mobiltelefon, okostelevízió, GPS navigációs eszköz.

Ezek közül a legváltozékonyabb rendszer a kiszolgálógép (szerver), amely funkciójánál fogva a legtöbb digitális bizonyítékkal kecsegtethet. Azonban ennek tartalma valamilyen távoli hozzáféréssel (LAN, wifi, mobil hálózat stb.) könnyen manipulálható[9].

Jól érzékelhető, hogy a legváltozékonyabb rendszer ellentéte a megváltoztathatatlan adattartalmú adathordozó (CD, DVD-R, egyszer írható CD-ROM). Ezek megkeresése, azonosítása a nyomozás későbbi szakaszában sem okozhat problémát.

Online eszközök esetében a bevett gyakorlat, hogy az online eszközt offline eszközzé kell tenni, természetesen ezt csak megfelelő felhatalmazás birtokában teheti meg a nyomozó hatóság. Ha megszüntettük az online eszköz lehetséges kapcsolódásait, elkezdhető a vizsgálata. Ha a kapcsolatok nem szüntethetők meg teljeskörűen, akkor a vizsgálatkori állapotot mindenképpen rögzíteni kell.

Ez után szükséges az eszközök nyomozó hatóság és/vagy szakértő általi dokumentált azonosítása. Ez jellemzően a bűnjelcímkék használatával történik meg. Ezen jól olvashatóan fel kell tüntetni a bizonyíték sorszámát úgy, hogy azt ne lehessen eltávolítani. Ugyanilyen fontos, hogy fel legyen tüntetve a lefoglalás helyszíne, időpontja. Ha nincs az eszköznek egyedi azonosítója, akkor a nyomozó hatóság munkatársának és/vagy a szakértőnek kell alkalmaznia valamilyen egyedi azonosítást lehetővé tevő jelzést.

9 15000/390/2015. Bü. Szabolcs-Szatmár-Bereg MRFK Btk. 360. §-ban indult nyomozás során végrehajtott feladatok.

A digitális bizonyítékok összegyűjtése

A bizonyítékok összegyűjtése során az egyik legfontosabb az eredeti állapot megőrzése. Ez azért nagyon fontos, mert az e követelménynek megfelelés szavatolja, hogy a későbbiekben megakadályozhassunk mindenféle beavatkozást, illetve ekkor kell megkezdeni azt a dokumentálási folyamatot, amely végigköveti és felügyeli a bizonyíték kezelésének teljes folyamatát. Ennek segítségével dokumentálttá válik, hogy a bizonyíték mikor, hol és kinek a kezelésében volt, azzal mi történt, illetve történt-e az állapotában bármilyen változás.

Lényeges mozzanat a bűnjelek (később bizonyítékok) csomagolása. A bűnjelet olyan módon kell becsomagolni és megőrizni, hogy annak tartalma illetéktelen személy előtt rejtve maradjon. Ez kétféle követelményt jelent. Egyrészt csomagolóanyagként olyan eszközt, anyagot kell alkalmazni, amely a bűnjelet megóvja a károsodástól, s egyúttal azt is megakadályozza, hogy mérgezést, fertőzést stb. okozzon. Másrészt olyan csomagolóanyagot kell választani, amely nem átlátszó, illetve megóvja a bűnjelet a lehetséges károsodástól.

A gyakorlatban legtöbbször asztali számítógép, laptop, vagy ezeknél kisebb eszközök lefoglalására kerül sor. A számítógépek csomagolására két módszert alkalmaznak. Az egyik legelterjedtebb a műanyag vagy papírzsák ragasztószalaggal körbetekerve. A másik a számítógép elő- és hátlapjának A4-es papírral történő fedése körberagasztva körcímkékkel. A körcímkéken szerepel a lefoglalást elszenvedő aláírása. Mind a két megoldás megfelel a jogszabályi előírásoknak, bár az első tartósabb lehet.

Felvetődik a kérdés, hogy például milyen csomagolásban foglalható le egy működő okostelefon, amelyről tudjuk, hogy PIN-kóddal védett, és a tulajdonosa a hatósággal nem működik együtt, tehát a kódot nem árulja el, illetve nincs mentőegységünk, hogy a pillanatnyi állapotát kimenthessük. Egy szemeteszsák széles ragasztóval körbetekerve nem látszik a legbiztosabb megoldásnak. A bekapcsolt állapotban lefoglalt telefon esetében gondoskodni kell arról, hogy az akkumulátora ne merüljön le addig, amíg vizsgálhatóvá, vagy menthetővé válik. Ehhez nagyobb teljesítményű akkumulátort kell a telefonhoz csatlakoztatni. Arról is gondoskodni kell továbbá, hogy online állapotából offline állapotba hozzuk és tartsuk annak érdekében, hogy annak tartalmát ne lehessen távolról megváltoztatni. Ehhez valamilyen árnyékolásra képes csomagolóanyagba, például alufóliába kell csomagolni a telefont és a csatlakoztatott akkumulátort. Ez után már jöhet a nem átlátszó műanyag vagy papírzsák

és a ragasztószalag. Természetesen a lefoglalást követően, ha lehet, azonnal szakértőhöz kell juttatni az eszközt, és annak tartalmát haladéktalanul ki kell menteni. A lefoglalás során nem árt, ha nemcsak a telefont foglaljuk le, hanem annak tartozékait is, legfőképpen a telefonhoz tartozó töltőt.

Alapesetben az eszközökben található akkumulátorokat ki kell szerelni, s azokat az eszközökkel együtt kell lefoglalni. Az alvó állapotban lefoglalt eszközök magukban hordozzák annak kockázatát, hogy azok például LAN-szkenneres módszerrel felderíthetők, és ennek következtében illetéktelenek felügyelete alá kerülhetnek.

A digitális bizonyítékokká váló bűnjelek esetében véleményünk szerint nem szükséges a nem átlátszó csomagolóanyag megkövetelése. Ennek oka, hogy a digitális bizonyítékká váló bűnjel más, mint egy okirati bizonyíték, vagy egyéb tárgyi bizonyítási eszköz, mert tartalma, amely bináris formában van tárolva, közvetítőeszköz, például egy másik számítógép nélkül nem figyelhető meg, és ezen az sem változtat, hogy a csomagolása átlátszó-e, vagy nem.

A nagyon kis méretű eszközök megtalálása, azonosítása még a lefoglalást elszenvedő személy együttműködése esetén is nehézséget okozat.

A digitális bizonyítékok szállítása

A házkutatás helyszínén felkutatott és azonosított, majd – szigorú dokumentálás mellett – összegyűjtött digitális bizonyítékokat bűnjelraktárba szállítják. A digitális bizonyíték ennél a fázisnál van a legjobban kitéve a sérülésnek, illetve a kis méretű bűnjelek fokozott figyelmet igényelnek. A kis méretű bűnjelek szállításához célszerű gyűjtőcsomagolást használni, amellyel megakadályozható mind a sérülés, mind az elvesztés, elkeveredés.

A szállításra és a bűnjelraktárba történő átadás tételes azonosítással kell hogy történjen.

A szállítás két tipikus útvonalon szokott megtörténni. Az egyik a házkutatás helyszíne és a nyomozó hatóság bűnjelraktára közötti mozgatás, míg a másik a bűnjelraktár és a szakértő telephelye vagy a hatóságnál dolgozó elemző-értékelő munkahelye közötti szállítás.

Utóbbi esetben a szakértő vagy az elemző-értékelő a bűnjelraktárból kiadással egyidejűleg el kell hogy végezze a tételes átvételt és a csomagolás sértetlenségének ellenőrzését. Ennek dokumentálása történhet egy közepes felbontási képességű (öt megapixel vagy ennél nagyobb) digitális fényképezőgéppel, de az átadás-átvétel teljes képi dokumentálása lenne a legjobb. Az

itt észlelt eltéréseket (például sérült eszköz, csomagolás sérülése stb.) a szakértő a szakvéleményében (ami bizonyítékként értékelendő), míg az elemző-értékelő az általa készített értékelőjelentésben szerepelteti (ez nem bizonyíték ugyan, de sok esetben elégségesnek tartják az ügyészségek, bíróságok).

A szállítás közben tilos felügyelet nélkül hagyni a szállított bűnjeleket!

A digitális bizonyítékok tárolása

A bűnjelraktárban történő tároláskor gondot okozhat, ha a lefoglaláskor elmulasztották megszüntetni az eszköz alvó állapotát, majd az akkumulátorát kiszerelni. Így előfordulhat, hogy a bűnjelraktárban csörögni kezd egy mobiltelefon, ami az egyéb gondokon túl azzal is jár, hogy ez esetben már nem garantálható a bizonyíték eredeti állapota.

A szakértőnél történő tárolás esetében a kiszerelt alkatrészek nagy száma (például HDD-k, CD-k, DVD-k stb.) okozhat keveredést, különösen akkor, ha párhuzamosan több ügyben is érintett eszközökről van szó. Így ezek azonosítása és nyomon követése nehézséget okozhat a szakértőknek, a sértetlenség és a változatlanul hagyás jogszabály által előírt követelményének azonban mindenképpen meg kell felelni.

A digitális bizonyítékok vizsgálata

A bizonyítékok vizsgálata jellemzően szakértőre, ritkábban a nyomozó hatóság elemző-értékelő munkatársára van bízva. Önmagában ez a szakasz jelentős része a büntetőeljárásnak, azon belül a bizonyítékok kezelésének.

Hosszan lehetne foglalkozni azzal az eszközrendszerrel, amelynek segítségével a szakértők, illetve a nyomozó hatóságok tagjai a digitális bizonyítékok vizsgálatát végzik, ettől azonban jelen írásban eltekintünk. A vizsgálattal kapcsolatos követelményeket csak címszavakban soroljuk fel. A vizsgálatot jellemzően az eredeti digitális bizonyíték másolatán kell végezni, biztosítva ezzel az eredeti bizonyíték minimális használatát; kötelezően dokumentálni kell minden változást; a bizonyításhoz nélkülözhetetlen szabályokat be kell tartani; tilos olyan dolgot vizsgálni, amelyre a vizsgálatot végző tudása nem terjed ki.

A digitális bizonyítékok vizsgálatát és belőlük digitális bizonyítékok szerzését jellemzően szakértők kirendelésével oldják meg a nyomozó hatóságok.

Ritkábban alkalmaznak erre a célra elemző-értékelő munkatársat. Ennek oka, hogy nem minden nyomozó hatóságnál vannak meg azok az eszközök, amelyekkel a digitális bizonyítékok az előírásoknak megfelelően vizsgálhatók lennének, továbbá nem minden nyomozó hatóságnál áll rendelkezésre olyan elemző-értékelő munkatárs, aki végzettségénél és képzettségénél fogva végezheti ezt a tevékenységet. Ezért a jelenlegi gyakorlat szerint az elemző-értékelő munkatársak a szakértők által megszerzett digitális bizonyítékok értelmezésénél és a konkrét ügyben történő felhasználhatóság eldöntésénél kapnak nagyobb szerepet.

A digitális bizonyíték vizsgálatának végeztével a szakértő vagy az elemző-értékelő munkatárs mind a bűnjeleket, mind az azokból megszerzett digitális bizonyítékokat átadja a kirendelőnek.

Nincs olyan norma, vagy ajánlás, hogy mi történjen a szakértő vagy az elemző-értékelő munkatárs számítógépén található digitális bizonyítékokkal. A gyakorlat azt mutatja, hogy a szakértők egy része töröl mindent, míg a másik része nem. Az utóbbi egy sor kérdést vet fel, például meddig őrizhető meg a tárolt digitális bizonyíték, ki viseli a tárolás költségeit, stb.

A nem egységes gyakorlat bizonytalanságát egyértelműsítené egy norma vagy ajánlás.

A digitális bizonyítékok elemzése

A digitális bizonyítékok megszerzése után – jelen gyakorlat alapján – jellemzően a szakértő átadja a bizonyítékokat a nyomozó hatóságnak. Ezt követően az esetek egy részében az ügygazdák, egy másik részében az elemző-értékelő munkatársak elemzik és értékelik a megszerzett digitális bizonyíték és a konkrét ügy kapcsolatát.

Ha a nyomozó hatóság érintett tagjainak nincs meg a megszerzett digitális bizonyíték értelmezéséhez szükséges szaktudásuk, akkor szintén sor kerülhet igazságügyi szakértő bevonására.

Az e folyamatban részt vevő igazságügyi szakértő, vagy az elemző-értékelő munkatárs szorosan együtt kell hogy működjön az ügy előadójával.

Azonban nem szabad elfeledkeznünk arról, hogy a digitális bizonyítékok nyomozó hatóság munkatársai által történő vizsgálata függ néhány alapvető tényezőtől. Az egyik ilyen a nyomozó hatóság munkatársainak informatikai felkészültsége, tudása. A másik a rendelkezésükre álló eszközök milyensége, míg a harmadik a vizsgálandó bizonyítékok mennyisége. Itt gondolnunk kell

az első és a második tényezőre, mégpedig arra, hogy az elemzés elvégzéséhez van-e megfelelő eszköz a nyomozó hatóság birtokában, illetve van-e megfelelő kompetenciával felruházott személy, aki az elemzést képes elvégezni. Ha több elemző-értékelő munkatárs igénybevételére van szükség, akkor utóbbi két tényező halmozottan jelentkezik, mégpedig: rendelkezésre áll-e több megfelelő eszköz, illetve minden elemző-értékelőnek, akinek a részvételét tervezik az elemzésben, van-e szükséges kompetenciája.

A rendőrségen több fejlesztés is történt az utóbbi években, így rendelkezésre állnak olyan eszközök és alkalmazások, amelyek szükségesek az elemzésekhez, sok mérnök, mérnök-informatikus, informatikus végzettségű elemző-értékelő munkatárs dolgozik már a nyomozó hatóságoknál, de ez mégsem mondható általánosnak. Azoknál a szervezeti egységeknél, amelyeknél egyik tényező esetében sem állnak rendelkezésre megfelelő erőforrások, továbbra is egyetlen megoldás az igazságügyi szakértők bevonása az elemzésekbe.

Összegzés

Kijelenthető, hogy a digitális bizonyítékok szerepe – bizonyos ügytípusoknál különösen – egyre nagyobb mértékű. Ennek okán szükséges lenne a jogszabályi keretek és ajánlások pontosabb megfogalmazása, illetve a büntetőeljárásban részt vevők megfelelő szintű képzése és megfelelő eszközökkel való ellátása.

FELHASZNÁLT IRODALOM

Braid, Matthew: Collecting Electronic Evidence After a System Compromise. AusCERT, Brisbane, 2001

Brinson, Ashley – Robinson, Abigail – Rogers, Marcus: A cyber forensics ontology: Creating a new approach to studying cyber forensics. in digital investigation 3S (2006) S37 – S43, Amsterdam, 2006. http://www.dfrws.org/2006/proceedings/5-Brinson.pdf

Casey, Eoghan: Digital Evidence and Computer Crime. Elsevier, Amsterdam, 2011

Kunos Imre: Bűnelemzés. Tanfolyami jegyzet. ORFK, Budapest, 1997

Máté István Zsolt: A multimédia technológiák kulturális hatásai. PTE BTK Kommunikáció és Médiatudományi Tanszék, Pécs, 2012

Máté István Zsolt: A digitális bűnfelderítés gyakorlata, avagy az igazságügyi informatikai szakértő a büntetőeljárásban. In: **Gaál Gyula – Hautzinger Zoltán (szerk.):** Tanulmányok „A változó rendészet aktuális kihívásai" című tudományos konferenciáról. Pécs, 2013 [Pécsi Határőr Tudományos Közlemények XIV.]

Máté István Zsolt: Az igazságügyi informatikai szakértő a büntetőeljárásban. Doktori értekezés. Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola, Pécs, 2017

Tremmel Flórián – Fenyvesi Csaba: Kriminalisztika tankönyv és atlasz. Dialóg Campus, Budapest–Pécs, 2002

Tremmel Flórián: Bizonyítékok a büntetőeljárásban. Dialóg Campus. Budapest, 2012

JOGSZABÁLYOK

1978. évi IV. törvény a Büntető Törvénykönyvről

1998. évi XIX. törvény a büntetőeljárásról

13/2001. (X. 2.) ORFK Utasítás

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

9/2006. (II. 27.) IM rendelet az igazságügyi szakértői szakterületekről, valamint az azokhoz kapcsolódó képesítési és egyéb szakmai feltételekről

282/2007. (X. 26.) kormányrendelet a szakterületek ágazati követelményeiért felelős szervek kijelöléséről, valamint a meghatározott szakkérdésekben kizárólagosan eljáró és egyes szakterületeken szakvéleményt adó szervekről

31/2008. (XII. 31.) IRM rendelet az igazságügyi szakértői működésről

2012. évi C. törvény a Büntető Törvénykönyvről

2016. évi XXIX. törvény az igazságügyi szakértőkről

2017. évi XC. törvény a büntetőeljárásról

DOI: 10.38146/BSZ.2018.7-8.3

MÁTÉ ISTVÁN ZSOLT

Informatikai rendszerek elleni támadások szakértői vizsgálata – a digitális nyomok rögzítésének szerepe

Az igazságügyi informatikai szakértők munkájában az informatikai rendszerek elleni támadások vizsgálata az elmúlt tíz évben a kimutathatóság határán mozgott egy nem reprezentatív, de a trendeket vázoló empirikus kutatás adatai[1] szerint. A kutatás adatgyűjtési periódusa után gyűjtött információk arra utalnak, hogy az informatikai rendszereket érő támadások – amelyek a büntetőeljárás során szakértői vizsgálat hatókörébe is kerülnek – mértéke növekszik. Ez a tény nemcsak az igazságügyi informatikai szakértőket készteti a vizsgálati területükre vonatkozó módszerek és eljárások frissítésére és megújítására, hanem a nyomozó hatóságok munkatársait is új típusú – korábban nem tapasztalt – próbák elé állítja.

Jelen írásmű az alapfogalmi környezet tisztázása után esettanulmányok formájában mutatja be azokat a tevékenységeket, amelyek jelentősen befolyásolhatják az igazságügyi informatikai szakértői vizsgálat eredményességét. A tanulmány a tipikus problémák bemutatása mellett megoldási és továbblépési javaslatokat is megfogalmaz elsősorban amerikai egyesült államokbeli és ausztráliai példák és jó gyakorlatok felhasználásával.

Cybernetics – Cyberpunk – Cybercrime

Akár önállóan, akár szóösszetételben használva a kiber vagy cyber szó az informatikával, a számítógépes hálózatokkal, de legalábbis az elektronikus rendszerekkel kapcsolódik össze az olvasók gondolatvilágában. E kapcsolódást az ógörög κυβερνητης (kybernetes) szó jelentése alapozza meg, mely kormányzót, irányítót jelent, s e jelentéstartalommal került a komplex önszerveződő rendszerek matematikai leírásának címébe.[2] A nagy távolságú számí-

1 Máté István Zsolt: Az igazságügyi informatikai szakértő a büntetőeljárásban. PhD-értekezés. Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola, Pécs, 2017, 33–40. o.

2 Norbert Wiener: Cybernetics. Or Control and Communication in the Animal and the Machine. Hermann & Cie, Paris, Cambridge, Massachusetts, 1948

tógép-hálózatok kialakulásával közel egy időben a fogalom rövid művészeti kitérő után – amely érintette a képzőművészetet[3] és az irodalmat[4] egyaránt – a múlt század kilencvenes éveitől kezdődően került jelenlegi értelmezési tartományába: nevezetesen a globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerekkel[5] kapcsolatos fogalomkörbe.

Amint a GoogleBooks rendszer Ngram Viewer szolgáltatása segítségével lekérhető adatokból[6] is kitűnik, a cyber szó használta a GoogleBooks angol nyelvű szövegkorpuszában az előző évezred végén dinamikus növekedést mutatott, ez egyben arra is utal, hogy a fogalom szerteágazóan kapcsolódott az emberi tevékenységekhez.

A megjelenő új szóösszetételek (legalább 457 kifejezés) közül a cybercrime (kiberbűncselekmény) fogalma kapcsolódik jelen tanulmány tárgyához: az informatikai közegben elkövetett és az informatikai rendszerre irányuló bűncselekmények szakértői vizsgálatához.

Kiberbűncselekmények

A kiberbűncselekmény fogalma az 1960-as években elkövetett első számítógépes rendszereket érintő csalások[7] után formálódott, jórészt párhuzamosan a számítógépes bűncselekmény *(computer crime)* fogalmával. Egységes tudományos meghatározás a mai napig sem jött létre, így a jelenségre a cselekménytípusok és -fajták felsorolásával hivatkoznak a szerzők.

A típusmeghatározás során a kiberbűncselekményeket jellemzően két nagy csoportba sorolják:

– közvetlenül a számítógépes rendszerre irányuló cselekmények; illetve

– azok a cselekmények, amelyekben a számítógépek a cselekmény részei.[8]

Az Interpol szóhasználatában az előbbi elkülönítés a következőképpen jelenik meg:

3 http://www.kunstkritikk.no/kommentar/the-reinvention-of-cyberspace/

4 Veronica Hollinger: Cybernetic deconstructions: Cyberpunk and postmodernism. Mosaic: A Journal for the Interdisciplinary Study of Literature, vol. 23, no. 2, 1990, pp. 29–44.

5 2013. évi L. törvény 1. § 22.

6 https://books.google.com/ngrams/graph?content=cyber&year_start=1940&year_end=2000 &corpus=15&smoothing=3&share=&direct_url=t1%3B%2Ccyber%3B%2Cc0

7 Thomas A. Johnson (ed.): Forensic Computer Crime Investigation. CRC Press, Boca Raton, 2005

8 https://www.acorn.gov.au/learn-about-cybercrime

– fejlett, vagy csúcstechnológiás kiberbűncselekmények *(advanced cyber-crime);* illetve
– kapcsolódó kiberbűncselekmények *(cyber-enabled crime).*[9]

A tudományos megközelítés árnyalja a bemutatott képet:

– számítógép-központú bűnözés *(computer centred crime)* esetén a célpont maga a számítógépes rendszer, hálózat, adattároló, vagy egyéb eszköz (például kereskedelmi weboldal tartalmának módosítása). Ez tekinthető egy új bűncselekménytípusnak is, amely új eszközrendszert használ (tudniillik a számítógépet);
– számítógéppel támogatott bűnözés *(computer assisted crime),* amikor is a számítógépet mint eszközt használja az elkövető a cselekmény során, amely „segíti" a tevékenységét, de nem feltétlenül szükséges hozzá (például gyermekpornográfia). Itt hagyományos bűncselekményekről beszélhetünk, új módszerek alkalmazása mellett;
– járulékos számítógépes bűnözés *(incidental computer crime),* amikor a számítógépes rendszer a bűncselekmény szempontjából mellékes, lényegében egy hagyományos eszköz kiváltását jelenti (például könyvelés számítógéppel, papíralapú dokumentáció helyett).[10]

Az egyes típusokon belüli elkülönítés a cselekmények tételes felsorolásával történhet, ezekre jellemző példát szolgáltat a már idézett kiberbűncselekmények ausztráliai online bejelentési hálózata *(Australian Cybercime Online Reporting Network; ACORN)* által alkalmazott elkülönítés:

1. Számítógépes rendszer elleni támadás
   a) illetéktelen hozzáférés, vagy a rendszer feltörése,
   b) kártékony kódok (vírusok, férgek, kémprogramok stb.),
   c) túlterheléses támadások;
2. Online zaklatás
   a) sértő üzenetek, képek és videók küldése,
   b) nem kívánt üzenetek küldése (spam),
   c) gyalázkodó üzenetek, vagy e-mailek küldése,
   d) online kirekesztés, vagy megfélemlítés,
   e) hamis közösségi hálózati profilok és sértő weboldalak létrehozása,
   f) rosszindulatú híresztelések online terjesztése,

---

9 https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

10 Ewa Huebner – Derek Bem – Oscar Bem: Computer Forensics – Past, Present And Future. University of Western Sydney, Sydney, 2007

g) a digitális kommunikáció bármely olyan formája, amely kirekesztő, megfélemlítő, szándékos fájdalom- vagy félelemkeltési célzatú;

3. Tiltott illegális tartalom közzététele
   a) gyermekek szexuális kizsákmányolására vonatkozó tartalmak,
   b) terrorszervezeteket vagy -cselekményeket támogató anyagok,
   c) gyűlöletkeltő tartalmak;
4. Gyermekek online zaklatásával kapcsolatos tartalmak
   a) gyermekpornográfiával összefüggő tartalmak birtoklása, terjesztése, gyártása, hirdetése vagy hozzáférés lehetővé tétele ezekhez,
   b) tizenhat év alatti[11] fiatalokkal szexuális tevékenység folytatása, vagy erre vonatkozó kommunikáció folytatása;
5. Személyiséglopás
   a) adathalászat,
   b) online hozzáférés megszerzése, feltörése,
   c) személyes adatok visszakeresése szociális médiából,
   d) üzleti adatokhoz történő engedély nélküli hozzáférés;
6. Online kereskedelemmel kapcsolatos ügyek
   a) online eladással kapcsolatos csalás (megvásárolt termék nem érkezik meg a vásárlóhoz),
   b) meghirdetettnél magasabb vételár kikényszerítése a vásárlótól,
   c) csodálatos gyógymód felkínálása,
   d) nem kért üzleti szolgáltatások terjesztése kisvállalkozások számára,
   e) adománygyűjtéses csalás jótékonysági szervezetek nevében;
7. Elektronikus levelezéssel kapcsolatos visszaélések
   a) kéretlen elektronikus levelek küldése,
   b) adathalászat;
8. Online csalás
   a) nyereményekkel kapcsolatos csalások,
   b) társkereséssel kapcsolatos csalások,
   c) fenyegetésekkel és zsarolással kapcsolatos esetek,
   d) munkalehetőséggel és befektetésekkel kapcsolatos csalások,
   e) személyiséglopás[12].

11 Ausztrál szabályozás szerinti életkor, lásd CRIMES ACT 1900 – SECT 55 Sexual intercourse with young person.
http://www8.austlii.edu.au/cgi-bin/viewdoc/au/legis/act/ consol_act/ ca190082/s55.html

12 https://www.acorn.gov.au/learn-about-cybercrime

Amint az a részletes felsorolásból is látszik, az egyes cselekményfajták között átfedés, azonosság is található, amely arra utal, hogy a vizsgált jelenség még nem ágyazódott be sem a büntetőjog, sem általában a társadalomtudományok fogalomkészletébe.

Mindamellett valamennyi felsorolt cselekmény közös vonásaként értékelhető az a tény, hogy kibertérben digitális nyomokat, digitális bizonyítékokat[13] hagynak maguk után, amelyek alkalmasak lehetnek a cselekmények részletes feltárására. Ezt a tevékenységet a nyomozó hatóságok kirendelése alapján az igazságügyi informatikai szakértők végzik, akik a *„a tudomány és a műszaki fejlődés eredményeinek felhasználásával”*[14] készített szakértői véleményükben foglalják össze az álláspontjukat. Tevékenységük megismeréséhez nélkülözhetetlen néhány alapfogalom – mint a digitális bizonyíték és kapcsolódó fogalmak – megismerése.

A digitális bizonyítékok

A digitális bizonyíték tételes meghatározása a digitális bizonyítékokkal foglalkozó amerikai tudományos társaságtól *(Scientific Working Group on Digital Evidence; SWGDE)* származik, e szerint: Bizonyító erejű információk, amelyeket bináris formában tároltak, vagy továbbítottak[15].

A definícióval csaknem szó szerint egyező szöveg került a digitális bizonyítékok azonosítására, összegyűjtésére, kinyerésére és megóvására vonatkozó nemzetközi szabvány szövegébe a következők szerint: Binárisan tárolt, vagy továbbított információ vagy adat, amelyre bizonyítékként lehet hivatkozni.[16]

Az előzőekben körülírt fogalom Magyarországon az új büntetőeljárási törvény révén került be a bizonyítás eszközei közé elektronikus adat elnevezéssel a következőképpen: *„Elektronikus adat a tények, információk vagy fogalmak minden olyan formában való megjelenése, amely információs rendszer*

13 A tanulmányban a digitális bizonyíték az angolszász *digital evidence* kifejezés értelmében szerepel, ez megfelel a magyar jogi szaknyelv bizonyítási eszköz fogalmának.

14 Az igazságügyi szakértőkről szóló 2016. évi XXIX. törvény 3. § (1) bek.

15 SWGDE/SWGIT Digital & Multimedia Evidence Glossary Version: 1.0 (July 25, 2005), p. 5. https://www.swgde.org/documents/Archived%20Documents/SWGDE-SWGIT%20Digital%20and%20Multimedia%20Evidence%20Glossary%20v1-0

16 ISO/IEC 27037:2012(E) Information technology – Security techniques – Guidelines for identification, collection, acquisition, and preservation of digital evidence. International Organization for Standardization, Geneva, 2012, p. 10.

általi feldolgozásra alkalmas, ideértve azon programot is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja."[17]

Ahhoz, hogy valamely számítógépes adat digitális bizonyítékká váljon, elsőként át kell hogy essen az azonosítás *(idetification)* folyamatán, amelynek során eldől, hogy a binárisan tárolt vagy továbbított információ vagy adat releváns-e a vizsgálat szempontjából[18]. Így válik a potenciális digitális bizonyítékból digitális bizonyíték.

A digitális bizonyítékok beszerzésének lehetőségei és módjai a korábbiakban felsorolt kiberbűncselekmények esetén jelentős eltérést mutathatnak: míg a helyi eszközökön megjelenő nyomokat a *computer forensics* hagyományos eszközeivel nyeri ki a szakértő, addig a számítógépes hálózatokban megjelenő potenciális digitális bizonyítékokat a *network forensics,* vagy *cloud forensics* eszközrendszerével kell azonosítania és értékelnie.

A *computer forensics* kissé leegyszerűsítve a szó szoros értelmében kézzelfogható adattárakból történő adatkinyerésen és adathelyreállításon alapul, míg a *network* és *cloud forensics* esetén a számítógépes hálózati forgalom egyes hozzáférhető adatainak elemzésével szerezhető meg a digitális bizonyíték. Mindezekhez járul még a potenciális digitális bizonyítékok változékonyságában mutatkozó különbség is: míg a *computer forensics* módszereivel vizsgált adatok kevésbé változékonyak, addig a *network* és *cloud forensics* módszereinek alkalmazásakor gyakran rendkívül tünékeny adatokkal kerül kapcsolatba a szakértő.

A következőkben a digitális bizonyítékok azonosításának, kinyerésének és elemzésének három különböző esetén keresztül kerül sor a tevékenységhez használt eszközök, szabványok és jó gyakorlatok egy-egy példájának bemutatására.

Online zaklatás szakértői vizsgálata – esettanulmány

A vizsgált esetben a nyomozó hatóság a büntető törvénykönyvről szóló 2012. évi C. törvény 222. § (1) bekezdésébe ütköző, és a (3) bekezdés a) pontja szerint minősülő házastárs volt házastárs, élettárs, volt élettárs sérelmére elkövetett zaklatás vétségének megalapozott gyanúja miatt ismeretlen tettes ellen

17 A büntetőeljárásról szóló 2017. évi XC. törvény 205. § (1) bek.

18 ISO/IEC 27042:2015(E) Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence. International Organization for Standardization, Geneva, 2015, p. 3.

induló büntetőügyben felmerülő informatikai szakkérdés megválaszolására rendelte el igazságügyi informatikai szakértői vizsgálat lefolytatását.

Ez az ügytípus a korábbiakban vázolt osztályozás szerint a számítógéppel támogatott bűnözés *(computer assisted crime)* körébe sorolható, hiszen a kérdéses esetben a zaklatás közege volt a kibertér, maga a cselekmény pedig „hagyományos" bűncselekmény.

Az ügyben lefoglalták a sértett és a terhelt hordozható számítógépét, valamint a terhelt megrongált állapotú okostelefonját.

A digitális eszközök esetén – amelyek a digitális adatok feldolgozására vagy tárolására használatos eszközök[19] – kiemelten fontos a dokumentálás. Ha a vizsgálat alá vont eszközök állapota (például sérülésmentessége) nincs megfelelően dokumentálva, akkor a későbbiekben felvetődhet – akár a nyomozó hatóság, akár a szakértő részéről – a szándékos vagy véletlen rongálás megtörténte. Ezért kiemelten fontos a potenciális digitális bizonyítékok (tudniillik digitális eszközök) összegyűjtésekor az állapot rögzítése, majd ennek az állapotnak az ismételt feljegyzése a keletkező dokumentumokban, így a szakértőt kirendelő határozatban is.

Az SWGDE sérült mobileszközök összegyűjtésének jó gyakorlatai című ajánlása[20] szerint a következő feladatok elvégzése és körülmények figyelembevétele szükséges:

- Mivel az eszköz áramellátása további károkat okozhat, nem szabad azt semmiféle áramforráshoz csatlakoztatni (akkumulátor, hálózati adapter).
- A fizikai sérülés nem feltétlenül jelenti a készülék üzemképtelenségét vagy az adat-helyreállítás meghiúsulását.
- A sérülés jellegét minden esetben dokumentálni kell, és arról tájékoztatni szükséges a vizsgálatot végző személyt.
- Bármilyen az eszköz fizikai megtisztítását célzó tevékenység előtt egyeztetni kell a műveletek sorrendjét (például DNS, nem látható nyomok kinyerése) a vizsgálatot végzőkkel.[21]

Az előbbiek mellett, a dokumentálás a digitális bizonyítékok értékelésénél is fontos szerepet kap, hiszen egy adott digitális nyom másként értékelendő akkor, ha a sértett, és másként, ha a terhelt digitális eszközén találja meg a szakértő.

---

19 ISO/IEC 27037:2012(E) i. m. 2. o.

20 SWGDE Best Practices for Collection of Damaged Mobile Devices, v1.1. 2016, p. 4. https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Collection%20of%20Damaged%20Mobile%20Devices

21 Az ajánlás további részletes útmutatást ad az egyes sérüléstípusok esetén követendő tevékenységekről.

Jelenleg a lefoglalt eszközök részletes és pontos dokumentálása nem ritkán hiányos – mint a vizsgált esetben is –, így a szakértői vizsgálat ezen adatok beszerzésével kell hogy elkezdődjön. A probléma kezelésére az SWGDE már idézett, illetve további elérhető ajánlásainak átvétele és/vagy adaptálása adhat megoldást.

Visszatérve a konkrét ügyre, az adott esettípus vizsgálata a hagyományos *computer forensics* eszközökkel történik, amelynek során a szakértő – dokumentált módon – eltávolítja az egyes készülékek tárolóeszközeit[22], majd írásblokkoló eszközön *(forensic write blocker)* keresztül megkezdi a vizsgálatot és a releváns adatok kinyerését *(aquisition)*.

A kinyerés során – amely a vizsgált eszköz adatkészletén belüli adat vagy adatok másolását jelenti[23] – teljes fizikai, vagy részleges logikai mentésre kerülhet sor. Előbbi olyan bitazonos mentés, amelynek során az eredeti tárolómédián található valamennyi adatterület bekerül egy lemezképállományba *(forensic image)*. Ez a lemezképállomány lesz a későbbiekben a részletes elemzés tárgya. A logikai kinyerés esetén célzott adatterületek – például egyes könyvtárak és/vagy fájlok – mentése történik meg.[24]

A vizsgált ügyben a zaklatás elektronikus levelezés útján történt, illetve felmerült Gmail- és Facebook-fiókokhoz történő illetéktelen hozzáférés, valamint billentyűzetleütést naplózó alkalmazás telepítése is, így a szakértői vizsgálat elsődlegesen ezekre a körülményekre koncentrált.

Mivel a szakértő a részletes vizsgálatot alapvetően az egyes eszközök bekapcsolása nélkül, írásvédelem alkalmazása mellett végzi, minden olyan körülmény feltárására sor kerül, amely az adott eszköz lefoglalásának időpontja és a szakértői vizsgálat megkezdésének ideje közötti adatmódosulásra utalhat. Ebből adódóan az eszközök nem dokumentált bekapcsolása a nyomozó hatóság munkatársa és/vagy az ügyész részéről a digitális bizonyíték hitelességét gyengítheti, vagy akár meg is semmisítheti.

Az ilyen beavatkozást az angolszász szakirodalom *tampering* (illetéktelen hozzáférés) néven ismeri, és tartalmát a már idézett ISO/IEC 27037:2012(E) szabvány 3.21 pontja rögzíti a következők szerint: *„Az illetéktelen hozzáférés a digitális bizonyíték módosítására vonatkozó szándékos cselekmény, vagy erre adott engedély.”*[25]

---

22 Mobil- és okostelefonok esetén a vizsgálati eljárás eltérő.

23 ISO/IEC 27037:2012(E) i. m. 2. o.

24 SWGDE Best Practices for Computer Forensic Acquisitions. v1.0. Scientific Working Group on Digital Evidence, 2018

25 ISO/IEC 27037:2012(E) i. m. 4. o.

Ezért fontos a potenciális digitális bizonyítékokkal közvetlenül kapcsolatba kerülő munkatársak felkészítése és továbbképzése, különösen annak tükrében, hogy egy friss felmérés szerint az informatikai eszközökkel kapcsolatos eljárásrendek ismerete – tehát a felhasználói szintnél magasabb hozzáértés – csak a megkérdezettek 3,4 százalékát jellemezte a saját megítélése szerint.[26]

A vizsgált esetben a részletes szakértői vizsgálat során a sértett hordozható számítógépén található operációs rendszer rendszerleíró adatbázisa *(registry)* elemzésével megállapítható volt, hogy a kérdéses eszközön billentyűzetleütés-megfigyelő program nem működött. A sértett és a terhelt közötti kommunikáció egyes elemeinek mentésével – mind a sértett, mind a terhelt számítógépéről – alátámasztható volt a cselekmény időbeli és tartalmi lefolyása. A böngészőprogramok (Google Chrome) és azonnali üzenetküldő programok (Skype) naplóadatai, valamint a kommunikációt dokumentáló képernyőképek és digitális fényképek metaadatai (létrehozó eszköz, dátum és idő, GPS-koordináták) révén a szakértői vizsgálat releváns adatokat tudott szolgáltatni a nyomozó hatóság elemző és értékelő tevékenységet végző munkatársainak.

A vizsgált ügyben és a hasonló ügytípusok esetén a kinyert adatok hagyományos átadási médiája az optikai adathordozó – jellemzően CD-R, DVD-R vagy DVD-R DL –, különösen jelentős adatmennyiség esetén pedig külső merevlemez (egy munkapéldány, egy biztonsági másolat).

A hasonló ügyekben szereplő digitális bizonyítékok mennyiségének növekedésével már a közeljövőben változtatni kell a szakértői vizsgálat során kinyert adatok átadási módján, hiszen több száz gigabyte-nyi adat kezelése optikai adathordozón már akadályozhatja a nyomozó hatóság értékelő- és elemzőmunkáját. A megoldást várhatóan a mágneses és/vagy elektronikus külső tárolók vagy a központosított biztonságos tárolást és elérést nyújtó bűnügyiadat-tárházak jelenthetik.

Információs rendszer elleni kibertámadás szakértői vizsgálata – esettanulmány

A következő esettanulmány átmenetet mutat a számítógép-központú bűnözés *(computer centred crime)* és a számítógéppel támogatott bűnözés *(computer assisted crime)* között. Ebből adódóan a szakértői vizsgálat eszközei részben a *computer forensics,* részben a *network forensics* eszközkészletéből származnak.

26 Simon Béla: A rendőrség állományának felkészültsége a kiberbűnözésre. Hadtudományi Szemle, 2018/1., 402–403. o.

A kérdéses ügyben a vidéki nagyváros rendőrkapitánysága a büntető törvénykönyvről szóló 2012. évi C. törvény 423. § (2) bekezdés b) pontjába ütköző, és a (2) bekezdés b) pontja szerint minősülő információs rendszer vagy adat megsértésének bűntette elkövetésének gyanúja miatt folytatott büntetőügyben rendelte el igazságügyi informatikai szakértő bevonását.

Az ügyben szereplő informatikai rendszer egy hálózatra csatolható tárolóegység *(Network Attached Storage; NAS)* volt, amely biztosította a sértett gazdasági társaság részére az alaptevékenységhez kötődő adatok központosított tárolását oly módon, hogy azok az internet irányából történő bejelentkezés után elérhetők legyenek a feljogosított munkatársak számára.

A NAS tároló a cselekmény feltételezett időpontjában elérhetetlenné vált a munkatársak részére, így a gazdasági társaság alaptevékenysége akadályoztatást szenvedett.

A kirendelő hatóság az ügy szakértői vizsgálatához a feltételezés szerint megtámadott informatikai rendszer naplóállományát küldte meg a szakértőnek (26 oldal terjedelemben, papír alapon, az eszköz tényleges azonosítása – értsd: gyártó és típusmegjelölés – nélkül), valamint a terhelt által használt hordozható számítógépet, amelynek lefoglalására a feltételezett kibertámadást követő 157. napon került sor. A szakértői vizsgálat a lefoglalást követő 19. napon kezdődött meg.

Az ügytípus jellemzője ebben az esetben az, hogy a feltételezett támadást elszenvedett rendszer (informatikai eszköz) rendelkezésre áll, így annak tartalma részletesen vizsgálható, amennyiben a nyomozó hatóság lefoglalja – erre a vizsgált esetben, a rendelkezésre álló adatok alapján nem került sor. Az eszköz rendszernaplójának a feltételezett támadás időszakára vonatkozó részét azonban lefoglalták, ez tartalmazta a feltételezett támadást megelőző tizenkét nap, valamint az utána következő egy nap rendszereseményeit.

A szakértői vizsgálat a rendszernaplót létrehozó eszköz beazonosításával kezdődött, amelyet a kirendelő hatóság munkatársa végzett el a sértett gazdasági társaságtól történő adatbekéréssel. A kérdéses eszköz D-Link gyártmányú DNS-320L modellszámú készülék. Az eszközre vonatkozó további fontos adat a készülék ismert sérülékenységeinek *(well known vulnerabilities)* megismerése (ha van ilyen). Az eszköz közvetlen vizsgálhatóságának hiányában a szakértő a releváns szakmai adatbázisokat – jelen esetben SecurityFocus Vulnerability Database[27] – vizsgálja át. Az adatbázis szerint – amely gyártói információkon alapult – a kérdéses eszközre jellemző volt egy úgynevezett tá-

27 https://www.securityfocus.com

voli parancsbejuttatási sérülékenység *(Remote Command Injection Vulnerability),* amely a feltételezett kibertámadás időpontja előtt három évvel már ismert volt, és a sérülékenység kiküszöbölésére vonatkozó javítócsomag is rendelkezésre állt.

Amint az jól látható, a megtámadott eszköz részletes dokumentálásának és lefoglalásának, vagy bitazonos mentésének hiánya nehezítette a készülék azonosítását, ebből adódóan a támadhatóságra vonatkozó szakértői megállapítások megalapozhatóságát, valamint azt is, hogy az adott készülékről eldönthető legyen, megvolt-e az ismert sérülékenysége, vagy nem.[28]

A feltételezés szerint megtámadott eszköz lefoglalásának hiányából adódóan a szakértő számára feltett egyik kérdésben megfogalmazódott az a feltételezés, miszerint a támadó a „TXT fájl küldésével az – sértett-gazdasági-társaság – Kft. – települési címén lévő szerverén lévő adatokat elérhetetlenné tette", megvizsgálhatatlanná vált (tudniillik a kérdéses állomány nem állt rendelkezésre).

A bemutatott problémákat a részletes dokumentálás mellett megoldhatja a szaktanácsadó igénybevétele:

„Az ügyészség, a nyomozó hatóság, illetve a rendőrség belső bűnmegelőzési és bűnfelderítési feladatokat ellátó szerve, valamint a rendőrség terrorizmust elhárító szerve szaktanácsadó közreműködését veheti igénybe, ha a bizonyítási eszközök felderítéséhez, felkutatásához, megszerzéséhez, összegyűjtéséhez vagy rögzítéséhez különleges szakismeret szükséges. A vádemelés után az ügyészség a bizonyítási indítvány megtétele, bizonyítási eszköz felkutatása és biztosítása érdekében vehet igénybe szaktanácsadót."[29]

Az angolszász gyakorlatban a szaktanácsadó feladatkörét a nyomozó hatóság munkatársa, a digitális bizonyítékok helyszíni vizsgálója *(Digital Evidence First Responder; DEFR)* végzi, aki *„képzettséggel és jogosultsággal rendelkezik arra vonatkozóan, hogy egy esemény helyszínén elsőként elvégezze a digitális bizonyítékok összegyűjtését és megszerzését"*[30]. Ugyanezt a tevékenységet az európai uniós Hálózat- és Információbiztonsági Ügynökség kiadványa elsősorban a számítógépes vészhelyzetkezelő csoportok *(computer emergency response team)* tagjainak munkaterületeként értelmezi, és részükre teszi közzé a jó gyakorlatokat összefoglaló kiadványait, amilyen az

28 A sérülékenységi adatbázis tartalmazta a készülékre vonatkozóan a sérülékeny és biztonságos működtetőprogramok verziószámait, ezek alapján a sérülékenység kihasználásának lehetősége valószínűsíthető vagy kizárható lett volna.

29 2017. évi XC. törvény 270. § (1) bek.

30 ISO/IEC 27037:2012(E) i. m. 2. o.

elektronikus bizonyítékok – alapvető segédlet azonnali beavatkozók részére *(Electronic evidence – a basic guide for First Responders*[31]*)*.

A hiteles képzési anyagok – forráshelyüktől függetlenül – javíthatják a kiberbűncselekmények szakértői vizsgálatát megalapozó információk minőségét, ezért az ajánlások és jó gyakorlatok magyar nyelvre és jogi környezetre történő adaptálása elkerülhetetlen lesz a közeljövőben.

A vizsgált esethez visszatérve: az alapadatok tisztázása után kerülhet sor a cselekmény körülményeit tartalmazó rendszernapló elemzésére. Az összesen 800 bejegyzést tartalmazó – elsőként papír alapon átadott, majd elektronikus formában is beszerzett – napló kinyerése a szakértő által nem ismert (vele nem közölt) körülmények között zajlott, így annak hitelessége, teljeskörűsége megkérdőjelezhető.

A hasonló helyzetek elkerülését oldhatja meg a korábbiakban bemutatott DEFR szerepkörnek megfelelően kiképzett munkatársak alkalmazása, akik a lehetséges digitális bizonyítékokra vonatkozó döntések és tevékenységek mellett fenntarthatnák a felügyeleti láncot is *(chain of custody)*. Utóbbi *„végigvonul a bizonyítékok kezelésének teljes életútján, mely alapján végig követhető marad, hogy mely időszakban hol, kinek a felügyelet alatt volt a bizonyíték, történt-e változás annak állapotában”*[32].

A rendszernapló bejegyzéseit a szakértő értelmezhetővé teszi az elemző- és értékelőmunkát végző szakemberek részére oly módon, hogy annak műszaki tartalmát és a hozzá fűzött magyarázatokat a rendelkezésükre bocsátja. A tárgyalt esetben az egyes rendszerfolyamatokhoz tartozó leírásokat – köztük kiemelten az energiaellátásra és a bejelentkezésre vonatkozó bejegyzéseket – lefordították, és megtörtént ezek részletes magyarázata például a következők szerint *(táblázat)*.

A működési körülmények mellett kiemelten fontos a külső bejelentkezések forrásának azonosítása, amely elsődlegesen az IP-címek alapján történik. A rendszernapló adataiból (automatizált folyamattal) kigyűjtött IP-címek szolgáltatóit *(Internet Service Provider; ISP)* és az IP-címekhez kapcsolódó geolokációs információkat az interneten elérhető tömeges lekérdezést lehetővé tevő adatbázisokból szerezheti meg a szakértő. A megkapott információkat a rendszernaplóval összefűzve könnyen értelmezhető és elemezhető adatsorok kerülhetnek a nyomozó hatóság munkatársaihoz, akik az adatsort a

---

31 Electronic evidence – a basic guide for First Responders, Good practice material for CERT first responders. European Union Agency for Network and Information Security, 2014

32 Máté István Zsolt: i. m. 100. o.

A rendszernapló bejegyzései

Bejegyzés tartalma	Magyarázat
mail_daemon: System Has Rebooted From A Power Failure.	Rendszer újraindulását követő hibaüzenet küldése: elektromos tápellátás hibája
rtc: System Time Is Updated By RTC.	A real-time-clock áramkör beállítja a rendszeridőt
fan_control: Set Fan Speed To “LOW”.	A ventilátorvezérlő ALACSONY sebességre kapcsolja a ventilátort
fan_control: Set Fan Speed To “HIGH”.	A ventilátorvezérlő MAGAS sebességre kapcsolja a ventilátort
fan_control: Set Fan Speed To “STOP”.	A ventilátorvezérlő LEÁLLÍTJA a ventilátort
fan_control: Set Fan-Control Mode To “Auto(Off/Low/High)”	A ventilátorvezérlő AUTOMATIKUS üzemmódba kapcsolja a ventilátorvezérlést
system_daemon: System is rebooted or power up successfully.	Rendszerüzenet: a rendszer újraindult, a bekapcsolás sikeres

hagyományos nyomozati eszközökkel összegyűjtött információkkal összevetve igazolhatják vagy cáfolhatják a terhelttel kapcsolatos feltételezéseiket. Ha a terhelt részéről rendelkezésre áll egy digitális eszköz – jelen esetben hordozható számítógép –, az adatok köre tovább bővíthető a hagyományos *computer forensics* eljárásaival kapott információkkal. Ez még akkor is jelentős lehet, ha – mint a vizsgált esetnél is – az adatkinyerés nem szolgáltatott további digitális bizonyítékokat, ugyanis a lefoglalt HP dv6-3107eg laptopon megtalált operációs rendszert a feltételezett kibertámadást követő 53. napon telepítették egy olyan adathordozóra (KINGSTON SHFS37A SSD), amely nem volt része az eredeti konfigurációnak. Ilyen és hasonló esetekben a szakértő jelezheti a nyomozó hatóság munkatársainak a tényt, miszerint a készülék eredeti adathordozóját lecserélték, és javaslatot tehet annak felkutatására.

Összefoglalva: a vizsgált ügyben összegyűjtött digitális bizonyítékok nem tették lehetővé a biztonsági esemény kategorikus azonosítását, ezért két valószínűsíthető eseménysor bemutatására került sor a szakértői véleményben:

1. A D-Link DNS-320L tárolórendszer firmware-ének sérülékenységét kihasználva 2017 (hónap, nap) 15.59:04-kor távoli parancsbejuttatás történhetett a tárolórendszer működtető rendszerébe, ez érinthette a jogosultságkezelési alrendszert is. A támadó a megszerzett jogosultságot felhasználva 2017 (hónap, nap) 18.48:56-kor adminfelhasználóként bejelentkezett, majd lekapcsolta a tárolórendszer áramellátását.
2. A D-Link DNS-320L tárolórendszer firmware-ének sérülékenységétől függetlenül több bejutási kísérlet is történt az eszközre különböző időpontok-

ban. Egyes esetekben sikertelen volt a megosztott könyvtárak felcsatolása az egyes regisztrált felhasználók részéről. A tárolórendszer működésének – a rendszernapló által rögzített – utolsó periódusában több alkalommal megtörtént elektromos tápellátás kiesése, amelynek következtében a tárolórendszer újraindult. A biztonsági esemény bekövetkezésekor 2017 (hónap, nap), vasárnap 18.49:39 után az újraindulás – ismeretlen okból – nem következett be. A tárolórendszer – szakértő feltevése szerint – a hétvégi időszakban nem volt közvetlenül fizikailag hozzáférhető az kft. irodája (a rendelkezésre álló adatok szerint irodaház található az adott címen), így a tárolórendszer áramellátása nem volt visszakapcsolható. Az áramellátás legkésőbb az esemény utáni napon 09.36:26-kor helyreállt.

Amint az jól látszik a bemutatott esettanulmány adataiból, a hatékonyságot növelhette volna a kirendelő hatóság vizsgálatának első szakaszában alkalmazandó szaktanácsadó, valamint a folyamatos dokumentálás és információátadás a szakértőnek.

Beékelődéses támadás szakértői vizsgálata – esettanulmány

A harmadik esettanulmány a kiberbűncselekmények egyik klasszikus változatát mutatja be: az informatikai rendszer elleni közvetlen támadást.

A kérdéses ügyben a vidéki kisváros rendőrkapitánysága a büntető törvénykönyvről szóló 2012. évi C. törvény 375. § (1) bekezdésébe ütköző, és az (1) bekezdése szerint minősülő információs rendszer felhasználásával elkövetett csalás bűntettének megalapozott gyanúja miatt ismeretlen tettes ellen induló büntetőügyben felmerülő informatikai szakkérdések megválaszolására rendelt ki igazságügyi informatikai szakértőt.

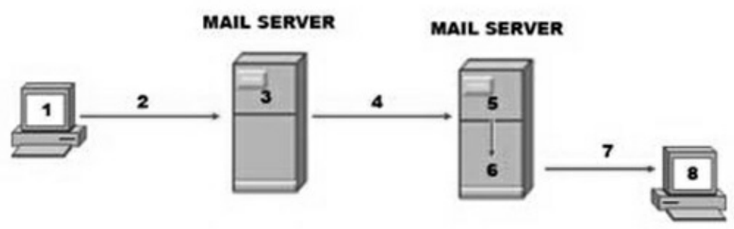
Az esettípusra jellemző, hogy közvetlenül nem fér hozzá sem a nyomozó hatóság munkatársa, sem a kirendelt igazságügyi informatikai szakértő a megtámadott rendszerhez és a támadásban érintett egyéb rendszerekhez. Az ügyben a sértett fél külföldi partnerének levelezőrendszerét érte kibertámadás a feltételezések szerint, amikor is a sértett és partnere kommunikációjában a partner helyét a támadó vette át, aki a partner helyett eljárva az igénybe vevendő szolgáltatásért pénzt csalt ki a sértettől. A kommunikáció a sértett gmail-fiókjában volt.

A kérdéses ügyben tehát a potenciális digitális bizonyítékokat egy felhőszolgáltatásból – *software as a service,* azaz felhőből szolgáltatott szoftver – kellett kinyerni, amihez a sértett együttműködését vette igénybe a szakértő. A művelet során a sértett belépett a saját Gmail-fiókjába, ahol a levelezési szolgáltatásban a szakértő közreműködésével megjelölte az ügy szempontjából releváns levélpéldányokat, amelyeket a szakértő *SZAKÉRTŐ* címkével (tag) látott el. Az így megjelölt levélpéldányokat a szakértő a Google saját archiválási szolgáltatása felhasználásával m-box formátumú, zip tömörítéssel ellátott archívumfájlba exportálta. A vizsgálat alapját mindössze a kinyert elektronikus levélpéldányok fejlécében *(header)* található továbbítási információk jelentették.

A vizsgálat nagyságának felméréséhez érdemes tisztázni néhány alapfogalmat, így az elektronikus levélküldés folyamatát is (lásd az *ábrá*t), amelynek alapvető lépései a következők:

– elektronikus levél megszerkesztése a küldő számítógépén (1);
– elektronikus levél továbbítása a küldő fél postafiókját kezelő levelezőszerver *(mail server)* felé valamilyen kommunikációs csatornán (2);
– a küldő fél postafiókját kezelő levelezőszerver fogadja, majd továbbítja a levelet a címzett postafiókját kezelő levelezőszervernek (3, 4);
– a címzett postafiókját kezelő levelezőszerver az elektronikuslevél-példányt elhelyezi a címzett postafiókjába (5, 6);
– a címzett letölti az üzeneteit valamilyen kommunikációs csatornán keresztül a saját számítógépére (7, 8).

Az elektronikuslevél-küldés folyamata



Forrás: http://ccnaq.blogspot.hu/2013/01/Refer-to-the-exhibit-The-diagram-represents-the-process-of-sending-e-mail-between-clients.html

A vázolt kommunikációs folyamatba úgynevezett beékelődéses támadással *(man-in-the-middle attack)* lehet bekapcsolódni, amelynek során a támadó informatikai alapú megtévesztést[33] használva (például címfeloldás hamisítása – *ARP spoofing;* dinamikus IP-cím-hamisítás – *DHCP spoofing,* vagy kap-

33 Chad Calvert – Taghi M. Khoshgoftaar – Maryam M. Najafabadi – Clifford Kemp: A Procedure for Collecting and Labeling Man-in-the-Middle Attack Traffic. International Journal of Reliability, Quality and Safety Engineering, vol. 24, no. 1, 2017

csolódásipont-lopás – *port stealing*) veszi át a kommunikációban részt vevő szerepét, majd az ő nevében folytatja a kommunikációt.

A vizsgált ügyben a sértett szóbeli tájékoztatása és a rendelkezésre álló adatok alapján a levelezőpartner postafiókjának jogszerű felhasználója oldalán történt beavatkozás az informatikai rendszerbe. Ebből adódóan a beavatkozással kapcsolatos digitális bizonyítékok is a postafiók jogszerű felhasználójának rendszerében keletkeztek. A fogadó (sértett) oldalán megjelenő digitális nyomok a kommunikáció során keletkezett elektronikus levelek fejlécében található továbbítási információkból származnak. Ezek alapján az a tény volt megállapítható, hogy mely IP-címekről kezdeményezték a kommunikációt a sértettel. Az IP-címeket az adott időben használó természetes személyek azonosítása az adott szolgáltatók megkeresésével és az IP-címek, valamint a küldési időpontok megadásával történhet meg az adott szolgáltató együttműködése esetén.

A vizsgálat adataiból e következtetések vonhatók le:

1. A sértett által küldött levelek nem tartalmaznak az adott postafiókot használóra vonatkozó IP-cím- és helyszínadatokat.
2. A postafiókból érkező elektronikus levelek azonosítható forráscímei a következő hálózatokból származtak:
   a) 177.209.×××.×××, 201.18. ×××.××× Oi Velox / Telemar Norte Leste S.A, Boa Vista város (Brazília, Amazonas szövetségi állam),
   b) 190.103.×××.×××, Axesat Peru S.A.C., Lima város (Peru, Lima tartomány),
   c) 181.41.×××.×××, Guyana Telephone & Telegraph Co., Georgetown város (Guyana, Demerara-Mahaic régió);
3. A postafiókból érkező elektronikus levelek továbbításában a következő kiszolgálók és szolgáltatók vettek részt:
   a) InternetNamesforBusiness.com, Fort Lauderdale város (Florida, Amerikai Egyesült Államok),
   b) ××× Kft., Budapest (Magyarország).

A rendelkezésre álló digitális bizonyítékokból az említetteknél több információ nem nyerhető ki az ügyre vonatkozóan.

Amint megfigyelhető, a feldolgozott ügyben az önálló, elszigetelt vizsgálat alig hoz eredményt. Feltételezve, hogy a csalás több sértettet is érinthetett, az információk összegyűjtése és megosztása – a nemzetközi bűnügyi adatcsere – lehet a megoldás a bizonyítás hiányosságaira.

Mivel a sértetti oldalon az Európai Unió és más európai országok állampolgárai mellett dél-amerikai gazdasági társaság is megtalálható (tudniillik a magyarországi sértett üzleti partnere) és az elkövetői oldalon álló személyek kiléte az elszigetelt vizsgálat adataiból nem állapítható meg, feltételezhető, hogy a nemzetközi együttműködés megszervezése és lebonyolítása nem lesz egyszerű folyamat. Ez a kérdés ugyanakkor messze túl mutat jelen tanulmány vizsgálati körén, mindamellett rendkívül fontos és a büntetőeljárások eredményét is jelentősen befolyásoló körülményről van szó, különösen a tárgyalt kiberbűncselekmény-típus esetén.

A GDPR várható hatásai a kiberbűncselekmények szakértői vizsgálatára

Amikor kiberbűncselekmények igazságügyi informatikai szakértői vizsgálatáról és a cselekmények felderítésének lehetőségeiről beszélünk, nem hagyhatjuk figyelmen kívül a jogi környezet aktuális változását, amely akár jelentősen is befolyásolhatja a vizsgálatok sikerességét.

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.), amely a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (*General Data Protection Regulation; GDPR* – általános adatvédelmi rendelet) szól, 2018. május 25-től alkalmazandó az unió tagországaiban.

Már többen is felhívták a figyelmet – ahogy azt a legutóbb az Európai Jogi Szaktanácsadói Hálózat *Digitalizáció* című konferenciájának büntetőjogi szekciójában megtartott előadásában[34] *Kökényesi-Bartos Attila* ügyész is megtette – arra, hogy megszűnik az IP-címekhez kapcsolódó információk – amelyek közül az egyik legfontosabb a doménregisztrációt végző személy(ek) adatai – visszakeresésére használt WHOIS-adatbázisok nyilvános elérése. Mivel a WHOIS-adatbázisokhoz történő hozzáférés elengedhetetlen a kiberbűncselekmények elleni hatékony fellépés és a felderítés területén, zavar keletkezhet a büntetőeljárás során a nyomozó hatóságok és az igazságügyi informatikai szakértők munkájában.

34 Kökényesi-Bartos, Attila: Overview of cybercrimes & European Judicial Cybercrime Network. Digitalisation – Criminal Law Section. Budapest, 05. 23. 2018.

Az IP-cím-tartományok kiosztásáért és a tartománynév-regisztrációért felelős szervezet *(Internet Corporation for Assigned Names and Numbers; ICANN)* úgy döntött, hogy a nyilvánosan elérhető WHOIS rendszert offline állapotba helyezi a személyes adatokhoz történő hozzáférés tekintetében a GDPR előírásainak megfelelően.[35] Az ICANN a GDPR alkalmazásának megkezdése utáni időszakra átmeneti modellt[36] javasol a rétegzett hozzáférés érdekében, ez egy akkreditációs rendszerbe történő bejelentkezést jelent a szolgáltatást igénybe venni kívánó szervezetek – például nyomozó hatóságok – részéről.

A Számítástechnikai Bűnözés Elleni Európai Igazságügyi Hálózat *(European Judicial Cybercrime Network; EJCN)* nyilatkozatban figyelmeztette az Eurojustot[37] és az Európai Tanácsot a WHOIS-adatbázisokhoz történő jogszerű hozzáférés várható következményeiről, amelyek között büntetőügyekben folyó nyomozások akadályoztatása, valamint a biztonságra és az áldozatok jogaira gyakorolt káros hatások is szerepeltek.[38]

Az előbbiekben írtak gyakorlatban tapasztalható hatásaként említhető, hogy a második és a harmadik esettanulmányban szereplő kiberbűncselekmények feltárásához alapvető fontosságú a Regionális Internetregiszterek *(Regional Internet Registries; RIRS)* adataihoz történő hozzáférés, amely meggyorsíthatja a kérdéses ügytípusok felderítését.

Összegzés

A bemutatott példák csupán szűk szegmensét fogták át a kiberbűncselekmények széles skálájának, mindamellett rámutattak azokra a fontos és néha kritikus pontokra, amelyek esetében nélkülözhetetlen az igazságügyi informatikai szakértők és a nyomozó hatóságok munkatársainak szorosabb együttműködése. Ennek az együttműködésnek a formája még vitatott[39], mindazonáltal nyilvánvalóan szükséges is.

Ugyancsak szükségesnek látszik a nyomozó hatóság potenciális digitális bizonyítékokkal kapcsolatba kerülő munkatársainak képzése, továbbképzése

35 Uo. 48–50. o.

36 Proposed Interim Models for Compliance with ICANN Agreements and Policies in Relation to the European Union's General Data Protection Regulation – For Discussion. ICANN, 01. 12. 2018. https://www.icann.org/en/system/files/files/interim-models-gdpr-compliance-12jan18-en.pdf

37 Az bűnözés súlyos formái elleni fokozott küzdelem céljából a tanács 202/187/IB határozatával létrehozott európai uniós szerv.

38 Kökényesi-Bartos Attila: i. m. 50. o.

39 Simon Béla: i. m. 399. o.

is. Végső célként megfogalmazható a digitális bizonyítékok helyszíni vizsgálója tudásszint elérése, rövid és középtávú célként pedig ennek megközelítése, de legalább az ez irányba történő elmozdulás.

A képzés és továbbképzés információhordozóiként olyan eszközöket kell használni, amelyek akár a napi gyakorlatban is használhatók, s amelyekre találhatunk jó és követendő példákat.[40] Ezek meghonosítása a hazai gyakorlatban olyan szereplőkre – szellemi műhelyekre – hárul, mint a milyen a Nemzeti Közszolgálati Egyetem Rendészettudományi Karán újonnan alakult kiberbűnözés elleni tanszék, illetve a Magyar Igazságügyi Szakértői Kamara Informatikai és Hírközlési Szakmai Tagozata.

40 Best Practices For Seizing Electronic Evidence v.3 A Pocket Guide for First Responders. U.S Department of Homeland Security / U.S. Secret Service, 2006. https://publicintelligence.net/u-s-secret-service-best-practices-for-seizing-electronic-evidence/

DOI: 10.38146/BSZ.2018.7-8.4

FAZEKAS ISTVÁN

A mesterségesintelligencia-kutatás eredményei a kriminalisztika néhány vonatkozásában

A kultúrtörténet során akkor következtek be a legnagyobb változások, amikor egyfajta információs forradalom zajlott. Ilyen volt az írás feltalálása, a könyvnyomtatás megjelenése vagy éppen a mobilkommunikáció térhódítása. Minden egyes ilyen alkalommal a korábban meglévő tudás megsokszorozódott, éreztetve áldásos hatását – és olykor átkos következményeit is. Az információrobbanás – a számítógépek tömeges elterjedése nyomán bekövetkező adatsokszorozódás – napjainkban is tartó folyamata az ismeretek korábban nem tapasztalt mértékű gyarapodását idézte elő. A mennyiségi növekedésen túl (éppen az informatika és társtudományai hihetetlen fejlődésének köszönhetően) azonban egy minőségi ugrás is bekövetkezett karnyújtásnyira hozva a tanulni képes, esetenként már kreatív gépek korát.

A digitális kor és a big data

Az International Data Corporation (IDC) által immár több mint harminc éve folyamatosan végzett és a világ digitális fejlődésére vonatkozó adatgyűjtő kutatások egyre megdöbbentőbb eredményeket tárnak a nagyközönség elé. A szervezet 2018 februárjában közzétett legfrissebb kutatási dokumentumainak tanúsága szerint 2020-ra mintegy 44 zettabyte mennyiségű felhalmozott adattal számolhatunk.[1]

De mennyi adat is ez?

Nos, ha az egyes után leírandó – és aztán azt csak sok ezer kilométeres távolságokban kifejezni képes – analógiát szeretném segítségül hívni, aligha sikerülne szemléletesen érzékeltetnem ezt az adatmennyiséget. Ezért más utat választok – tegyük fel, hogy az olvasó szereti a filmeket, méghozzá jó minőségben nézni.

A 4K felbontás már csodás vizuális élményt nyújt, a képpontok száma olyan nagy egy meglehetősen kis felületen (ennek megfelelően a méretük is

1 https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm

roppant kicsi), hogy két egymás melletti pontocskát közvetlen közelről még erős nagyítóval is igencsak nehézkes megkülönböztetni. Az interneten fellelhető 4K nagyfilmes tartalmak (itt kilencvenperces filmekre kell gondolni) átlagosan negyven gigabyte méretűek, vagyis kb. kilenc DVD-re férne el egy alkotás. Ilyen filmeket valamivel több mint négymillió évig nézhetnénk megszakítás nélkül. Hát ennyi az annyi.

Gyaníthatóan kérdések tömkelegét veti fel ez a kis számolás és a végeredménye az emberben, ezek közül én most csak egyet ragadok ki: honnan ez a rengeteg adat?

A teoretikusok nagyjából megegyeznek abban, hogy a digitális korszak valamikor a 2000-es évek legelején vette kezdetét. Az időpont meghatározása nem önkényes, annak során azt vették alapul, amikor a digitális tárolási kapacitás mértéke meghaladta az ugyanazon időpontban rendelkezésre álló analóg tárolási kapacitást.[2] Azóta az „adattermelés" éves üteme folyamatosan nő, 2011-ben valamivel több mint hatvan százalékkal volt nagyobb az előző évinél, napjainkra pedig egyes becslések szerint minden évben megduplázódik. Szintén az IDC felméréséből derül ki az, hogy két év múlva egy ember másodpercenként 1,7 megabyte adatot fog előállítani, és akkor még nem beszéltünk az üzleti jellegű adatdömpingről, az emberi beavatkozás nélkül létrejövő szenzorikus adatgyűjtésből származó nullák és egyek garmadájáról és a ma még nem is létező technológiák szolgáltatta adatáradatról.[3] Az adattermelés immár önálló technológiává vált, ennek a neve a sokat emlegetett big data. Ez a technológia (más megközelítésben a kifejezés a digitális kor szinonimája) legegyszerűbben úgy jellemezhető, hogy óriási adatmennyiség, amely a korszerű informatikai eszközökön keresztül közvetlen kapcsolatba hozható a mindennapi életünkkel, és képes azt befolyásolni. Egyfajta új természeti erőforrás ez, egyúttal számtalan kockázat forrása is.[4]

Ezek a kockázatok nem új keletűek, van azonban valami, ami napjainkban új szintre emeli őket – a kibertér kialakulása. A sci-fi szerző *William Gibson* által 1982-ben alkotott fogalom bejárta a világot és mára általánosan elfogadott megnevezése lett annak a virtuális térnek, amelyben az elektronikusan létrehozott adatok tárolódnak, és amelyben az online kommunikáció folyik. Ebben a virtuális térben öltenek formát azok a szándékok is, amelyek

2 Martin Hilbert – Priscilla López: The World's Technological Capacity to Store, Communicate, and Compute Information. Science, vol. 332, no. 6025, 2011

3 https://www.newgenapps.com/blog/big-data-statistics-predictions-on-the-future-of-big-data

4 Zsigovits László: A Big Data mint a rendvédelem egyik nagy kihívása. In: Gaál Gyula – Hautzinger Zoltán (szerk.): Tanulmányok „A változó rendészet aktuális kihívásai" című tudományos konferenciáról. Pécs, 2013 [Pécsi Határőr Tudományos Közlemények XIV.]

egyre több fejtörést okoznak a bűnüldözés szakembereinek. A számítógépes bűnözés vélhetően egyidős a digitális korral, az ellene való védekezésnek mára hatékony formái jöttek létre. Alapjuk, hogy a szakemberek a tapasztalatok fényében egy konzekvens és jól áttekinthető rendszerbe szervezik a megelőzés, felderítés és ellenállás módszereit, és ezeket nemzetközi joghatással párosítják[5] (a kiberbűnözés elleni fellépés dokumentumai). Az elkövetés stratégiája alapján a digitális bűnelkövetéssel foglalkozó tudományok *(Digital Forensic Science)* három területet különítenek el. A számítógép-központú, a számítógéppel segített és a járulékos számítógépes bűnözés területét. Az első esetben célpontként a számítógépes rendszer, hálózat, adattároló, vagy egyéb eszköz jelenik meg (például kereskedelmi weboldal tartalmának módosítása). Ez egyben tekinthető egy új bűncselekménytípusnak is, amely új eszközrendszert használ (tudniillik a számítógépet). A számítógéppel segített bűnözés esetében a számítógépet mint eszközt használja az elkövető a cselekmény során, ami „segíti" a tevékenységét, de nem feltétlenül szükséges hozzá. Itt hagyományos bűncselekményekről beszélhetünk, új módszerek alkalmazása mellett. Végül az a terület, amelyben a számítógépes rendszer a bűncselekmény szempontjából mellékes, lényegében valamely létező hagyományos eszköz kiváltását jelenti (például könyvelés számítógéppel, papíralapú dokumentáció helyett).

A fenyegetések formáinak és módszereinek feltérképezése mellett fontos az elkövetés kategóriáinak tisztázása, hiszen a büntetés – a visszatartó erőt jelentő hatás – ennek alapján határozható meg. Az cybercrime egyezmény[6] kiemel számos bűncselekménycsoportot, amelyeket a kiberbűncselekmények (a kibertérben elkövetett törvényellenes cselekmények) fogalmi körébe sorol, majd az egyes bűncselekményeket ezeken belül tipizálja:

1. Számítástechnikai rendszer és számítástechnikai adat hozzáférhetősége, sérthetetlensége és titkossága elleni bűncselekmények
   a) jogosulatlan belépés,

5 Például az Európai Parlament és a tanács rendelete az elektronikus hírközlés során a magánélet tiszteletben tartásáról és a személyes adatok védelméről, valamint a 2002/58/EK irányelv hatályon kívül helyezéséről (elektronikus hírközlési adatvédelmi rendelet javaslata, 2017); az Európai Parlament és a tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (elektronikus hírközlési adatvédelmi irányelv); az Európai Parlament és a tanács 2011/92/EU irányelve (2011. december 13.) a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről, valamint a 2004/68/IB tanácsi kerethatározat felváltásáról.

6 Az Európa Tanács Budapesten, 2001. november 23-án kelt számítástechnikai bűnözésről szóló egyezménye (ETS 185).

b) jogosulatlan kifürkészés,
c) számítástechnikai adat megsértése,
d) számítástechnikai rendszer megsértése,
e) eszközökkel való visszaélés;

2. Számítógéppel kapcsolatos bűncselekmények
   a) számítógéppel kapcsolatos hamisítás,
   b) számítógéppel kapcsolatos csalás;
3. Számítástechnikai adatok tartamával kapcsolatos bűncselekmények
   a) gyermekpornográfiával kapcsolatos bűncselekmény;
4. Szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekmények.[7]

A kiberbűnözés e keretei a továbbiakban már megfelelő alapot adnak az ellene való hatékony fellépéshez, illetve rugalmasságánál fogva lehetővé teszik az újabb törvényellenes jelenségek rendszerszintű asszimilálását az azok elleni harchoz. Szükség is van erre a fajta proaktív magatartásra, hiszen a technológia rohamos fejlődése az elkövetés módozatainak és célterületeinek bővülését hozta magával.

Eddig a kártékony kódok hálózati rendszereket fenyegető réme, a kiskorúak tapasztalatlanságával és védtelenségével való visszaélés legkülönbözőbb formái és az adatmanipuláció jelentette a legtöbb kapacitást lekötő veszélyeket. Az okoseszközök elterjedése (okostelefonok, -órák, -tévék, legújabban -porszívók, -hűtők és már erotikus segédeszközök is) roppantmód kiszélesítette a támadható célpontokat egyelőre még a klasszikusnak számító elkövetés módszerei mellett. Van azonban a fejlődésnek – amit gyakran negyedik ipari forradalomként is emlegetnek – egy olyan szegmense, amely már nem csupán mennyiségi, hanem minőségi változásokat képes generálni a kiberbűnözésben. Ez pedig a mesterségesen létrehozott kognitív képességek (gyűjtőnevén mesterséges intelligencia; AI) bűnelkövetés területén való felhasználásának lehetősége.

7 Máté István Zsolt: Az igazságügyi informatikai szakértő a büntetőeljárásban. PhD-értekezés. Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola, Pécs, 2017

A mesterségesintelligencia-kutatások rövid áttekintése és jelene[8]

A mesterségesintelligencia-kutatások kezdete egészen az 1940-es évek elejére nyúlik vissza. Az első hivatalosan is a területhez sorolt eredmény *W. McCulloch* és *W. Pitts* nevéhez fűződik, akik 1943-ban ez első mesterségesneuron- (a neuron természetes körülmények között az idegrendszer elemi építőköve) modellt javasolták, és kimutatták, hogy az ezekből felépített háló képes a tanulásra. A mesterséges intelligencia elnevezés *(Artificial Inteligence) John McCarthy*tól származik 1956-ból. Ez után a töretlen lelkesedés és az elvárások fokozódása jellemezte azokat a kutatási területeket (számítógépes nyelvészet, játékelmélet, alakzatfelismerés és gépi tanulás stb.), amelyek megalapozták a mesterséges intelligencia fejlődését. Jelentősebb sikereket azonban nem igazán tudtak felmutatni a szakemberek. Az áttörést a szakértői rendszerek kifejlesztése hozta meg, amelyek többnyire specializált folyamatok szabályokkal jól leírható feladatait hajtották végre (ilyen például a számítógéprendszerek komponenseit tartalmazó megrendelések konfigurálása). A nyolcvanas évek elején az AI-kutatások eredményeinek felhasználása ipari méreteket öltött. Aztán egy évtizeddel később a túlzottan optimista várakozások tükrében tett ígéretek teljesíthetetlensége miatt beköszöntött az „AI tele”, amikor a kutatások finanszírozása szinte teljes mértékben megszűnt, a felhasználói oldalon alakult cégek nagy része pedig tönkrement.

Egyetlen dolog maradt töretlen, a hit, hogy a mesterséges intelligencia létrehozása nem csupán álom. Ettől az erőtől hajtva megszállott tudósok az egyes részterületekre fókuszálva gyötrelmes, apró lépésekben valódi tudományos eredményeket produkáltak (ellenőrzött körülmények között létrejött, reprodukálható eredmények) olyan területeken, mint a beszédfelismerés, a robotika, a gépi látás vagy éppen a tudásreprezentációk. Az elért eredményeken felbátorodva a szakemberek a kilencvenes évektől egy új problémakörre összpontosítottak, amit a „teljes ágens” fogalmával jelöltek. Ezen a valós környezetbe ágyazott, folytonos szenzorikus adatokat fogadó mesterséges entitást értették. Az ilyen intelligens ágensek szempontjából az egyik legfontosabb működési környezet az internet. Mára a világhálós alkalmazásokban az AI-rendszerek mindennaposak lettek (spamszűrés, vírusdetektálás, online-magatartás-vizsgálatokra épülő ajánlórendszerek, interaktív csevegőalkalmazások, weboldal-optimalizálás, keresőgépek stb.), olyannyira, hogy a ’bot’[9]

8 http://mialmanach.mit.bme.hu/aima/ch01s03

9 A robot szó végéről „levált” ’bot’ kifejezés az automatikus, felügyelet nélküli programot jelöli.

szóvégződés már a mindennapi nyelvbe is beépült. A korrektség kedvéért idekívánkozik, hogy a teljes ágens és az intelligens robot nem ekvivalens kifejezések. Az integrált, szintetikus egyedeken belüli általános mesterséges intelligenciára (AGI) valójában még nincs példa. A rendszer azon elemei, amelyek az előzőkben felsorolt területeken működnek, úgynevezett szűk tudásterű AI-megvalósulások.[10]

A kockázatok felmérése

A mesterséges intelligenciához, még inkább a gondolkodó és érző robotok víziójához kapcsolódó félelmek gyakran tárgyalt jelenség. Regények, filmek és a tudomány prominens alakjai foglalkoznak azzal, hogy mit is jelent majd az AGI megjelenése, ha egyáltalán sor kerül rá. Van tehát egy általános viszonyulás a közvélemény részéről, amelyet a média által közvetített hírek alakítanak, és amely többnyire valamiféle szerves–szintetikus szembenállás formájában ölt testet, miközben van egy másik megközelítés, amely kevésbé körvonalazódott. Ez pedig a kibertérben végrehajtott bűncselekmények oldaláról közelít a területhez. A korábban tárgyalt számítógépes bűnözés új formáinak megjelenését a mesterségesen létrehozott kognitív entitások, a szűk tudásterű AI térhódítása idézi elő, amellyel a kiberbűnözés mintegy szintet ugrik.

Az új helyzetben a kockázatok és fenyegetések felmérése sokkal nagyobb mértékű szervezettséget és együttműködést kíván a törvényesség védelmében munkálkodók és a tudományos közösség tagjai között, miközben a tájékoztatás irányába is nagyobb aktivitást feltételez. 2018 elején egy 26 szerző által (tudósok, rendvédelmi szakemberek, jövőkutatók) jegyzett tudományos értekezés jelent meg[11]. A tanulmány a jelenleg már használatos AI-eredményekre fókuszál, illetve felveszi a repertoárba az öt éven belül várható fejlődés eredményeit is. A dokumentumban a szerzők megpróbálnak képet adni a mesterségesintelligencia-kutatások eredményeinek szándékosan rosszindulatú felhasználása esetén meglévő kockázatokról és veszélyekről, illetve javaslatot tesznek a megelőzésre és a már bekövetkezett biztonsági események okozta károk enyhítésére. Az együttműködés szükségességének felismerését tehát gyorsan követte a tett, ami mind az együttműködés szorosabbra voná-

10 Martin Ford: Robotok kora. Milyen lesz a világ munkahelyek nélkül? HVG Kiadó Zrt., Budapest, 2017, 250–251. o. [HVG-könyvek]

11 Miles Brundage et al.: The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. February 2018. https://www.eff.org/files/2018/02/20/malicious_ai_report_final.pdf

sában és elmélyítésében, mind a széles körű tájékoztatás gyakorlatában jelentős előrelépés. Az értekezés olyan stratégiai gondolatokat fogalmaz meg, mint a lehetséges célterületek klaszterezése (digitális, fizikai és politikai biztonság) vagy a várható fenyegetések módszertani besorolása (a tradicionális célpontok, módszerek és elkövetői kör bővülése, az „új típusú fenyegetések" megjelenése, a már meglévő fenyegetések jellegének megváltozása). További erénye a dokumentumnak, hogy – bár kiveszi a rosszindulatú felhasználás köréből – kitér az AI mint technológiai fejlődési jelenség által okozott (munkaerőpiac, vásárlói szokások átalakulása stb.) problémákra, illetve az AI-kutatás és -innováció területén a versenyelőny megszerzésére tett lépésekből származó veszélyekre (nemzetbiztonsági és titokvédelmi kockázatok). A vázolt megállapítások figyelembevételével immár kísérlet tehető arra, hogy a fenyegetettség forrásait, mértékét és célterületeit is számba lehessen venni.

Általánosítható és elsődleges jellegét tekintve a kockázat a világ digitalizált és globális mivoltából fakad. Ezt tovább súlyosbítja az a jellegzetesség, hogy eszközeink nagyobb része immár mobilis, multifunkcionális és hálózatba kötött, így bármikor, bárhol és bárhonnan, nem utolsósorban pedig bárki – már amennyiben birtokában van a megfelelő kapacitásoknak – által elérhetővé válhat.

Ha ez a „valaki" képességeinek megsokszorozására mesterségesintelligencia-elemeket használ, akkor olyan előnyhöz jut, amelynek birtokában a ma rendelkezésre álló védelmi rendszerek többsége hatékonyan kijátszható.

A falnak is szeme van

Az AI-kutatások kezdete óta foglalkoztatja a szakembereket a gépi látás problémája. Hogyan lehetne az emberi érzékelés (érzékszervek) analógiájára a környezetet a mesterséges entitások részére is érzékelhetővé tenni. Az már régen ismert és kihasznált tény, hogy a napi információáradat feldolgozásában a szemnek jut a legnagyobb szerep. Óvatos becslések szerint is a minket érő információs hatások több mint nyolcvan százaléka vizuális természetű. A gépi intelligencia működése során a környezet felfogása, az abban való tájékozódás kiemelt fontosságú. Ez pedig azt jelenti, hogy fel kell készíteni a gépeket a vizuális ingerek felfogására és feldolgozására. A kezdeti alakfelismerési problémák megoldása után a képfelismerési algoritmusoknak köszönhetően a gépi látás most már olyan összetett feladatok ellátására is képes, mint a valós időben való alakfelismerés és -követés akár több célobjek-

tum esetében is, vagy éppen a nézőponthalmazok elemzése után való vizuális 3D-rekonstrukció (mozgóképes felvételek esetében egy-egy nézőpontban látható tárgy vagy személy térbeli képének rekonstrukciója még gyengébb minőségű felvételek esetén is). A biometrikus azonosítás területén egyre nagyobb teret hódít az arckép-/arcvonás-detektálás módszere, amelyben a tanulóalgoritmusok szintén jelentős szerepet kapnak. A Google arcképazonosító algoritmusa nagyobb pontossággal ismeri fel az arcokat, mint az ember, és a fejlődés még csak az elején tart. Némi képzelőerő és az előbbi tények ismeretében nem ördöngösség felmérni a kockázatokat. A hálózatba kötött köztéri vagy magánüzemeltetésű biztonságikamera-rendszerek a nap huszonnégy órájában folyamatosan pásztázzák a teret, a műholdak funkciójuktól függően szintén képi információval látják el az üzemeltetőiket vagy bérlőiket. Az autonóm rendszerek – legyen szó önvezető járművekről, vagy éppen egy raktár készleteinek elrendezését végző rendszerről, nem is beszélve némely katonai alkalmazásról – szintén jelentős mértékben támaszkodnak a környezetből érkező vizuális természetű információkra.

Az ezekhez való illetéktelen hozzáférés után – amelyhez talán már valamely AI-komponenst használt az elkövető – a behatoló képessé válik akár az irányítás átvételére, vagy olyan adatok megszerzésére, amelyeket egy későbbi alkalommal használ fel (azonosítás megtévesztése, megfigyelési rendszerek kijátszása stb.)[12]. A már ma is működő retinaszkennerek esetében egy webkamera feletti irányítás átvételét követően, a szemről készített megfelelő felbontású képek AI „tisztítása” és a retina rekonstrukciója után rendelkezésre áll egy klón, amely lehetővé teszi egy biztonsági rendszer feltörését. A pénzszállító járművek mozgásának és útvonaljellemzőinek kameraképeit neurális háló segítségével elemezve megtalálhatók a sikeres támadást lehetővé tevő rések.

A megtévesztés mesterei

A másik olyan terület, amely napjainkra kiemelkedően jó színvonalon képes működni, a beszédfelismerés és a beszédszintézis. A számítógépes nyelvészet alapjaiból kifejlődő tudományág mára szintén életünk számos területére belopódzott. Ezekre építenek az intelligens asszisztensek (Siri), a chatbotok és

12 Kevin Townsend: The Malicious Use of Artificial Intelligence in Cybersecurity. Security Week, March 28, 2018. https://www.securityweek.com/malicious-use-artificial-intelligence-cybersecurity

még számtalan online alkalmazás. Ma már az ügyfélszolgálatok, a helpdesk szolgáltatásokat nyújtó szervezetek vagy éppen az online termékajánlatok készítői is előszeretettel használják ezt a technológiát. Az emberi természetes beszéddel való vezérlés már nemcsak a számítógépek – erre már az angol nyelvű Windows XP is képes volt – sajátja, szóbeli utasításokkal vezérelhetjük a porszívónkat, vagy éppen a garázskaput. A gépek értik és válaszolnak is, a válaszok pedig már régen nem a klasszikus szintetikus robothangok, hanem kifinomult emberi vokalitások. Nem nehéz elképzelni azt a helyzetet, amelyben a mesterséges intelligencia nemes egyszerűséggel ismerősünk hangján csevegve átveri a vonal túlsó végén gyanútlanul vele társalgó embert. De ugyanígy egy hangazonosítás alkalmával is kiválóan teljesíthet, hozzáférve védett tartalmakhoz, vagy egyéb értékekhez. Ha mindehhez hozzátesszük, hogy ezek az alkalmazások a nyelvek közötti átjárhatóság (fordítók, szinkrontolmács alkalmazások) területének vezető megoldásai, akkor nyilvánvalóvá válik, hogy a globális kibertérben a veszélyek is globálisan jelentkeznek.

Szegregáció kontra aggregáció

Az új, intelligens algoritmusok kínálta lehetőségek egyik kiemelkedően fontos jellemzője, hogy túllépnek az adatok egyszerű felhalmozásán (aggregáció). Bonyolult számítástudományi, statisztikai, hálózatelméleti és genetikus kódoláson alapuló elemzési módszereket alkalmazva összefüggéseket, rejtett kapcsolatokat tárnak fel. Más alkalommal az adatok elkülönítésének technikájával (szegregáció) dolgoznak, aminek eredményeképpen képesek kiszűrni az eltérő, egyedi jellegzetességeket és ezzel leszűkíteni egy keresés találatainak körét és számát. Ezeket a technikákat napjainkra a bűnmegelőzés és a bűncselekmények felderítése során is egyre gyakrabban alkalmazzák a szakemberek.

A védekezés területei és módszerei

A rendvédelem területén dolgozók, a biztonsági szolgálatok és az érzékeny adatokkal foglalkozó szervezetek már az AI-kutatások első kézzelfogható és használható eredményeinek megjelenése óta igyekeznek azokat munkamódszereikbe integrálni. Napjainkban már olyan stratégiai területeken vetik be a

mesterségesintelligencia-kutatások vívmányait, mint a vírusvédelem, a spamszűrés, a profilalkotás, az intelligens térfigyelő rendszerek és ezekkel összefüggésben a képjavítási technológiák és az azonosítás. A kifejezetten a bűnmegelőzés irányába mutató kezdeményezések mind Európa országaiban, mind a tengerentúl egyre nagyobb szerepet kapnak. Ezek közül kiemelkedő a statisztikai jellegű klaszterezés, amelyben az információs rendszerek szolgáltatta adatokat feldolgozva elkészítik egy-egy terület bűnmegelőzési szempontok alapján érzékenyített térképét. Ez mintegy előrejelzi a várható elkövetések lehetséges és legvalószínűbb helyszíneit, a szóba jöhető elkövetők személyét és a veszélyeztetettek körét is. Hasonló elvek alapján szerveződnek a legmodernebb adatbiztonsági rendszerek és védelmi struktúrák is. Élő példaként említhető az AI-alapú automatikus védelmi rendszer, a Vectra Cognito, amelyről a terület kiemelkedő szakemberei a következő jellemzést adták: *„A Cognito automatikusan, valós időben elemzi, rangsorolja, összeveti egymással és priorizálja a vállalaton belüli aktív fenyegetéseket, így jelentősen csökkenti a biztonsági elemzők túlterhelését.”* Ez lehetővé teszi a biztonsági csapatok számára, hogy a legkritikusabb fenyegetésekre összpontosítsanak anélkül, hogy elárasztanák őket az alacsony kockázatú eseményekre vonatkozó állandó riasztások.[13]

A bűncselekmények felderítésekor a tanulóalgoritmusok bevetése a nyomszakértésben, a DNS-vizsgálatokban és a kapcsolati rendszerek feltérképezésében jelentősen növeli a hatékonyságot. Sőt, a jövő fenyegetéseinek előrejelzésében és a rájuk való felkészülésben is egyre nagyobb szerepet játszanak, mint arra az előzőekben bemutatott módszerek utalnak. Az önvezető járművek, a csomagszállító drónok, az orvoslásban a nanotechnológia térhódítása olyan kihívások elé állítja a törvényesség védelmezőit, amelyeknek a hagyományos eszközökkel és felkészültséggel már nagyon nehéz megfelelni. A jövő a tudásalapú szervezetek előtt nyit nagyobb távlatokat, amit a rendvédelem területén sem szabad figyelmen kívül hagyni.

Kitekintés

1997-ben a Deep Blue elnevezésű nagy teljesítményű számítógép[14] legyőzte *Garri Kaszparov* sakknagymestert. A sakk azonban olyan játék, amelyben minden állás egzakt módon betáplálható egy gépbe, egy ilyen mérkőzés ki-

13 https://info.vectra.ai/hs-fs/hub/388196/file-1918923738.pdf
14 A Deep Blue 1997-ben a világ 259. legerősebb szuperszámítógépe volt.

menetele csak a tárolt adatokhoz való hozzáférés és azok feldolgozásának sebességén múlik. Az AI kezdetekben valójában azokon a területeken teljesített jól, ahol nagy mennyiségű adat feldolgozása vált szükségessé, de jól definiálható szabályok és állapotok, valamint a bizonytalanság kizárása mellett. Mára a helyzet gyökeresen megváltozott. A tanulóalgoritmusok túllépnek ezen a fajta hatékonyságon. Teljesítményük attól függően változik, hogy a felügyelt, a felügyelet nélküli vagy a részben vagy félig felügyelt tanulási szisztéma szerint működnek-e. Mindhárom esetben a kiinduló állapot azonos, a szoftver úgynevezett tanuló-adatbázisok adatait kapja meg. A különbség abban van, hogy kap-e ezekhez az adatokhoz azokat a megoldással összekötő közvetlen információkat, vagyis van-e jól definiált cél. Ha nincs ilyen egyértelmű kimenet, az algoritmusnak magának kell azt meghatároznia a rendelkezésre álló adatok halmazának elemzése alapján. Ekkor beszélünk felügyelet nélküli tanulásról. A mesterséges intelligencia ezen a szinten válik igazán önálló, mintegy intuitív és kreatív entitássá és ebben a formájában hordozza a legtöbb kockázatot.

Húsz évvel a Deep Blue győzelme után az AI újabb bravúrt hajtott végre immár a felügyelet nélküli tanulás algoritmusával felruházva[15]. Az algoritmusnak mindössze a sakk alapvető szabályait, a felállást, a lépéseket tanították meg, illetve azt, hogy mi számít győzelemnek (azaz mattnak). Alpha Zero ezután négy óra alatt nagymesteri szinten kezdett játszani, teljesen új nyerési stratégiákkal előállva. Hogy ezt diadalként, vagy a vészharang első kondulásaként értékeljük-e, az – jelen pillanatban még – rajtunk áll.

15 NAK: Új sakknagymestere van az emberiségnek. Index, 2017. december 8. https://index.hu/tech/2017/12/08/uj_sakknagymestere_van_az_emberisegnek_egy_gep/

DOI: 10.38146/BSZ.2018.7-8.5

NAGY TAMÁS

Business E-mail Compromise, avagy az átutalásokhoz kapcsolódó csalások

Az információs társadalom[1] korában az információ olyan önálló értékké kezd válni, amely a termelésben, a gazdaságban, illetve a társadalmi működésben is egyre fontosabb szerepet tölt be. Az információ, illetve ezzel szoros összefüggésben annak előállítása, elosztása, terjesztése és használata mára a technológiai fejlődés alapja. E folyamat eredménye, hogy az információfeldolgozáshoz szükséges technológiák globális szinten is beépültek a mindennapjainkba, ami a gazdasági, szociális vagy akár kulturális tevékenységeinket is nagymértékben megkönnyíti. A társadalmi átalakulás pozitív hatása mellett azonban fontos megemlíteni azokat a nehézségeket is, amelyek a technikai átalakulás következtében kerültek előtérbe. A gazdaság és a pénzügyi szektor legtöbb tevékenységét – kiváltva az emberi tényezőt – immár számítógépek végzik, ez azonban korántsem jelenti azt, hogy e rendszerek sérthetetlenek lennének. A biztonsággal kapcsolatos értelmezések viszonylag új eleme a kiberbiztonság, amely az adatokra és az információs rendszerekre leselkedő veszélyekre fókuszál.[2] A technológiai környezet folyamatos változása olyan új fenyegetéseket idézett elő ugyanis, amelyek közös jellemzője, hogy jogilag viszonylag meghatározatlanok, előfordulásuk tömegességéből adódóan azonban jelentős károkat képesek okozni.[3] A felvetődő kockázatok kezelése összetett és sokrétű feladat, amely az átfogó intézkedések mellett (ilyen például Magyarország Nemzeti Kiberbiztonsági Stratégiája[4], illetve az EU 2016/1148 irányelve[5]) egy-egy terület önálló felkészítését is szükségessé teszi. Véleményem szerint ebből a szempontból kiemelt szerep jut a nyomozó hatóságoknak, mivel a biztonság e for-

1 Az információs társadalom fogalmát *Fritz Machlup* amerikai közgazdász vezette be a *The production and distribution of knowledge in the United States* (A tudás termelése és elosztása az Egyesült Államokban) című, 1962-ben megjelenő művében.

2 Robert Fischer – Edward Halibozek – David Walters: Introduction to security. Elsevier Inc., New York, 2013, p. 435.

3 Nagy Zoltán András: Bűncselekmények számítógépes környezetben, Ad Librum Kiadó, Budapest, 2009, 21. o.

4 1139/2013. (III. 21.) kormányhatározat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról.

5 Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész unióban egységesen magas szintjét biztosító intézkedésekről.

májának megteremtésében a bűnüldözés szerepe megkérdőjelezhetetlen. Az új típusú nehézségek kezelésének időszerűségét jelzi, hogy a büntető törvénykönyv önálló fejezetében (XLIII. fejezet) foglaltak mellett[6] manapság már szinte valamennyi intellektuális bűncselekmény kapcsolódik az információs rendszerekhez. E mű középpontjában a csalás olyan újonnan megjelent formája áll, amelynek egyedi jellegét az adja, hogy az információs rendszerek működése mellett nagymértékben épít azokra az emberi tényezőkre is, amelyek megfelelő eszközökkel könnyedén befolyásolhatók. A következő oldalakon igyekszem röviden bemutatni a cselekménnyel kapcsolatos ismérveket és tapasztalatokat, továbbá olyan gyakorlati ajánlásokat megfogalmazni, amelyek – megfelelő körülmények között – elősegítik a megelőzést és a bűncselekmények felderítését.

Business E-mail Compromise a bűnügyi terminológiában

Az angolszász rendvédelmi terminológiában a Business E-mail Compromise (a továbbiakban: BEC) olyan bűncselekményi kört jelöl, amely kifejezetten a rendszeres pénzügyi tranzakciókat lebonyolító gazdasági szereplőket célozza. E bűncselekménytípus különleges jellemzője, hogy a pénzügyi átutalási[7] (vagy kifizetési) rendszerek működését befolyásolják a rendszert kezelő vagy irányító személyeken keresztül. Ahogy utaltam rá, a megnevezés összetett fogalmi kategóriát jelöl, amiben a legtipikusabb elkövetési módok a következők:

a) A cselekmény legjellemzőbb formája elsősorban a külföldi beszállítókkal dolgozó cégek esetében jelent valós veszélyt, mivel itt gyakorlati akadályai is lehetnek az ellenőrizhetőségnek. A támadók ebben az esetben hamis számlázási adatokat adnak meg a beszállítók nevében (és e-mail-címét felhasználva), jellemzően adatváltozásra vagy egyéb külső körülményre hivatkozva. Az adatváltozással érintett számlaszám természetesen nem a beszállítóhoz, hanem az elkövetőkhöz kapcsolódik.
b) Nem sokban különbözik az előbbi esettől az, amikor valamely vállalati vezető jogosultságait felhasználva adnak hamis utasítást a kifizetésre vagy pénzügyi ellenjegyzésre jogosult alkalmazottaknak.

---

6 A büntető törvénykönyvbe 1994-ben került be önálló bűncselekményi kategóriaként a számítógépes bűncselekmények normatív fogalma.

7 A bankszámla-tulajdonos (kifizető) kezdeményezésére teljesített olyan átírás, amely során a pénzintézet fizetés céljából pénzösszegeket vezet a kifizető bankszámlájáról a kedvezményezett bankszámlájára. Az átutalásokat belföldi és nemzetközi pénzforgalomban egyaránt használják.

c) Előfordulhat olyan eset is, amikor a kifizetésre vagy ellenőrzésre jogosult e-mail-fiókját feltörik, majd az onnan beszerzett adatokat felhasználva kérnek kifizetést valamely valós pénzügyi partnernek oly módon, hogy a számlaadatokat előzetesen megváltoztatták.
d) Bizonyos esetekben, az e-mailben a csalók olyan bizalmi személynek (adótanácsadó, ügyvéd, könyvelő stb.) adják ki magukat, aki az általános működésben részt vesz, azt a látszatot keltve, hogy az általuk kért átutalás hozzá tartozik a cég nem rendszeres pénzügyi tevékenységéhez.
e) Az előbbieken túl azokat a cselekményeket is a BEC körébe szokták sorolni, amikor a személyzeti vagy könyvelési alkalmazottakon keresztül szereznek azonosításra alkalmas személyes adatokat, amelyeket a korábban említett módokon használhatnak fel.[8]

Ahogy az egyes példák is mutatják, valamennyi elkövetési séma osztozik bizonyos közös jellemzőkön. Ilyen például az, hogy

– az elkövetők célja az anyagi haszonszerzés, amit a pénzügyi átutalások révén kívánnak megvalósítani;
– az elkövetés eszköze maga az elektronikus levél (e-mail), amelyet formailag és tartalmilag is úgy hoznák létre, hogy annak egyedi vonásai ne keltsenek gyanút (az e-mail nem tartalmaz olyan rosszindulatú hivatkozást vagy csatolmányt, ami miatt fennakadhatna a biztonsági rendszereken);
– az elkövetők minden esetben befolyásolnak olyan személyeket, akik a pénzügyi tevékenységben közreműködnek, vagy azokat irányítják.

A cselekménynek nincs általánosan elfogadott meghatározása, valószínűleg azért, mert maga az elkövetési mód sem egységes. A leírásra használt (és mára általánosan elterjedt) Business E-mail Compromise (BEC/AEC) elnevezést először az FBI[9] kezdte el használni, az egyes bűncselekményekkel kapcsolatos útmutatóiban. Mivel a BEC világszerte egyre elterjedtebb formája a csalásnak, ezért az ügynökség minden évben kiad egy olyan jelentést, amely összefoglalja a cselekménnyel kapcsolatos irányvonalakat, tendenciákat és teendőket. A legutóbbi, 2017-ben készült kiadvány statisztikai összefoglalója alapján a 2013 októberétől 2016 decemberéig eltelt időszakban több mint 40 203 olyan incidens történt világszerte, aminek elkövetési módszere meg-

8 Forrás: www.fbi.gov
9 Federal Bureau of Investigation (Szövetségi Nyomozóiroda) = az amerikai igazságügyi minisztérium (Department of Justice) alá tartozó, szövetségi szintű nyomozószerv, a legkiterjedtebb nyomozati jogkörrel az Amerikai Egyesült Államok területén.

egyezett a leírtakkal. A rendelkezésre álló adatok alapján e bűncselekmények mintegy 5 302 890 448 dollár kárt okoztak világszerte.[10] A jelentés alapján világosan körvonalazódik az a tendencia, miszerint a BEC nemcsak világméretűvé vált, hanem egyúttal nemzetközi jelleget is öltött. Az elmúlt években 131 országban követtek el ilyen cselekményeket úgy, hogy az elkövetőkhöz kapcsolódó bankszámlákat 103 országban azonosítottak.

Az elkövetés különleges jegyei

A Business E-mail Compromise gyakorlati szempontból a csalás nagyon kifinomult formájának tekinthető, amelyet nemcsak az tesz veszélyessé, hogy az alapvető eszközként használja a információs rendszerek nyújtotta előnyöket, hanem az is, hogy az elkövetés szinte valamennyi esetben jól megtervezett. Ez a tervszerűség magában foglalja azt, hogy az elkövetők sokszor akár több hónapos felkészülés után hajtják végre a cselekményt, ezzel egyidőben pedig megfigyelik, illetve adatot gyűjtenek a leendő célpontról. Az adatgyűjtés célja az érintett vállalkozással kapcsolatos információk beszerzése, a célpont releváns körülményeinek (különösen a pénzügyi szokások) felderítése, ami különösen a következőkre terjedhet ki:

– a vállalkozás tevékenységének és üzleti kapcsolatrendszerének feltérképezése (a vállalkozással üzleti/pénzügyi kapcsolatban álló egyéb vállalkozások és magánszemélyek);
– az állandó pénzügyi partnerek, illetve az egyes partnerekhez kapcsolódó részletes pénzügyi adatok beszerzése (szolgáltatás/tevékenység jellege, fennáll-e szerződéses jogviszony a felek között, kapcsolattartó adatai stb.);
– a főkönyvi számlákon szereplő egyéb azonosítható bejegyzések adatainak beszerzése (ki- és befizetések, csoportos beszedési megbízások, jóváírások és terhelések összege, jogcíme, kamatai stb.);
– a pénzügyi tranzakció önálló indítására és/vagy jóváhagyására jogosult személyek beazonosítása, illetve az e jogosultakra vonatkozó személyes adatok beszerzése;

10 Forrás: www.ic3.gov FBI-Internet Crime Compliant Center (internetes bűncselekmények panaszközpontja). A kiadvány statisztikai összefoglalójához nemcsak az egyes országok rendvédelmi szerveinek, hanem a nemzetközi pénzintézeteknek és gazdasági szereplőknek a beszámolóit is felhasználják, ezért a téma kapcsán általánosan elfogadott hivatkozási pontnak tekinthető.

– a vállalkozás által használt informatikai vagy hírközlő hálózat sajátosságainak (például levelezési program, operációs rendszer stb.) azonosítása, illetve az ezekhez való – korlátozás nélküli – hozzáférés biztosítása.

A gyakorlati tapasztalatok alapján az ilyen jellegű nyomozások általános jellemzője, hogy a hatékony felderítés, illetve az ahhoz kapcsolódó vagyonvisszaszerzés sikere nagyrészt azon múlik, hogy a rendelkezésre álló adatokat milyen gyorsan képesek a hatóságok beszerezni és értékelni. Ezzel összefüggésben fontos megjegyezni, hogy a BEC esetében – a pénzforgalmi adatok mellett – a levelezéshez kapcsolódó információk egyúttal a cselekmény felderítésének kulcsmomentumai is. Természetesen joggal vetődik fel a kérdés: miért is fontos ezt kiemelni?

A cselekmény szűkebb értelemben vett elkövetési eszköze az a megtévesztő jellegű e-mail, amelynek célja a címzett tévedésbe ejtése annak érdekében, hogy a kifizetésre jogosult az eseti vagy visszatérő jellegű tranzakció során az elkövető által megadott – e-mailben szereplő – számlaszámot tüntesse fel a tranzakció során.[11] A BEC esetében, függetlenül attól, hogy a cselekmény megelőzése vagy felderítése a cél, elengedhetetlen a cselekményhez kapcsolódó alapvető technikai kérdések tisztázása. A hazai és a nemzetközi gyakorlat azt mutatja, hogy a kompromittáló e-mailek azért alkalmasak a csalás elkövetésére, mert a legtöbb esetben formailag és tartalmilag is azt a látszatot keltik, hogy egyrészt a küldőként megjelölt személytől vagy pénzügyi partnertől származnak, másrészt valós követelésre vagy pénzügyi teljesítésre vonatkoznak. Ahhoz, hogy az elkövető ezen e-maileket kellőképpen előkészíthesse, be kell szereznie azokat az egyedi információkat, amelyek például a felek közötti kapcsolattartás jellegére, formájára vagy rendszerességére utalnak. Ennek kézenfekvőbb eszköze valamely felhasználó adatainak megszerzése, illetve az SMTP-szerverhez[12] kapcsolódó számítógép ellen végrehajtott vírustámadás. Ha az elkövető hozzáférése biztosított, a levelezési rendszer adatai alapján kiválasztja azt a partnert, amelynek inkognitóját a csalás elkövetéséhez felhasználja. Hogy az érintett felek ne fogjanak gyanút, az elkövető a kommunikációs csatorna (vagyis a számítógépes hálózat) átirá-

11 Az ilyen típusú csalásoknak létezik olyan formája is, amely esetén az e-mail lakossági szolgáltatások kisebb összegű elmaradásáról tájékoztat. Az e-mail a szövegtörzsében szereplő linken keresztül – hitelesnek tűnő – fizetési felületet biztosít, ennek kitöltése révén azonban az elkövetők megszerzik a sértett kártyaadatait.

12 A Simple Mail Transfer Protocol rövidítése, amely azt a szervert jelöli, amely a levelezéshez kapcsolódó szolgáltatást lehetővé teszi.

nyításával eléri, hogy a rendszer a kimenő üzeneteket minden esetben az általa kiválasztott (vagy létrehozott) címre továbbítsa. A gyakorlatban ezt közbeékelődéses támadásnak[13] nevezik, mivel a felek közötti kommunikációt úgy befolyásolja a támadó, hogy mindkét szereplő számára a másik félnek adja ki magát. Az üzenetváltások során a felek így valójában nem egymással, hanem a támadóval állnak kapcsolatban, aki az így beérkező üzeneteket (különösen azok tartalmát) felhasználja az átutalások manipulálására.

Az előbbiek is jól mutatják, hogy a nyomozó hatóságok számára miért is nélkülözhetetlen a levelezőrendszerekhez kapcsolódó adatgyűjtés (lefoglalás), majd az ezzel összefüggő elemző-értékelés. Ha a hálózatba történő behatolás módja (például trójai vírus vagy külső bejelentkezés) meghatározható, akkor az elkövetés helye, illetve az elkövetők személye nagyobb bizonyossággal azonosítható, mint az utalásokhoz kapcsolódó adatok önálló elemzésével. Mivel a kedvezményezetti számlaszám tulajdonosa általában olyan személy, aki pénzügyi – vagy egyéb – ellenszolgáltatásért cserébe létrehozza és fenntartja az érintett számlát, ezért utóbbi elsősorban e személyek azonosításához elegendő.

A cselekmény időszerűsége

A pénzügyi szektort vagy a gazdaság szereplőit célzó csalások hazai viszonylatban is egyre elterjedtebbek, miközben az ezekkel kapcsolatos, a cselekmények önálló felismerését célzó ismeretek kevésbé kimunkáltak. A BEC nagyobb számban először az Amerikai Egyesült Államokban jelent meg (a cselekmény leírására használt műszót is innen vette át például az Europol), ahol évről évre a kiberbűncselekmények egyre nagyobb hányada célozza az átutalási rendszereket, illetve okoz közvetlen károkat a pénzügyi szektorban. Mivel a cselekmények technikai összetettsége sok esetben szinte lehetetlenné teszi az utólagos felderítést, ezért az elmúlt években – a prevenciót hangsúlyozva – több olyan összefoglaló is napvilágot látott, amely a bűncselekmények fontosabb elemeinek bemutatását célozza. Ezek közül az FBI által készített prezentációs anyag az, amely a legkidolgozottabb formában tárja elénk, és – időrendben – egyúttal négy fontos mozzanatát különbözteti meg a cselekménynek.

13 Azonos jelentéssel bír a szakmai gyakorlatban szintén elterjedt *man-in-the-middle* angol kifejezés is.

A célpont kiválasztása

Az elkövető (vagy elkövetői csoport) kiválasztja azt a vállalkozást vagy személyt, amelynek pénzügyi portfóliója, illetve alkalmazotti (vagy vezetői) körre előzetesen megfelel azoknak a feltételeknek, amelyek alkalmassá teszik a kompromittálásra (ilyen például a nemzetközi ügyfélkör, a széles tevékenységi kör vagy az angol munkanyelv). A kiválasztás során nyílt adatgyűjtéssel is könnyen feltérképezhető a célpont profilja. Jelentős szerepet kaphatnak például azok a közösségi tartalmak, amelyekkel – közvetve vagy közvetlenül is – a vállalkozás működésére vonatkozó információ szerezhető be (például kapcsolati háló, munkarend, munkahelyi szokások stb.).

Célzott támadások

Az előzetesen beszerzett információk birtokában az elkövető célzott támadásokat indít vezető beosztású, vagy a pénzügyi területen tevékenykedő és a kifizetésekre jogosult személyek ellen. Az elkövetők az e személyekhez kapcsolódó tevékenységük során a manipuláció és nyomásgyakorlás különböző eszközeire építenek. Az ehhez szorosan kapcsolódó fiktív e-mailek vagy telefonhívások mellett (amely az emberi tényezőt célozza) megjelennek azok az eszközök is, amelyek például az informatikai rendszereket támadják. Ennek eszközei például az úgynevezett trójai vírusok vagy egyes kémprogramok, amelyek célja a rendszerbe való bejutás, valamint a rendszer sebezhetőségének felmérése. Fontos körülmény, hogy az említett kibertámadások célja nem a zavarkeltés, hanem a rendszer felhasználói adatainak – különösen az egyes profilokhoz kapcsolódó felhasználónevek, jelszavak és kódok – megszerzése, mivel ezek birtokában fizikai jelenlét nélkül is lehetséges a számítógépes hálózat közvetlen befolyásolása.

A pénzügyi ügylethez kapcsolódó adatok cseréje

A szükséges adatok beszerzése után az elkövető az általa kiválasztott pénzügyi partner arculatát (logó, elnevezés, karakterek, szimbólumok stb.) és e-mail-címét felhasználva[14] célzott e-mailt küld a vállalkozás munkavállalójának vagy tisztviselőjének. E levelek azt a látszatot keltik, hogy a küldőként megjelölt személytől vagy szolgáltatótól származnak és – a felek között fennálló üzleti

14 Az üzenetek eltérítésével vagy hamis e-mail-kliens (például közbeiktatott karakter) létrehozásával.

kapcsolat alapján – valós követelésre vagy pénzügyi teljesítésre vonatkoznak. Gyanúra adhat okot a kedvezményezett számlaadatainak változásáról szóló értesítés, vagy a küldő e-mail-címében felbukkanó eltérés is (például diamond-techniques@diamond.com helyett diamondtechniques@dyamond.com).

Átutalás, továbbutalás

Az e-mailben foglaltak alapján a megtévesztett személy utalást indít vagy utalást hagy jóvá a csalók által megadott kedvezményezetti számla vonatkozásában. Az eddig feltárt magyarországi esetek azt mutatják, hogy az átutalások a legtöbb esetben belföldi pénz- vagy hitelintézetek által vezetett folyószámlára érkeznek. A számlatulajdonosként bejegyzett vagy az ezek felett rendelkező személyek jellemzően olyan strómanok, akik anyagi ellenszolgáltatásért cserébe létrehozzák és fenntartják a számlát. A vagyoni hátrány megtérítése kapcsán e személyek szerepe sem mellékes, mivel a számla kezelésével összefüggésben ők azok, akik a továbbutalással vagy készpénzfelvétellel az elkövetők rendelkezésére bocsátják a megszerzett összeget. (Itt fontos megjegyezni, hogy a számla fenntartása, kezelése, illetve az annak egyenlegét érintő pénzügyi műveletek alkalmasak lehetnek a Btk.[15] 399–400. § szerint meghatározott pénzmosás bűntettének megállapítására.)

A normatív háttérről

A Business E-mail Compromise, vagyis az átutalásokhoz kapcsolódó csalások nem sokban különböznek a bűncselekmény más formáitól, egyedileg vizsgálva mégis olyan jellemzőkkel bírnak, amelyek felismerése a nyomozás kapcsán kiemelten fontos. Mivel a cselekmény felismerése kéz a kézben jár annak jellegzetes vonásaival, ezért érdemes lehet a fontosabb jellemzőit külön is kiemelni:

– a cselekmény célpontja a legtöbb esetben olyan – előre kiválasztott – természetes vagy jogi személy (gazdasági társaság, befektető stb.), akinek, illetve amelynek tranzakciós forgalma jelentős (számszerűségét, illetve az egyes tranzakciók értékeit figyelembe véve);
– a cselekmény előkészítésének lényeges eleme az adatszerzés, amelynek része a célpont informatikai rendszerének célzott támadása is;

15 A büntető törvénykönyvről szóló 2012. évi C. törvény.

– e támadások elsődleges célja az alkalmazotti kör feltérképezése, továbbá a felhasználói adatok megszerzése;
– az elkövető az előkészítés során azonosítja azokat a személyeket, akik átutalások kezdeményezésére vagy jóváhagyására jogosultak, majd valótlan pénzügyi teljesítésre vonatkozó célzott e-mailt küld részükre;
– a kifizetésre jogosult – abban a hitben, hogy valós kötelezettséget teljesít – utalást kezdeményez az e-mailben megjelölt számlaszámot felhasználva;
– a tranzakció jóváírása után a számla kezelője továbbutalással vagy a készpénz tényleges felvételével a csaló rendelkezésére bocsátja az így megszerzett összeget.

A hasonló jellegű bűncselekményeket vizsgálva egyértelműen megállapítható, hogy a legtöbb esetben – figyelembe véve a cselekménnyel összefüggésben keletkező eredményt, illetve az ehhez felhasznált eszközöket is – a Btk. 373. §-ában meghatározott csalás bűntette állapítható meg, így a cselekmény büntetőjogi értékelése kapcsán is ennek jellemzőit érdemes elsőként megvizsgálni:
– a cselekmény célzatos, az elkövető az általa megvalósított magatartással jogtalan haszonszerzésre törekszik;
– a cselekmény tettese bárki lehet;
– a bűnsegédi magatartás abban az esetben állapítható meg, ha valamely személy megteremti a tévedésbe ejtés vagy tévedésben tartás feltételeit;
– a csalás eredmény-bűncselekmény, eredményként az elkövetési magatartás következményét, vagyis a bekövetkezett kárt kell értékelni [Btk. 459. § (1) bek. 16. pont];
– az elkövetési magatartás része más személy tévedésbe ejtése vagy tévedésben tartása;
– amennyiben a kár nem annál a (természetes vagy jogi) személynél keletkezik, akivel, illetve amellyel szemben a tévedésbe ejtést vagy tévedésben tartást megvalósították, a bűncselekmény sértettje az a személy, akinél a kár ténylegesen bekövetkezett;
– a cselekmény rendbeliségét a sértettek száma határozza meg.

A cselekmény átutalásokhoz kapcsolódó (pénzügyi) jellegét a csalás tényállási elemeinek értékelésén túl elsősorban a – nyomozás során felvetődő – szituációs elemek vizsgálata alapján lehet megállapítani. Ezek tisztázása azért sem mellőzhető, mivel a hasonló cselekmények eltérő jogi minősítése – va-

lamint a bűncselekményi egység és halmazat kérdése – az eljárás nyomozati szakaszában is releváns szerepet játszik:

a) hely: az elkövetési magatartás megvalósításának helye (jelentőségét az illetékesség kapcsán fontos kiemelni)[16];
b) idő: mivel a cselekmény időben két jól elkülöníthető mozzanatra bontható, ezért az elkövetés ideje elsősorban a kísérlet és a befejezett bűncselekmény elkülönítésében játszik szerepet (befejezetté a hamis vagy megtévesztő e-mail elküldésével válik a bűncselekmény); ha az ehhez kapcsolódó pénzügyi tranzakció nem jön létre, befejezett kísérletről beszélhetünk;
c) mód: az elkövetési magatartáshoz kapcsolódó szituációs elem, amely ebben az esetben a hamis vagy megtévesztő – fizetési kötelezettségről tájékoztató vagy arra felszólító – elektronikus üzenet (e-mail) elküldését jelenti;
d) eszköz: szűkebb értelemben a hamis vagy megtévesztő tartalmú e-mail, tágabb értelmezésben pedig az a fizikai kiterjedésű informatikai eszköz vagy rendszer, amelyet ehhez felhasználnak.

Elhatárolások

Az eljárásokban a cselekmény jogi megítélése mellett fontos szerepet játszik az is, hogy a rendelkezésre álló információk birtokában a hasonló bűncselekményeket megfelelő módon lehessen egymástól elhatárolni. A BEC kapcsán ez több okból sem mellékes: egyrészt több olyan vonással is bír, amelyek miatt könnyen előfordulhat a cselekmény téves jogi megítélése, ami a hatékony hatósági fellépést is nehezíti (például a nem megfelelő elektronikus adatok lefoglalásával), másrészt nem kizárt több olyan bűncselekmény megállapítása az elkövetés kapcsán, amelyek utólag halmazatként értékelhetők. Az elhatároláshoz szükséges legfontosabb érdemi különbségeket – a teljesség igénye nélkül – a következő felsorolás tartalmazza.

Gazdasági csalás

„Aki jogtalan haszonszerzés végett színlelt gazdasági tevékenységet végez, és ezzel vagyoni hátrányt okoz, gazdasági csalást követ el.”[17]

A gazdasági csalás célzata (jogtalan haszonszerzés), illetve az elkövetési magatartással összefüggésben bekövetkező eredmény (kár) azonos ugyan, azonban

16 Az ügyészek a nyomozás, illetve a vádemelés során – általánosságban – a magatartás megvalósításának helyére alapítják az illetékességet (KF.6908/2005/7-II.).
17 Btk. 374. §

a gazdasági csalás elkövetési magatartása minden esetben valamilyen színlelt gazdasági tevékenységhez[18] kapcsolódik (ez összetettségében túlmutat a tévedésbe ejtésen vagy tévedésben tartáson). Az elhatárolás alapja az, hogy a hamis vagy megtévesztő elektronikus üzenet – hiába utal gazdasági tevékenység alapján fennálló követelésre – nem értékelhető színlelt gazdasági tevékenységként.

Információs rendszer felhasználásával elkövetett csalás[19]

„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, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő.”[20]

Az információs rendszer felhasználásával elkövetett csalás célzata szintén a jogtalan haszonszerzés, a büntetőjogi szabályozás által védeni kívánt jogi tárgyként azonban – a vagyoni viszonyok mellett – megjelenik az információs rendszerek, és a készpénzkímélő fizetés zavartalan működéséhez fűződő társadalmi érdek is. Az e-mailek felhasználásával elkövetett csalást különösen a Btk. 375. §-ában megjelenő tényállás első és második fordulatától szükséges elhatárolni. Elviekben ugyanis elképzelhető a jogtalan haszonszerzés átutaláshoz kapcsolódó olyan formája, amikor az elkövető fizetési vagy pénzügyi elszámolórendszerek befolyásolásával (például könyvelési rendszerben új kedvezményezett rögzítésével vagy a hozzá kapcsolódó számlaszám megváltoztatásával) valósítja meg az utalást.

Tiltott adatszerzés

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

c) más közlést tartalmazó zárt küldeményét felbontja vagy megszerzi, és annak tartalmát technikai eszközzel rögzíti,

---

18 Gazdasági tevékenységnek valamely tevékenység üzletszerű, illetve tartós vagy rendszeres jelleggel történő folytatása minősül, amennyiben az ellenérték elérésére irányul vagy azt eredményezi, és annak végzése független formában történik. A személyi jövedelemadóról szóló 1995. évi CXVII. tv. 3. § 46. pont.

19 A cselekmény önálló szabályozása a korábbi Btk. (1978. évi IV. tv.) 1994. évi módosításával, számítógépes csalás néven került be a szabályozási környezetbe. Az önálló szabályozás szükségességének indoka az volt, hogy az elkövetési magatartásból hiányzik a klasszikus értelemben vett tévedésbe ejtés vagy tévedésben tartás.

20 Btk. 375. §

d) elektronikus hírközlő hálózat – ideértve az információs rendszert is – útján másnak továbbított vagy azon tárolt adatot kifürkész, és az észleltet technikai eszközzel rögzíti, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő."[21]

A tiltott adatszerzés törvényi tényállása számos esetben lefedi azt a tevékenységet, amely a csalás kapcsán az elkövető előkészületi tevékenységeként is értékelhető (személyes adatot, illetve – a sértett gazdasági tevékenységével összefüggésben – gazdasági vagy üzleti titkokat derítenek fel). A tiltott adatszerzés a csalással, illetve más – az információs rendszereket sértő – bűncselekményekkel halmazatban is megállapítható.

Információs rendszer vagy adat megsértése

„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,

bűntett miatt három évig terjedő szabadságvesztéssel büntetendő."[22]

A családhoz kapcsolódó adatgyűjtő tevékenység büntetőjogilag önálló formában úgy is értékelhető, ha az elkövető által megvalósított magatartás – amennyiben tiltott adatszerzés nem valósul meg – az információs rendszerek vagy adat sérelmével jár. A Btk. 423. § (1)–(2) bekezdésében foglalt tényállás elkövetési tárgya az információs rendszer vagy adat, amely egyúttal a tiltott adatszerzéstől való elhatárolásának alapja is (az elkövetési magatartás ebben az esetben nem célzatos).

Az előbbiekben nevesített bűncselekményeken túl érdemes megjegyezni azt is, hogy az átutalásokhoz kapcsolódó csalás esetén az okozott kár a sértett pénzforgalmi számláin keletkezik. Ezzel összefüggésben az elkövető

21 Btk. 422. § (1) bekezdés c) és d) pontja
22 Btk. 423. §

szándéka nemcsak a téves tranzakció megvalósítására, hanem a tévesen utalt összeg feletti rendelkezésre is kiterjed. A kedvezményezetti számla lehet az elkövető saját nevén fenntartott számlaszám, jellemzőbb azonban, hogy a számla felett olyan – az elkövetővel kapcsolatban álló – személy diszponál, aki az arra beérkező összeg(ek) kezeléséért – anyagi vagy egyéb – ellenszolgáltatásban részesül. Abban az esetben, ha a számla felett rendelkezési jogot gyakorló személy az alapcselekmény elkövetésében nem vett részt, a számla kezelésével kapcsolatos magatartása (megőrzés, használat, kezelés, felhasználás vagy annak felhasználásával más anyagi javak beszerzése) a pénzmosás[23] bűntettének megállapítására lehet alkalmas.

A hatáskör és illetékesség vizsgálata

A BEC kapcsán folytatott belföldi nyomozások során a hatáskör és illetékesség vizsgálata az általános szabályoktól nem tér el. A hatáskör és az illetékesség vizsgálata kapcsán azonban – a büntetőeljárásról szóló törvényben[24] megfogalmazott, valamint az ehhez kapcsolódó végrehajtási rendeletben szereplő egyéb rendelkezések[25] mellett – érdemes figyelembe venni azokat a jogforrásokat is, amelyek a joggyakorlat egységesítése kapcsán relevanciával bírhatnak. Kifejezetten a csalásra vonatkoztatva, ilyen egyedi forrás a Kúria – büntetőjogi működésével összefüggésben keletkezett – BH 2009.11.317. számú határozata, amely kimondta, hogy az elkövetési magatartás (tévedésbe ejtés) kifejtésének és az eredmény (kár) bekövetkezésének helye mellett a károkozó magatartás kifejtésének a helye is megalapozhatja a bíróság illetékességét. A bíróság érvelésének hátterében az a nézőpont állt, miszerint a terhelt tevékenységének lényegi eleme a kár okozása, ennek megfelelően pedig a kár bekövetkezésének helye az illetékesség szempontjából sem lehet közömbös, holott azt a befejezett eredmény-bűncselekményeknél nem szokás vizsgálni.[26]

A nyomozások során az ilyen és hasonló rendelkezések figyelembevétele abban az esetben lehet releváns, ha az illetékesség szempontjából fontos tényállási elemek vagy körülmények vitatottak, vagy nem állapíthatók meg megnyugtató bizonyossággal.

---

23 Btk. 399. § (2) bekezdés b) pontja

24 A büntetőeljárásról szóló 1998. évi XIX. törvény.

25 A rendőrség nyomozó hatóságainak hatásköréről és illetékességéről szóló 25/2013. (VI. 24.) BM rendelet 2–3. §.

26 Forrás: www.kuriaidontesek.hu

Célszerű intézkedések

A hasonló jellegű bűncselekmények felderítése során – különös tekintettel a tényállás teljes körű tisztázására – elengedhetetlen a cselekmény alapvető feltételeinek ismerete, illetve ezzel összefüggésben azon technikai jellegű bizonyítékok beszerzése, amelyek az eljárás érdemi eredménye szempontjából elengedhetetlenek. Ahogy arról korábban már szó volt, a nyomozás sikere kapcsán kritikus szerepe van az idő múlásának, vagyis a nyomozó hatóságnak – a tudomásszerzés után – haladéktalanul meg kell tennie azokat az intézkedéseket, amelyek az elkövetéshez kapcsolódó (elsősorban elektronikus) adatok megőrzését szolgálják. E körben gondoskodni kell

– a felhasználói rendszerekhez kapcsolódó belépési és műveleti adatok lementéséről;
– az egyes felhasználók adatainak beszerzéséről (különösen a felhasználónevek, jelszavak és jogosultságok tekintetében);
– a sértett korábbi számlaforgalmi adatainak teljes körű beszerzéséről (mivel a cselekményt sok esetben több hónapos előkészítés előzi meg, illetve a folytatólagos elkövetés sem kizárt, ezért indokolt a nagyobb időtartamra vonatkozó adatgyűjtés);
– a belső informatikai rendszerről, az azt kiszolgáló eszközök, illetve az egyes munkaállomásokon (vagy a munkaállomások többségén) használt programokkal kapcsolatos állapotfelmérésről;
– az elektronikus/informatikai rendszert érintő korábbi támadások, illetve az ezekkel kapcsolatban tapasztalt következmények feljegyzéséről;
– annak megállapításáról, hogy milyen adat- és vírusvédelmi megoldásokat alkalmaztak a számítógépes hálózattal összefüggésben;
– annak megállapításáról, hogy milyen könyvelési, elszámolási vagy fizetési rendszert használnak;
– a levelezési rendszert kiszolgáló (SMTP-) szerver adatainak lementéséről (ezt a sértett mellett indokolt azon vállalkozás szerverére is kiterjeszteni, amely az e-mail alapján az utalás kedvezményezettje volt)[27].

Az informatikai rendszerekben fellelhető adatok lefoglalásával és elemzésével párhuzamosan a következő nyomozati cselekmények végrehajtása indokolt:

27 Ez azért elengedhetetlen, mert a rendszer által naplózott folyamatok (hibaüzenetek, bejövő és kimenő adatok, bejelentkezések stb.) adataiból kiszűrhetők az olyan bejelentkezések, amelyek a felhasználói adatokat felhasználva, ám kívülről történtek, vagyis – bizonyos esetben – ezekből következtetni lehet a rendszer kompromittálására.

– a kedvezményezetti számlaszámhoz kapcsolódó adatok beszerzése (számla felett rendelkező személy adatainak, az általa kezelt más számlák adatainak, a számlavezető pénzintézet, a számlanyitás időpontja, valamint a kapcsolódó szolgáltatások és a teljes számlatörténet beszerzése);
– előzménykutatást kell végezni az azonos, vagy hasonló módon elkövetett bűncselekmények kapcsán;
– azonosítani kell, hogy milyen forrásból és partnerektől érkezik egyéb jóváírás a számlára;
– a vagyonelkobzás biztosítása érdekében a bűncselekménnyel összefüggésben fel kell mérni, hogy a számlatulajdonosnak milyen nagyobb értékű ingó vagy ingatlantulajdona, vagy tartozása van (a közhiteles nyilvántartások, például gépjármű- és ingatlan-nyilvántartás, illetve a KHR adatainak beszerzése);
– az azonosított számlán vagy számlákon kezelt – a bűncselekménnyel összefüggően beérkező – összegre indokolt a zár alá vétel elrendelése;
– a számlaforgalmi adatok alapján (beérkező és kimenő utalások) azonosítani kell a számlatulajdonos pénzügyi partnereit;
– listázni kell a készpénzfelvételek helyét, összegét, továbbá be kell szerezni az ezzel kapcsolatban elérhető ATM- vagy egyéb kamerafelvételeket (ha voltak ilyenek) a közreműködő személyek azonosítása érdekében.

Egy hazai példa

A Készenléti Rendőrség Nemzeti Nyomozó Iroda 2015 júniusában eljárást indított a Btk. 373. § (1) bekezdésébe ütköző, és az (5) bekezdés a) pontja szerint minősülő, különösen jelentős kárt okozó csalás gyanúja miatt. A nyomozás elrendelésére a Robert Bosch Elektronikai Kft. feljelentése alapján került sor, mivel ismeretlen személy vagy személyek a vállalat üzleti partnere, a KCE Singapore Ltd. képviselőjének nevében elektronikus levelet juttattak el a Bosch pénzügyi ügyintézőjének, ebben arra kérték, hogy a felek között fennálló (beszállítói) szerződés alapján esedékes számlák ellenértékét a megszokottól eltérő számlaszámra utalják, mivel a cég folyamatban lévő auditálása miatt a számla kezelése bizonytalanná vált. Az ügyintéző az e-mailben szereplő tájékoztatás alapján – 2015. május 6-tól június 10-ig – összesen tíz átutalást indított a megadott számlaszámra mintegy 2,2 millió dollár értékben.

A nyomozás során a következő tényállást sikerült rekonstruálni. A csalók az e-mail elküldését megelőzően a partnercég (KCE Singapore Ltd.) belső

rendszerét feltörték, majd az onnan megszerzett adatokat felhasználva támadást intéztek a Bosch belső rendszere ellen. Ennek következtében a Bosch több alkalmazottjának egyedi adatait is sikerült megszerezniük. Az elkövetők ezek birtokában több postafiókot, például az ügyintéző által kezelt belső fiókot is lemásolták, így egyebek között a cég levelezési rendszerébe beérkező, onnan kiküldött, valamint az abban kezelt levelezéshez is hozzáfértek (az egyes partnerek eltérő anyanyelve miatt az üzenetváltás angolul folyt). A levelezés, illetve a pénzügyi tevékenység adatait felhasználva a csalók kiválasztották a KCE Singapore Ltd.-t, mivel a Boschnak e céggel – nagy értékű utalások formájában – állandó pénzügyi kapcsolata volt. Az e-mailben megadott számlát a Lengyelországban működő PEKAO Bank vezette. A beszerzett pénzügyi és egyéb adatok elemzése rámutatott, hogy a számla egy fiktív lengyel cég nevén van, illetve arra is, hogy a számla felett kizárólag a cég ügyvezetőjének van rendelkezési joga (aki az Egyesült Királyság állampolgára).

A nyomozás elrendelése után a lengyel hatóságok – jogsegélykérelem alapján – zárolták a számlán lévő összeget, így a tévesen utalt összeg jelentős részét sikerült visszaszerezni (a fennmaradó kárérték közel 690 ezer dollár). Ezzel kapcsolatban fontos megjegyezni, hogy ez nagymértékben a hatóság gyors intézkedésének, illetve a külföldi hatóságok együttműködésének volt köszönhető. Az e-mail nyomozás során történő elemzése nem hozott érdemi eredményt, azt ugyanis egy olyan kanadai cégnél regisztrálták, amelynek szerverszolgáltatóját az Amerikai Egyesült Államokban jegyezték be. Az átutalásban közreműködő alkalmazottak tanúkihallgatása, illetve a rendszeradatok és naplófájlok adatai a feljelentésben szereplő tényállást támasztották alá, ezzel összefüggésben nem vetődött fel az ügyintéző vagy más személyek szándékos közreműködésének gyanúja.

A nyomozás során megállapítható volt, hogy az e-mail feladója közvetlenül nem azonosítható, mivel az üzenet egy külső szerveren keresztül, átirányítás útján került a címzetthez. A beszerzett adatok arra utaltak, hogy az e-mail eredeti feladója feltehetően Indiában él.

Mivel a jogsegély útján beszerzett dokumentumok alapján az Egyesült Királyságban és Lengyelországban is tettek feljelentést olyan csalások miatt, amelyek összefüggésbe hozhatók az érintett lengyel céggel, ezért az érintett külföldi hatóságok által feltárt adatok beszerzése érdekében a Nemzeti Nyomozó Iroda jogsegélykérelmet terjesztett elő. Az ebben foglalt nyomozati cselekmények, illetve az egyes kérdésekre vonatkozó adatok begyűjtéséig és továbbításáig az eljárást az illetékes ügyészi szerv felfüggesztette.

Következtetés

A bűnügyi rendészet szerepe kapcsán általánosan elfogadott tézis, hogy annak célja a büntető igazságszolgáltatás előkészítése, tágabb értelmezésben pedig az állam büntetőjogi igényének biztosítása.[28] Különösen fontos ez abban a folyamatosan változó környezetben, amely egyre újabb és újabb feladatok elé állítja a nyomozó hatóságokat. A bűncselekmények mögött megbúvó emberi szándék szinte semmit sem változott ugyan az elmúlt évtizedekben, az elkövetési módszerek tekintetében mégis szembetűnő különbségek tapasztalhatók. A nyomozások egyre fontosabb része tehát az az elméleti tudás és gyakorlati ismeret, amely megfelelő reakciót jelenthet a megváltozott e környezetben. Ahogy a korábbi összegzés is mutatja, a Business E-mail Compromise és a hasonló jellegű bűncselekmények veszélye nemcsak a tömeges előfordulásban rejlik, hanem abban is, hogy a sikeres hatósági eljárásokhoz új típusú szemlélet szükséges. A BEC kapcsán tett bejelentések száma 2016-ban világszerte ötven százalékkal nőtt.[29] Ez a tendencia is azt sugallja, hogy a hatékony fellépés igénye egyre sürgetőbb. Meglátásom szerint a hasonló nyomozások sikerének záloga – a megfelelő felkészítés mellett – mindazon szereplők bevonása, akik a tudásközösség kialakítása révén hatékony fellépésre képesek. A megelőzés mellett a jövőben célszerű lehet tehát a nemzetközi együttműködés olyan formáinak fejlesztése is, amelyek elméleti (például a büntetőjogi normák uniós szintű harmonizációjával) és gyakorlati szinten (például közös nyomozó csoportok[30] felállításával) is lehetővé teszik a hatóságok közötti együttműködést.

28 Finszter Géza: Rendészetelmélet. Nemzeti Közszolgálati és Tankönyv Kiadó Zrt., Budapest, 2014, 242. o.

29 Forrás: www.ic3.gov

30 Olyan nyomozó csoportok, amelyeket az Európai Unió két vagy több tagállamának hatóságai hozhatnak létre, előre meghatározott céllal, korlátozott időtartamra.

DOI: 10.38146/BSZ.2018.7-8.6

NAGY RICHÁRD

A kibertérben elkövetett vagyon elleni bűncselekmények nyomozásának egyes kérdései

A XXI. század digitális dinamizmusa kihat a mindennapjainkra, és ha nem kellő körültekintéssel használjuk a modern kor eszközeit, nem csupán előnyökkel, hanem hátrányokkal is járhat. A digitális kor infrastruktúrájának lehetőségeit a bűnelkövetők is kihasználják, elég, ha az anonimitást lehetővé tevő rendszerekre gondolunk.

A nemzetközi szervezett bűnözés és a nemzetközi terrorizmus az internet nyújtotta lehetőségeket teljes mértében kihasználja, a tagok toborzásától, hálózat építésétől kezdve az illegális termékek (például kábítószer, tiltott pornográfia) forgalmazásán, terjesztésén át az illegális szerencsejáték szervezéséig.[1]

A számítógépes bűnözés napjainkban egyre növekvő probléma az olyan országok számára, mint például az uniós tagállamok, amelyek nagy részében az internet-infrastruktúra jól fejlett és a fizetési rendszerek online módon működnek.[2]

Kijelenthető, hogy az úgynevezett kiberbűncselekmények fenyegetéseinek szintje mára azonos a bevándorlás jellegű fenyegetés mértékével, a tevékenység globális hatása a fokozott, hatékony nemzetközi fellépést sürgeti.[3]

Az országhatárokon átívelő, határokat nem ismerő internet nyújtotta lehetőségek sok esetben kihívást jelentenek a bűnüldöző szerveknek, azonban a közös fellépés, a különféle egyezményekhez való csatlakozás lehetővé teszi az információk gyors áramlását, ezáltal a bűncselekmények eredményes felderítését.

1 Nagy Zoltán András: A szervezett bűnözői jelenségek a számítógépes hálózatokon. Belügyi Szemle, 2012/6., 108–125. o.

2 https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime

3 Molnár Dóra: Egységes európai kibertér? Az Európai Unió kiberbiztonsági politikájának fejlődése. Hadmérnök, 2017/1., 256. o.

A kiberbűncselekmények fogalmi megközelítése

A világhálón elkövethető jogsértések elleni egységes fellépés érdekében nemzetközi szinten kiemelt jelentőségű a számítástechnikai bűnözésről szóló egyezmény (úgynevezett budapesti egyezmény vagy cybercrime egyezmény)[4], amelyet a 2004. évi LXXIV. számú törvénnyel hirdettek ki.

A budapesti egyezmény a bűncselekményeket a következők szerint csoportosítja:

1. Számítástechnikai rendszer és számítástechnikai adat hozzáférhetősége, sérthetetlensége és titkossága ellen bűncselekmények
   a) jogosulatlan belépés,
   b) jogosulatlan kifürkészés,
   c) számítástechnikai adat megsértése,
   d) számítástechnikai rendszer megsértése,
   e) eszközökkel való visszaélés;
2. Számítógéppel kapcsolatos bűncselekmények
   a) számítógéppel kapcsolatos hamisítás,
   b) számítógéppel kapcsolatos csalás;
3. Számítástechnikai adatok tartalmával kapcsolatos bűncselekmények
   a) gyermekpornográfiával kapcsolatos bűncselekmények;
4. Szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekmények.

Az Európai Rendőrségi Hivatal (Europol) megállapítása[5] szerint a kiberbűnözés a bűncselekmények széles spektrumát öleli fel, amelyek közül – a teljesség igénye nélkül – a legjellemzőbbek a következők:

– online indentitáslopás;
– számítógépes csalás;
– bankkártyacsalás;
– gyermekek szexuális kizsákmányolása;
– különböző termékek illegális kereskedelme (például fegyverkereskedelem);
– online felhasználói fiókokba történő illetéktelen belépések;
– kritikus infrastruktúra és információs rendszerek ellen irányuló kibertámadások.

4 Az Európa Tanács által kidolgozott, a számítógépes bűnözés elleni egyezményt huszonhat európai és négy tengerentúli ország (Kanada, Japán, Dél-Afrika és az Egyesült Államok) képviselője írta alá 2001. november 23-án, Budapesten.

5 https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime

A kiberbűncselekmények egységes fogalmi meghatározása nehéz, mivel e bűncselekmények köre túlságosan széles, nem mindegyik sorolható be egy meghatározott fogalmi kategóriába, valamint a gyorsan kialakuló új módszerek hamar anakronisztikussá tehetnek egy fogalmi meghatározást.[6]

A kibertérben elkövetett vagyon elleni bűncselekmények meghatározása esetén pedig figyelembe kell vennünk azt is, hogy milyen cselekmények tartoznak szűkebb értelemben a vagyon elleni bűncselekmények közé. A büntető törvénykönyvről szóló 2012. évi C. törvény (Btk.) XXXVI. fejezete tartalmazza e bűncselekményeket, azonban jelentős részük nyilván nem tartozik, tartozhat a kibertérben elkövetett vagyon elleni bűncselekmények fogalmi körébe.

A kibertérben elkövetett vagyon elleni bűncselekményeknek egzakt meghatározása még nem alakult ki, a folyamatos információtechnológiai fejlődésnek és az azt követő jogi szabályozás változásának következtében nem is alakulhatott ki. Erre figyelemmel olyan taxatív felsorolás sem létezik, hogy konkrétan mely bűncselekmények tartoznak ebbe a kategóriába. A bűncselekmények széles köre követhető el ma már számítógép és az internet felhasználásával, online térben, nem beszélve arról, hogy a számítógép bizonyítási eszközök tárháza is lehet, akár egy rongálás bizonytékait is megtalálhatjuk az elkövető számítógépén, informatikai eszközein.

A Btk. vagyon elleni bűncselekményeket tartalmazó fejezetéből tulajdonképpen a csalás és az információs rendszer felhasználásával elkövetett csalás sorolható szűkebb értelemben a kibertérben elkövetett vagyon elleni bűncselekmények körébe.

Nem a Btk. vagyon elleni bűncselekményeket taglaló XXXVI. fejezetében található ugyan, azonban e kategóriába illeszthető további két bűncselekmény, egyrészt a Btk. 423. §-ában meghatározott információs rendszer vagy adat megsértése, illetve a Btk. 424. §-ában írt információs rendszer védelmét biztosító technikai intézkedés kijátszása, amelyeknek lehet akár vagyoni vonzatuk is.

Az internet megjelenésével és intenzív ütemű terjedésével egyre nagyobb teret hódít az online vásárlás, valamint a digitális (elektronikus) ügyintézés; a közösségi hálók, az azonnali üzenetküldést segítő, illetve egyéb (például vásárlást lehetővé tevő) alkalmazások átszövik a mindennapi életünket. Az e-kereskedelem és az online szolgáltatások nagy lehetőségeket rejtenek maguk-

6 Dornfeld László: A kiberbűnözés elleni küzdelem kihívásai. 2015, 29. o. blszk.sze.hu/downloadmanager/index/id/345/m/1904Elektronikus Periodika Archívum

ban, ez azonban magával vonzza a világhálón elkövetett bűncselekmények elterjedését és mértékének növekedését, amely magában foglalja a digitális térben történő vásárláshoz köthető, anyagi károkozással járó jogellenes cselekményeket is. Az elkövetők jogtalan haszonszerzési célzattal tévesztik meg az online térben vásárló fogyasztókat, kihasználva az anonimitás nyújtotta lehetőségeket.

A bűncselekmények minősítése

Jelen tanulmány elsősorban az internet útján, annak felhasználásával elkövetett vagyon elleni bűncselekmények nyomozására, illetve a nyomozások során szerzett tapasztalatokra koncentrál, azonban közismert, hogy online térben nem csupán vagyoni érdeket sértő deliktumok követhetők el.

A jogalkotó, reagálva a technikai fejlődésre, a Btk. 375. §-ában megalkotta az információs rendszer felhasználásával elkövetett csalás tényállását – amelynek törvényi tényállása részben átveszi a büntető törvénykönyvről szóló 1978. évi IV. törvény (régi Btk.) 300/C §-ában szabályozott számítástechnikai rendszer és adatok elleni bűncselekmény, valamint a régi Btk. 313/C §-ában rögzített készpénz-helyettesítő fizetési eszközzel visszaélés bűncselekmény tényállási elemeit –, s ezzel valójában egy új vagyon elleni bűncselekményt pönalizált.

Az előbbi, vagyoni érdeket is sértő jogellenes magatartásokkal szemben elsődlegesen a Btk. 373. §-ába ütköző csalás, valamint a Btk. 375. §-ába ütköző információs rendszer felhasználásával elkövetett csalás bűncselekmény gyanúja miatt lehet eljárni, amelyhez a Btk. 345. §-ába ütköző hamis magánokirat felhasználása bűncselekmény (is) kapcsolódhat.

Az e-kereskedelem körében, az online térben elkövetett bűncselekmények elkövetési módszerei rendkívül változatos képet mutatnak, a technológiai fejlődésnek megfelelően szinte naponta jelennek meg újabb és újabb módszerek. Emiatt a nyomozó hatóságoknak rendkívül nehéz lépést tartaniuk a sokszor csúcstechnológiát is felhasználó elkövetőkkel és az általuk kidolgozott elkövetési technikákkal, továbbá azokra megfelelő felderítési módszereket alkalmazni. Valamennyi bűncselekmény felderítése során egyedileg kell meghatározni a nyomozás metodikáját, ezért univerzálisan és kötelezően végrehajtandó feladatok sem határozhatók meg egyértelműen.

Az online térben elkövetett bűncselekmények csak azok észlelése után, a cselekmény rendkívül gyors elkövetéséhez viszonyítottan hosszabb idő eltel-

tével jutnak a nyomozó hatóságok tudomására.[7] A feljelentések megtételének módja nem tipizálható, azokat személyesen és elektronikus úton egyaránt eljuttatják a nyomozó hatósághoz, a postai úton küldött feljelentések e körben értelemszerűen nem jellemzők.

Tapasztalataink szerint az említett deliktumok miatt indított nyomozások tárgyát jelentős részben a Btk. 375. § (5) bekezdésébe ütköző információs rendszer felhasználásával elkövetett csalás alkotja, azonban nem elhanyagolható az internetes hirdetések feladásához köthető csalás gyanújának megállapíthatósága sem. Az internet útján elkövetett csalás jellemzően – eltérően a „klasszikus" csalástól – hirdetés feladása útján realizálódik, amikor is az egymással kapcsolatba kerülő sértett és elkövető nem feltétlenül találkozik személyesen, sok esetben csupán elektronikus levelezést vagy telefonos egyeztetést folytatnak egymással, így állapodnak meg az ügylet részleteiben. Az információs rendszer felhasználásával elkövetett, kárt okozó magatartások elsősorban vagyoni érdekeket sértő, csalásszerű magatartások, mindazonáltal ezeket a csalástól elkülönítetten indokolt szabályozni, hiszen hiányzik a klasszikus értelemben vett tévedésbe ejtés vagy tévedésben tartás. A kárt az információs rendszer jogtalan befolyásolása okozza. A törvény ennek megfelelően a vagyon elleni bűncselekmények fejezetében önálló tényállásként szabályozza az információs rendszer felhasználásával elkövetett csalást.

Az információs rendszer felhasználásával elkövetett csalás egyik leggyakoribb elkövetési magatartása a jogosulatlanul megszerzett elektronikus készpénz-helyettesítő fizetési eszköz (tipikusan bankkártyaadatok) felhasználása, ami elsősorban különböző online oldalakon történő vásárlásban manifesztálódik. E magatartás a külföldi szakirodalomban a Card Not Present Fraud (CNP) néven ismert, azaz a kártya jelenléte, annak fizikai birtoklása nélkül követik el a bűncselekményt.

A megszerzés módozatai lehetnek egyedi (alkalmi) elkövetések és tömeges adatszerzések. Utóbbira példa a tömeges adathalász telefonos üzenetek vagy e-mailek kiküldése, illetve internetfelhasználók trójai vírussal való megfertőzése. Az adathalász üzenetek lényege, hogy a címzettek részére valamely pénzintézet nevében biztonsági okokból kérik a bankkártya- vagy online bankolási adatok megadását vagy új jelszó generálását. A címzettek listája (e-mail, telefonszám) általában szintén hozzáférhető az interneten különböző adatcsomagokkal kereskedő oldalakon. A pénzintézetek és a rendőr-

7 Parti Katalin: Az internetes bűncselekmények nyomozásának egyes kérdései. In: Irk Ferenc (szerk.): Kriminológiai Tanulmányok 41. Országos Kriminológiai Intézet, Budapest, 2004, 260. o.

ség is folyamatosan felhívják a figyelmet arra, hogy a gyanús üzenetekre ne válaszoljanak, hanem azonnal jelentsék az esetet a pénzintézetnek, illetve a rendőrségnek, azonban a címzettek nagy száma alapján néhány felhasználó elég hiszékeny ahhoz, hogy mégis megadja biztonsági adatait.

A bankkártyák és egyéb készpénz-helyettesítő fizetési eszközök biztonsági adatain túlmenően egyéb adatok (például PayPal-azonosító) jogosulatlan megszerzésére is irányulhat az elkövetők magatartása haszonszerzési célzattal, bár indokolt megemlíteni, hogy a PayPal e tekintetben fokozta az ügyfélbiztonságot a tranzakciók telefonon történő megerősítése lehetőségének megadásával.

Az adatok felhasználásának végső célja mindig az, hogy az elkövető pénzhez (elsősorban készpénzhez vagy kriptovalutához) vagy egyéb értékhez jusson, így a felhasználás módozatai is ehhez igazodnak. Jellemzően internetes piactereken vásárlással, különböző telekommunikációs cégek honlapján való mobilegyenleg-feltöltéssel vagy szolgáltatásmegrendeléssel próbálnak haszonra szert tenni.

Az elkövetési magatartás egyes mozzanatait ugyanaz az elkövető is végrehajthatja, de az elkövetők gyakran elkülönülnek. A gyakorlatban elkövetői oldalon előfordulnak a bankkártyát kibocsátó pénzintézetnél dolgozó személyek is, akik hozzáférhetnek az ügyfelek bizalmas számlaadataihoz, így tehetős banki ügyfelek biztonsági adatait (például kártyaszámot, PIN-kódot) illetéktelen személyeknek kiadhatják.[8] Minden kártyaadattal összefüggő nyomozás elején a bankkártyát kibocsátó vagy elfogadói hálózatot üzemeltető pénzintézet bevonásával, illetve a sértett nyilatkoztatásával szükséges vizsgálni, hogy az adott visszaélésnek mi lehet a forrása, hol szerezték vagy szerezhették meg a biztonsági adatokat.

Az információs rendszer felhasználásával elkövetett csalás – egyebek mellett – a jogosulatlanul megszerzett készpénz-helyettesítő fizetési eszköz felhasználásával valósulhat meg, ezáltal a készpénz-helyettesítő fizetési eszközzel visszaélés az előbbi bűncselekménynek rendszerinti eszközcselekménye. A Btk. 375. § (5) bekezdésében a törvény összetett bűncselekményként törvényi egységet hozott létre, a két bűncselekmény halmazata tehát kizárt. Ennek következtében csak az előbbi bűncselekmény megállapításának van helye.[9] Ha tehát csupán az adatszerzés történt meg, de az adatok felhasználására még nem került sor, akkor a Btk. 393. § (1) bekezdésének valamelyik

8 Sinku Pál: A bankkártya, mint elkövetési tárgy büntetőjogi és eljárásjogi problémái. In: Gál István – Nagy Zoltán András (szerk.): Informatika és büntetőjog. Pécs, 2006, 164. o.
9 BH 2015.244.

fordulata szerinti készpénz-helyettesítő fizetési eszközzel visszaélés gyanúja vetődhet fel[10], míg az adatok felhasználásával a Btk. 375. §-ában meghatározott információs rendszer felhasználásával elkövetett csalás valósul meg.

A pénzintézet internetes felületén végrehajtott olyan pénzügyi műveletek azonban, amelyek a pénzintézettel megkötött Net-számlacsomagok, illetve az internetbanki szerződésben foglaltaknak megfelelnek, a számítógépes rendszer rendeltetésszerű igénybevételét jelentik, ezért az információs rendszer felhasználásával elkövetett csalás különös részi tényállását nem valósítják meg.[11]

Meg kell jegyezni, hogy ezeknek a cselekményeknek a felderítése és bizonyítása a gyakorlatban nehéz, a kártyák leolvasásának utólagos bizonyítása, a vásárlók azonosítása rendkívül problematikus, ráadásul ezekre gyakran a bűncselekmény megvalósítása után több hónappal, néha évekkel később kerül sor.[12]

A vagyon elleni bűncselekmények közül ki kell emelni a napjainkban rendkívül elterjedt, úgynevezett pszichológiai manipulációs csalást *(social engineering fraud, SEF)*. A SEF lényege, hogy a bűnelkövetők, manipulálva az embereket, bizalmas információkhoz jutnak hozzá (például jelszavak, banki adatok). A jelenség és az ahhoz kapcsolódó pénzmosás 2014-ben Magyarországon is megjelent. 2015 második felétől jelentősen megnőtt azoknak a pénzmosási bejelentéseknek a száma, amelyek alapcselekménye a külföldön elkövetett SEF típusú csalás (nemzetközi szinten általában a BEC/CEO fraud elnevezés használatos).

A jelenség azt a jellemzően gazdálkodó szervezetek (ritkábban: állami szerv, ügyvédi iroda, magánszemély) ellen elkövetett csalási módszert jelenti, amely során az elkövetők általában a célpont üzleti partnere informatikai rendszerének feltörését követően pszichológiai manipulációval ráveszik a sértett gazdálkodó szervezet pénzügyi műveletek teljesítéséért felelős alkalmazottját, hogy teljesítse részükre az üzleti partner nevében, de valójában az általuk megküldött hamis vagy hamisított fizetési utasításban foglaltak szerinti átutalást. Az informatikai rendszer feltörésével az elkövetői csoport hozzájut a két cég közötti gazdasági kapcsolatra vonatkozó minden információhoz: korábbi és aktuális szerződésekhez, szállítási levelekhez, valamint a teljes kommuni-

10 Gál István László: A pénz- és bélyegforgalom biztonsága elleni bűncselekmények. In: Polt Péter (főszerk.): Új Btk. kommentár 7. kötet. Különös Rész. Nemzeti Közszolgálati és Tankönyv Kiadó, Budapest, 2013, 220. o.

11 BH 2017.252.

12 Sinku Pál: i. m. 164. o.

kációs anyaghoz, ideértve a kapcsolattartó személyek azonosítási, elérhetőségi adatait is. Az összegyűjtött információk alapján – a legtöbb esetben – az üzleti partnernek az ügyletek lebonyolítására használt e-mail-címével szinte teljesen megegyező, az elkövetők által készített e-mail-címről küldenek a partner nevében olyan fizetési utasítást, amelyben a cégek között ténylegesen létrejött szerződéshez kapcsolódó fizetési kötelezettség teljesítését kérik a cég megváltozott fizetési számlaszámára, amely már az elkövetők ellenőrzése alatt áll.

Az említett ügyekben a bűnös úton szerzett vagyon biztosítása érdekében tett intézkedéseken túl vizsgálni kell, hogy a bűncselekmény útján szerzett vagyonnal kapcsolatban az alapcselekmény befejezettségét követően az alapcselekmény elkövetője vagy más személy végzett-e olyan további cselekményt, amely a Btk. 399–400. §-ában írt pénzmosás valamelyik alakzata szerint tényállásszerű. Ilyen esetekben a pénzmosás miatti eljárás lefolytatása elengedhetetlen.[13]

Közvetlenül nem tartozik ugyan a vagyon elleni bűncselekmények körébe, azonban közvetve számolni kell, illetve lehet kárral, illetve vagyoni hátránnyal a Btk. 423. § (1) bekezdésében szankcionált információs rendszer vagy adat megsértése bűncselekmény elkövetése esetén. E tényállás tekintetében nem szükséges a célzat vizsgálata, hiszen az nem tényállási elem, így mindegy, hogy az elkövető milyen célzattal követte el cselekményét. Leggyakoribb elkövetési magatartásként jellemzően *„érzékeny”* adatokat kísérelnek meg megszerezni az elkövetők, amelyeket a későbbiekben egyéb céljaik elérésére használhatnak fel.

Az információs rendszer felhasználásával elkövetett csalás megvalósítható adatbevitellel, adat módosításával, törlésével, hozzáférhetetlenné tételével, továbbá minden más olyan művelet elvégzésével, amely az információs rendszert befolyásolja, és ezzel kárt okoz.

A Btk. 424. §-ában büntetni rendelt információs rendszer védelmét biztosító technikai intézkedés kijátszása sui generis tényállás, mivel annak keretében a jogalkotó a Btk. 375., 422. és 423. §-ának előkészületi magatartásait pönalizálta.

13 A pénzmosás büntetőjogi aspektusaival kapcsolatban lásd részletesebben Gál István László: A pénzmosás. KJK-Kerszöv, Budapest, 2004.

Az elsődleges nyomozási cselekmények

Az elkövetett deliktum jellegéhez képest kell minden esetben dönteni a konkrét, elvégzendő nyomozási cselekmények meghatározását illetően. Indokolt esetben nyomozási tervet kell készíteni, felsorolva ebben az elvégzendő elsődleges feladatokat, amit azok végrehajtását és a beérkezett adatok, információk elemzése után bővíteni kell.

A kibertérben elkövetett bűncselekmények nyomozási tapasztalatai szerint az ilyen ügyekben jellemzően jelentősen elhúzódnak a nyomozások, elsősorban a szolgáltatókkal való nehézkes kapcsolattartás, illetve felvetődő szakkérdések miatt. Pedig az interneten megjelenő adatok, képek, fájlok stb. a „kézzelfogható" bizonyítékoknál (kinyomtatott papíralapú szöveg, ujjnyom, egyéb biometrikus jelek stb.) sokkal egyszerűbben és gyorsabban változtathatók, átalakíthatók vagy akár hozzáférhetetlenné tehetők, ez pedig csökkenti a bizonyítékok összegyűjtésére nyitva álló időt[14], így a nyomozások hatékonysága kerülhet veszélybe.

Mindenképpen kerülni kell a nyomozás indokolatlan elhúzódását. Az említett bűncselekmények gyanújával indított büntetőeljárások nyomozása során az időszerűség, ezzel párhuzamosan az eljárások hatékonyságának és eredményességének az elősegítése érdekében a következő eljárási cselekmények soron kívüli végrehajtása lehet indokolt.

– A feljelentő (sértett) mielőbbi mindenre kiterjedő, részletes kihallgatása.
– Kapcsolatfelvétel azzal a személlyel, aki az informatikai jellegű kérdésekre egzakt választ tud adni (milyen a hálózat felépítése, ki férhet hozzá a rendszer egyes elemeihez, milyen adattartalmú log fájlt készít a rendszer, azt meddig őrzi).
– Az internetszolgáltató megkeresése (az adott felhasználónevet ki milyen adatokkal, mikor, milyen IP-címről regisztrálta).
– Amennyiben egy hálózatot ért támadás, a hálózatot üzemeltető informatikustól be kell szerezni a nyomozás során elengedhetetlenül szükséges adatokat (például log adatokat).
– Meg kell keresni a hírközlési, illetve közösségi portált üzemeltető szolgáltatókat a releváns adatok beszerzése érdekében (híváslista, előfizetői adatok, IP-címek).

14 Parti Katalin: i. m. 251. o.

– Telefonszámok esetében a számhordozás ellenőrzése is indokolt annak érdekében, hogy a megkeresést a megfelelő szolgáltató részére meg lehessen küldeni.
– Az internet mint nyílt forrású hírszerzés *(Open Source Intelligence; OSINT)* kiaknázása elengedhetetlen.
– A közösségi portálok (például a Facebook) külön felületet hoztak létre a hatósági megkeresések teljesítése érdekében.
– Pénzintézeti megkeresések soron kívüli megküldése különös tekintettel az ATM biztonságikamera-felvételeinek beszerzésére (amennyiben rendelkezésre állnak a térfigyelő rendszer felvételei, azokat is be kell szerezni).
– Előzménykutatás elvégzése, tekintettel arra, hogy az internet felhasználásával elkövetett bűncselekmények esetében megalapozottan feltehető, hogy potenciálisan több személy sérelmére is megvalósul a bűncselekmény, akik feljelentése alapján több, különböző nyomozó hatóság előtt is indul büntetőeljárás.
– A későbbiekben tervezett kényszerintézkedésekre (házkutatások, lefoglalások) való megfelelő felkészüléshez szintén elengedhetetlen tudni, milyen módon, hol, milyen eszközzel valósult meg a konkrét bűncselekmény elkövetése[15].
– Házkutatás, lefoglalás foganatosítása, indokolt esetben igazságügyi szakértő bevonása az eljárásba. A házkutatás során a bizonyítási eszközök felkutatásán kívül célszerű a fellelt számítógépeken, egyéb informatikai eszközökön vizsgálatokat, adatmentést végezni[16].
– Ha az elkövetett bűncselekménynek nemzetközi vonatkozása van, indokolt a Nemzetközi Bűnügyi Együttműködési Központ (Nebek) megkeresése, és ha szükséges, jogsegélykérelem előterjesztése.

Joghatóság, hatáskör, illetékesség

A rendőrség nyomozó hatóságainak hatásköréről és illetékességéről szóló 25/2013. (VI. 24.) BM rendelet (a továbbiakban: rendelet) 3. § (1) bekezdése fő szabályként meghatározza, hogy a nyomozás lefolytatására az a nyomozó hatóság illetékes, amelynek illetékességi területén a bűncselekményt – sorozat-bűncselekmények esetén a bűncselekmények többségét – elkövették.

15 Goricsán Tamás Károly: A kényszerintézkedések végrehajtásának sajátosságai a számítástechnikai eszközök felhasználásával megvalósított bűncselekmények nyomozása körében. In: Gál István – Nagy András Zoltán (szerk.): i. m. 72. o.
16 Dornfeld László: A kibertérben elkövetett bűncselekményekkel összefüggésben alkalmazható kényszerintézkedések. Belügyi Szemle, 2018/2., 119–120. o.

A rendelet 4. § (1) bekezdése rendelkezik arról, hogy a nyomozó hatóság hatáskörét és az illetékességét hivatalból vizsgálja.

Az Országos Rendőr-főkapitányság már több alkalommal kifejtette, hogy a feljelentett cselekmény pontos jogi minősítésének, valamint a bűncselekmény elkövetési helyének a megállapítása a feljelentést fogadó nyomozó hatóság feladata. Mindaddig nem kerülhet sor az ügy áttételére, ameddig a hatáskör és az illetékesség kérdésében megalapozott döntés nem hozható. Ezzel az indokolatlan illetékességi viták is elkerülhetők.

Az internetes hirdetéssel megvalósított csalás esetén az elkövetési magatartás – a megtévesztés – akkor (és ott) valósul meg, amikor (és ahol) a sértett megnyitja a honlapon megtévesztési szándékkal közzétett eladási ajánlatot.[17] Az idézett bírósági határozat alapján általánosságban elmondható, hogy internet útján elkövetett bűncselekmények esetén a megtévesztő hirdetés sértett általi megnyitásának helye az irányadó. Nem elégséges csupán egy valótlan hirdetés megjelenítése, majd annak valaki általi olvasása, hanem az is szükséges, hogy a hirdetés alapján kialakuljon a sértettben a valóságtól eltérő téves tudattartam, amelynek következtében a sértett vagyoni joghatással járó cselekményt végez. Ez különösen az aukciós oldalakhoz kapcsolódó csalárd magatartások esetében nem elhanyagolandó szempont.

Indokolatlan azonban az, hogy ingatlan vagy egyéb nagy értékű dolog (például személygépkocsi) értékesítésére vonatkozó hirdetés kapcsán a hirdetés megnyitásának helye szerint illetékes nyomozó hatóság folytassa le a nyomozást, mivel az ingatlan megtekintése (vagy autó megtekintése és kipróbálása, az eladó által közölt információk személyes meghallgatása, valamint áralku) nélkül ritkán születik döntés annak adásvétele vonatkozásában.

A Legfőbb Ügyészség rámutatott arra, hogy amikor nem konkrétan meghatározható helyen történik a sértett bankkártyájának felhasználása (ATM-készülékből készpénzfelvétel, közvetlen vásárlás üzletben), hanem ismeretlen helyről, elektronikus úton indítják a vásárlást, és csak a célállomás helye, az online fizetési rendszer azonosítható, nem zárható ki a magyar joghatóság, illetve hogy Magyarországon (is) valósult meg tényállási elem. Ilyen feljelentések esetén a kár bekövetkezésének helye szerinti nyomozó hatóság az általános szabályokat alkalmazva rendelkezik a feljelentés kapcsán.

Az említett esetben a nyomozás során a joghatóságot körültekintően vizsgálni kell, és a Btk. 3. § (3) bekezdésében foglaltak fennállása esetén a nyomozás felügyeletét ellátó ügyészségre előterjesztést kell tenni, mivel a Btk. 3. § (2)

17 BH 2011.332.

bekezdés b) pont alapján a magyar állampolgár, a magyar jog alapján létrejött jogi személy és jogi személyiséggel nem rendelkező egyéb jogalany sérelmére nem magyar állampolgár által külföldön elkövetett, a magyar törvény szerint büntetendő cselekményre is kiterjedhet a törvény személyi hatálya.

A jogsegélyek szükségessége vonatkozásában a nyomozás felügyeletét ellátó ügyészség utasítását kell követni és annak megfelelően eljárni. Mérlegelés tárgya a jogsegély kérdése a bűncselekmény bizonyításának kérdésében azokban az esetekben, amikor arra áll rendelkezésre adat, hogy a külföldi hatóság az elkövetői kör kapcsán nyomozást folytat, illetve megalapozottan feltehető, hogy az elkövetők beazonosíthatók.

Annak megállapítására, hogy külföldi társhatóság indított-e büntetőeljárást, indokolt lehet a Nebek megkeresése.

A Btk. 423. §-ába ütköző információs rendszer vagy adat megsértése bűncselekmények nyomozása vonatkozásában felvetődött, az illetékesség kérdéskörét érintő gyakorlati problémák kapcsán a következő megállapítások tehetők. A jogsértő magatartás nem csupán levelezőrendszerekbe, hanem Facebook-profilokba történő jogosulatlan belépéssel, adatok törlésével is megvalósulhat. Alapvetően magyar információs rendszer tekintetében a szolgáltató megkeresésével tisztázható, hogy földrajzi értelemben hol üzemel az a szerver, amely a megváltoz(tat)ott adatokat tárolja, így az minősülhet a bűncselekmény joghatóságot és illetékességet megalapozó elkövetési helyének.

Ha az inkriminált szerver külföldön található (például Facebook, Yahoo stb.), a szolgáltató megkeresésével tisztázható – amennyiben nem, úgy feltehetően TOR hálózat használatára került sor –, hogy mely IP-címekhez kapcsolódik a bűncselekmény elkövetése, aminek alapján kétséget kizáróan beazonosíthatóvá válik az elkövető és a lakhelye. Ebben az esetben ez alapozhatja meg a joghatóságot, valamint az eljáró hatóság illetékességét, ugyanis a rendelet 3. § (3) bekezdése értelmében, mivel az elkövető a bűncselekményt Magyarország határain kívül követte el, a nyomozás lefolytatására – fogva tartás hiányában – az a nyomozó hatóság illetékes, amelynek illetékességi területén az elkövető utolsó ismert belföldi lakó- vagy tartózkodási helye van.

IRODALOM

Dornfeld László: A kiberbűnözés elleni küzdelem kihívásai. 2015. blszk.sze.hu/download-manager/index/id/345/m/1904Elektronikus Periodika Archívum

Dornfeld László: A kibertérben elkövetett bűncselekményekkel összefüggésben alkalmazható kényszerintézkedések. *Belügyi Szemle,* 2018/2.

Gál István László: A pénzmosás. KJK-Kerszöv, Budapest, 2004

Gál István László: A pénz- és bélyegforgalom biztonsága elleni bűncselekmények. In: **Polt Péter (főszerk.):** Új Btk. kommentár 7. kötet. Különös Rész. Nemzeti Közszolgálati és Tankönyv Kiadó, Budapest, 2013, 220. o.

Goricsán Tamás Károly: A kényszerintézkedések végrehajtásának sajátosságai a számítástechnikai eszközök felhasználásával megvalósított bűncselekmények nyomozása körében. In: **Gál István – Nagy András Zoltán (szerk.):** Informatika és büntetőjog. Pécs, 2006, 72. o.

Molnár Dóra: Egységes európai kibertér? Az Európai Unió kiberbiztonsági politikájának fejlődése. *Hadmérnök,* 2017/1.

Nagy Zoltán András: A szervezett bűnözői jelenségek a számítógépes hálózatokon. *Belügyi Szemle,* 2012/6.

Parti Katalin: Az internetes bűncselekmények nyomozásának egyes kérdései. In: **Irk Ferenc (szerk.):** Kriminológiai Tanulmányok 41. Országos Kriminológiai Intézet, Budapest, 2004, 260. o.

Sinku Pál: A bankkártya, mint elkövetési tárgy büntetőjogi és eljárásjogi problémái. In: **Gál István – Nagy Zoltán András (szerk.):** Informatika és büntetőjog. Pécs, 2006, 164. o.

DOI: 10.38146/BSZ.2018.7-8.7

MRÁZ ZOLTÁN

A digitális bizonyítási eszközök jelentősége a vagyon elleni bűncselekmények nyomozásában

A nyomozó hatóság tevékenysége számos követelménynek kell hogy megfeleljen. Elsőként említhető a szervezetszerű nyomás: az ügyet meg kell oldani, az elkövetőt fel kell deríteni. Ez természetesen az egyes eljáró nyomozók személyes szakmai ambícióját kielégítő, belső mozgatóerőként is működik. Nagyon hangsúlyos a jogszabályi környezetnek, a belső szakmai normáknak történő megfelelés. A beszerzett bizonyítási eszközöknek, a lefolytatott eljárási cselekményeknek a törvényesség és szakszerűség próbáját is ki kell állniuk. Hosszasan lehetne sorolni még azokat a külső tényezőket (például sajtóérdeklődés, jogvédő szervezetek ajánlásai), amelyek hatással vannak a nyomozásokra. Az eljáró szervek eredményességét és hatékonyságát alapvetően meghatározó elvárás a *korszerűség,* az adott társadalmi-gazdasági környezetnek való *megfelelés képessége.*

A tanulmány elsősorban a vagyon elleni bűncselekmények (betöréses lopások) aktuális kérdéseinek vizsgálatára vállalkozik, elsősorban az úgynevezett *utazó betörőkkel* kapcsolatos nyílt felderítési lehetőségek, az *informatikai környezet* adta adatszerzés kiaknázásával.

Utazóbűnözés, sorozatelkövetés

Az utazóbűnözés fogalma már évtizedekkel korábban megjelent a kriminalisztikában. *„Az utazó bűnöző az a személy, aki tudatosan – az elkövetési módszer szerves részeként – lakóhelyétől távol követ el bűncselekményt. A bűnöző e taktikával – a bűnüldöző szervek hatáskörének területi megosztottságát – ezen belül a közvetlen környezet és a helyi rendőri szervek előtti ismeretlenségét, a sorozatosan elkövetett bűncselekmények közötti összefüggések felismerésének megnehezítését próbálja kijátszani.”*[1]

1 Konczer István: A visszaeső bűnözők és a szervezett jellegű bűnözés kapcsolata a fővárosban. Belügyi Szemle, 1986/1., 10. o.

Ahogyan a tömegközlekedés korszerűsödött és egyre általánosabbá vált, az elkövetők felismerték, hogy a lebukás kockázata jelentősen csökkenthető azzal, ha a lakóhelyüktől távolabbi településeken követik el cselekményeiket, és ezek a helyszínek vonattal vagy autóbusszal könnyen megközelíthetők.

A helyszínek kiválasztásánál szempont lehet a fejlettebb gazdasági környezet (tehetősebb sértettek), a közlekedési csomópontok és a nagy átmenőforgalom nyújtotta előnyök.

A nyomozó hatóságok felderítési lehetőségeit csökkenti az is, hogy az elkövetőkről kevés adatot szolgáltatnak a helyi adatgyűjtések, az értékesítési vonal azonosítatlan marad. A személygépkocsik elterjedésével, a gyorsforgalmi utak kiépülésével, az Európai Unió schengeni határainak bővülésével az elkövetők előtt további lehetőségek nyíltak, hogy a sorozatban elkövetett, kisebb-nagyobb szervezettséget igénylő betöréseket úgy kövessék el, hogy személyük a helyi nyomozó szervek előtt szinte „láthatatlan" maradjon.

Az elmúlt időszakban Magyarországon felderített és betöréses lopás elkövetése miatt eljárás alá vont személyek között a magyar állampolgárokon kívül – akár a 2017-es évet is tekintve – több esetben cseh, szlovák és román nemzetiségű elkövetők is megjelentek. A kapcsolattartás eszköze a munkatelefon[2], a kommunikáció csatornája a hagyományos telekommunikáció mellett a például a Viber alkalmazás. A tettesek a családi házak és speciális helyszínek (például szociális otthonok) kiválasztásában internetes böngészőfelületeket, Google Maps alkalmazást használtak, a helyszínek megközelítéséhez navigációs alkalmazásokat vettek igénybe.

A nehezen tipizálható, változatos elkövetési módszerek és az elkövetők által használt *informatikai eszközök* a nyomozó hatóság részéről *szélesebb körű adatgyűjtést* és bizonyítási eljárást igényelnek. A korábbi általános metodikán felül a tanulmányomban bemutatott, újabb adatszerzési eljárási rend vált a mindennapok gyakorlatává.

Bizonyítás a büntetőeljárásban

A nyomozó hatóságok jogszabályban és belső normákban szabályozott adatgyűjtő tevékenysége a nyomozás.

„Kriminalisztikai szempontból a nyomozás *a múltbeli releváns esemény igazságnak megfelelő rekonstruálására és az eljárási célok elérésére irányu-*

2 Munkatelefon: kizárólag a bűncselekmény elkövetésének idején aktív, csak az elkövetők közötti kommunikációra használt mobilkészülék.

ló sokoldalú szellemi és gyakorlati tevékenység, amely a szükséges és lehetséges cselekvések tervszerű, tudatos, a vonatkozó eljárási szabályoknak megfelelő végrehajtása útján valósítható meg."[3]

A büntetőeljárásról szóló 1998. évi XIX. törvényben (Be.) foglaltak szerint a bizonyítási teher a vádlót, így közvetetten a nyomozó hatóságot terheli. A bizonyítás forrásai maguk a bizonyítási eszközök, így az eljárási célok eléréséhez elengedhetetlen azok törvényes és szakszerű összegyűjtése, értékelése. A Be. felsorolja a bizonyítás eszközeit (tanúvallomás, szakvélemény, tárgyi bizonyítási eszköz, okirat, a terhelt vallomása), ezek részben eljárási cselekmények, részben tárgyi bizonyítási eszközök.

Az előbbiekhez képest a 2017. évi XC. törvény (új Be.) a bizonyítás eszközeként már az elektronikus adatot is nevesíti.

A nyomozó hatóságok tevékenységének hangsúlyos része a tárgyi bizonyítási eszközök beszerzése. Ilyen bizonyíték lehet a büntetőeljárásban foglaltak szerint különösen, ami bűncselekmény

– elkövetésének nyomait hordozza;
– elkövetésével összefüggésben az elkövető nyomait hordozza;
– útján jött létre;
– elkövetéséhez eszközül szolgált; valamint
– amelyre a bűncselekményt elkövették.

A bizonyítékok beszerzésének speciális eljárása a *nyomkutatás és -rögzítés,* amelyet bizonyítási eljárás (szemle) keretein belül hajt végre a nyomozó hatóság. Az elmúlt évtizedekben az így rögzített elváltozások jellemzően lábbeli-, eszköz-, szag- és daktiloszkópiai nyomok voltak.

A büntetőeljárás során jelentőségük van a *megkereséseknek is,* amelyek során az eljáró hatóság nyílt adatgyűjtési módszerként állami és helyi önkormányzati szervet, hatóságot, köztestületet, gazdálkodó szervezetet, alapítványt, közalapítványt és egyesületet kereshet meg adatok közlése és átadása céljából. A megkeresett szervek döntően papír alapon, írásos formában *adatot, információt* (például híváslistákat, okiratokat) küldtek meg a nyomozó hatóságoknak, ezek elemzése és rendszerezése hosszadalmas volt. Az adatmennyiségek növekedésével az adatszolgáltatás már digitalizált formában, adathordozó megküldésével történik.

A megkeresés teljesítése utáni alapos szűrő-kutató munka és elemző-értékelő tevékenység az elkövető felderítéséhez, az eltulajdonított tárgyak felku-

3 Lakatos János (szerk.): Kriminalisztikai alapismeretek. Jegyzet. Rendőrtiszti Főiskola, Budapest, 2005, 24. o.

tatásához és a verziók ellenőrzéséhez szükséges információkhoz vezet. Fontos szempont a gyorsaság, így az adatgazdákkal kötött együttműködési megállapodások alapján a rendőrség jogosult a civil adatbázisokhoz való közvetlen hozzáférésre, betekintésre (Nemzeti Útdíjfizetési Szolgáltató Zrt., mobilszolgáltatók).

A betöréses lopások nyílt nyomozása klasszikusan a *helyszíni szemle* során megállapított összefüggésekre, a rögzített nyomokra épülő verziók felállításán alapult. Ezt követte a lakókörnyezetben végzett adatgyűjtés, az ismert értékesítési helyek ellenőrzése, az illetékességi területen nyilvántartott bűnözők elszámoltatása és „alibiztetése", a társadalmi kapcsolatok felkeresése, a rögzített nyomok szakértői vizsgálata.

Az elmúlt évtizedekben bekövetkező társadalmi, tudományos-technikai változások hatására a felderítés szempontjából releváns adatok egyre nagyobb százalékban *digitális alapúak,* megjelent a *digitális nyom* fogalma. Ez a folyamat jelentősen befolyásolta a bűnügyi szervek kriminalisztikai tevékenységét, így szükségessé vált a korábban bevett eljárások és gondolkodásmód megreformálása. A szemléken és házkutatásokon indokolt lett informatikus szakértő igénybevétele, és a nyomozó hatóságoknak a digitális nyomok rögzítésére és tárolására alkalmas berendezéseket is be kellett szerezniük. Fontos lett az is, hogy a nyomozók tisztában legyenek alapvető informatikai fogalmakkal (például IMEI-szám, CSV formátum, tömörített fájl).

Digitális nyomok és bizonyítási eszközök

Az informatika, a telekommunikáció robbanásszerű elterjedésével a magánszemélyek és a nyomozó hatóságok is egyre jobb műszaki hátterű eszközök birtokába jutottak. Az élet minden területén megjelent a digitalizáció, a világháló használata. Az adatgyűjtések és a bizonyítási eljárások során a nyomok és bizonyítási eszközök egy része nem kézzelfoghatóan, csak szakértői közreműködéssel volt felismerhető, rögzíthető és értelmezhető.

„Az informatika az adatok dinamikus beszerzésének, indexelésének, terjesztésének, tárolásának, keresésének, visszahívásának, megjelenítésének, integrálásának, elemzésének, szintézisének, megosztásának (magába foglalva az együttműködés elektronikus eszközeit) és publikálásának technológiai, társadalmi és szervezeti eszközeit és vonatkozásait kutatja, fejleszti és hasz-

nálja úgy, hogy az információk a társadalom minden rétegéből származó használók javára váljanak.”[4]

A nyomozás – az informatikához hasonlóan – adatok megszerzése, gyűjtése, feldolgozása. A nyomozó hatóságnak a megváltozott környezetben szervezetszerűen – de az egyének szintjén is – alkalmassá kellett válnia a számítógépekhez, telekommunikációs eszközökhöz kapcsolódó információgyűjtésre. A *digitális nyomok és bizonyítási eszközök* azonosítása és biztosítása új módszereket követelt meg, az elemzésükhöz is speciális szakértelem szükséges.

A betöréses lopások nyomozásában alkalmazott adatgyűjtő tevékenység során *leggyakrabban beszerzett digitális* bizonyítási eszközök és nyomok a következők:

– digitálisan rögzített audio-, videófájlok illetve fotók (például gépjármű-áthaladási adatok, térfigyelő kamerák felvételei);
– számítógépen és számítógépes rendszereken tárolt adatok (például e-mail-forgalom, böngészési előzmények);
– telekommunikációs eszközökön és rendszerekben tárolt adatok (például híváslisták, helymeghatározási adatok);

A betöréses lopások nyomozásának kezdeti szakaszában napjainkban elemi elvárás, hogy a nyomozó hatóság soron kívül intézkedjen a digitális nyomok beszerzésére. Ugyanilyen elvárás, hogy az elkövetők elfogása esetén foganatosított vagyon elleni kényszerintézkedések során a megfelelő gondossággal járjon el a mobilkészülékek, számítógépek felkutatására, szakszerű lefoglalására és tárolására.

Rendészeti és civil adatbázisok, az úgynevezett raszternyomozás jelentősége

Mint kifejtettem, a helyszínhez és az elkövetőhöz kapcsolódó eljárási cselekményeken túlmenően a nyomozói munka jelentős része célirányos adatgyűjtés és adatszerzés.

Az adatgyűjtések leghatékonyabb, és legkisebb energiabefektetéssel végrehajtható fajtája a civil és rendészeti adattárakban történő kutatás, adatkérés. Az együttműködési megállapodásoknak köszönhetően az adatkérések jelentős része már soron kívül, akár a rendőrségi ügyfeldolgozó rendszerből is elvégezhető. Ezekben az adattárakban a nyomozók lehetőségei a sokszorosuk-

4 President’s Committee of Advisors on Science and Technology, 2000.

ra nőnek, a feltételrendszerek megfelelő megválasztásával, az adatbázis-találatok összevetésével a lehetséges elkövetők, a felhasznált gépjárművek, a mobilkészülékek adatai kiszűrhetők.

A nemzetközi kriminalisztikai irodalom ezt a tevékenységet raszternyomozásnak nevezi, ez a terminológia a hazai gyakorlatban nem honosodott meg. A raszternyomozást *„úgy is lehet jellemezni, hogy a különböző szűrő munka megjelenítésével az adatállományok hálószerű kutatásával az egyes személyek fennakadnak a kifeszített hálón”*[5].

A nyomozások során leginkább kutatott és kutatható *civil adattárak:*

1. vezetékestelefon- és mobilszolgáltatások adatbázisa;
2. gépjármű-áthaladási és útdíjfizetési adatok;
3. pénzforgalmi információk adatbázisai;
4. térfigyelő kamerák felvételeit tároló rendszerek;
5. e-mail-forgalom, közösségi oldalak adatait tartalmazó szerverek;
6. OEP-nyilvántartások;
7. NAV-nyilvántartások;
8. önkormányzati nyilvántartások;
9. közüzemi szolgáltatók nyilvántartásai;
10. földhivatali információs rendszer (takarnet).

A felsorolás nem teljes körű, egyes nyomozásokban további információk beszerzése, adatbázisok használata lehet indokolt.

Fontos megemlíteni a Nemzeti Szakértői és Kutatóközpont Kriminalisztikai Szakértői Intézetben rendszerbe állított SICAR6 lábbeli- és gépjármű-nyom-nyilvántartó és -azonosító rendszert. Az adatbázis egyrészt a gyártók által közölt adatokból, másrészt a szakértői intézet „kódoló” munkatársa által felvitt helyszíni nyomokból épül fel.

A rendészeti nyilvántartások a következők:

1. Netzsaru/Robotzsaru Neo rendszerek;
2. Hermon körözési rendszer;
3. a Belügyminisztérium Nyilvántartások Vezetéséért Felelős Helyettes Államtitkárság nyilvántartásai (volt Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala);
4. Interpol-/Europol-nyilvántartások;
5. modusoperandi-nyilvántartás;
6. VÉDA-adatok.

5 Pilisi Fanni: Bűnügyi adatgyűjtés, különös tekintettel a raszternyomozásra. Büntetőjogi Szemle, 2012/2., 41. o.

Fontos rögzíteni azt a tényt, hogy az adattárak nem kompatibilisek egymással, és a keresés, szűrés jelentős személyi és munkaóraigénnyel jár.

Digitális bizonyítási eszközök jelentősége az utazóbűnözés felderítésében

A korábban bevezetett intézkedéseken túlmenően napjainkban a nyomozó hatóságoknak a betöréses lopások nyílt nyomozásaiban soron kívül intézkedniük kell

– a mobilszolgáltatók megkeresésére;
– a gépjármű-áthaladási adatok beszerzésére;
– helyszín közelében lévő, továbbá a település bevezető útvonalain és a benzinkutakon felszerelt kamerarendszerek felvételeinek biztosítására;
– a bűncselekmény sorozatjellegének folyamatos vizsgálatára.

A helyszíni szemle, a klasszikus adatgyűjtések érdemi adatai, valamint az adatbázisokból szerzett nagy mennyiségű digitális nyom birtokában kerülhet sor a kriminalisztikai alapkérdések alapján történő tudatos szűrésre és kutatásra. A beszerzett adatoknak és nyomoknak csak egy része válik tárgyi bizonyítási eszközzé, hiszen *„Bizonyítékot csak az képez, amely hitelt-érdemlő és a bizonyítandó tények megállapítására szolgál”*[6].

Az adatok rendszerezettsége, közérthetővé tétele és az összefüggések bemutatása miatt az elemzésekről készült jelentések szemléletességének és több adathalmaz együttes kezelésének jogos igénye is felvetődött. A rendőrségen rendszerbe állított alkalmazás több adatbázis (például cellaadatok, gépjármű-áthaladási adatok) összehasonlításával és elemzésével a bűncselekmény során használt járművekre, munkatelefonokra vonatkozó érdemi információkat áttekinthető és szemléletes módon mutatja be.

Lényeges az is, hogy az adatgyűjtés és az -elemzés is a nyomozás tényszerű információin, kriminalisztikai gondolkodáson alapuljon. A nyomozás kezdeti szakaszában a nagy tömegű adat tudatos szűrése vezethet az elkövető vagy *elkövetői csoport beazonosításához.* Az eljárások e szakaszában már megfelelő mennyiségű információhoz juthat a nyomozó hatóság ahhoz, hogy a sorozatjellegre vagy utazóbűnözésre utaló gyanúja alakuljon ki. Ez után a

6 Garamvölgyi Vilmos – Viski László (szerk.): Kriminalisztika. Belügyminisztérium Tanulmányi és Módszertani Osztálya, Budapest, 1961, 688. o.

nyomozók ismét és szintén célirányosan nagy mennyiségű adatot szereznek be a *sorozatbűncselekmény* felderítése, a *szélesítési intézkedések* keretében.

A tapasztalatok azt mutatják, hogy a nyilvántartások adatai, a digitális bizonyítási eszközök önmagukban nem mindig elegendők a büntetőjogi felelősségre vonáshoz. A kriminalisztikai azonosságok alapján leválogatott, majd *egyesített büntetőügyekben beszerzett, együttesen értékelt,* közvetett bizonyítási eszközök zárt logikai láncolata már megfelelő alap lehet. Különösen alkalmas a híváslisták, cellainformációk, gépjármű-áthaladási adatok és az azonos módszerrel elkövetett bűncselekmények helyszínén rögzített nyomok és elváltozások szakértői azonosságai alapján felépíteni a bizonyítást.

Az utazóbűnözők felderítését és a velük kapcsolatos sorozatszélesítést megalapozza az általuk *használt és lefoglalt mobileszközök,* számítógépek, adathordozók informatikus szakértői vizsgálata. Az eszközökről GPS-adatok, böngészési előzmények, a helyszínekre utaló digitális fotók biztosíthatók a szakértői tevékenység során.

A kényszerintézkedések során a nyomozó hatóság a *sértettektől eltulajdonított informatikai eszközöket,* mobilkészülékeket sok esetben sikerrel foglalja le. A kármegtérítésre irányuló büntetőjogi igény mellett a bizonyításban is fontos szerepet kap, ha az eszközök szakértői vizsgálata során kapott adatokból a sértetti kör bővítése és újabb helyszínek beazonosítása valósul meg (például a lefoglalt pendrive-on lévő családi fényképen látható utcanév újabb helyszín beazonosításához vezet).

Az internethasználat nem marad nyom nélkül. Az elkövetők *digitális lábnyomait* kutató módszereket a nemzetközi terminológia az OSINT *(Open Source Intelligence)* mozaikszóval jelöli. A nyílt forrású adatgyűjtés keretében a megfelelő informatikai alap- vagy szaktudással felvértezett nyomozó online és offline források kereső-szűrő elemzését végzi el. Az adatszerző tevékenység irányulhat közösségi oldalak, online kereskedelmi helyek, nyilvános adattárak tartalmára, segítségével a gyanúsítotti kör kapcsolatrendszere, mozgása, tevékenysége eredményesen felderíthető.

Összegzés, javaslatok

Az utazó betörők által alkalmazott módszerek fejlődtek, az általuk használt eszközök modernek, de a rendőrség bűnügyi tevékenysége meg tud felelni az *időszerűség és eredményesség követelményének* is. Megállapítható, hogy az informatika térnyerésével a nyomozó hatóságok eszköztára bővült, újabb le-

hetőségek nyíltak a felderítési pozíciók megtartására és javítására. A hatékony nyomozói munkához és felderítési eredményességhez azonban a tárgyi és személyi feltételrendszer *tudatos fejlesztése és a fejlődés fenntartása* szükséges.

Fontos megjegyezni, hogy a nyomozóknak a *digitális alapműveltség* birtokában kell lenniük ahhoz, hogy ezeket az eszközöket és eljárási módszereket eredményesen alkalmazzák a gyakorlatban. Ez évben már sor került az ORFK Bűnügyi Főigazgatóság szervezésében a *Nyomozások informatikai alapjai elnevezésű szakmai továbbképzésre.* A későbbi oktatások és képzések tematikája a gyakorlati problémák felismerésével és a szakmai igények megfogalmazásával alakul ki.

A digitális adatok lefoglalásával és tárolásával kapcsolatos *eljárási rend és oktatási program* alapjai rendelkezésre állnak, a további szakmai anyagok kidolgozása ennek alapján folyamatban van.

Felvetődött az igény egy intranetes bűnügyi felület kidolgozására is, amelyre az utazóbűnözéssel, sorozatbetörésekkel kapcsolatos bűnügyi információk és digitális adatok (például fotó-, videófájlok) feltölthetők, és visszakereshetők. Az interaktív felületnek adatvédelmi, szakmai szempontoknak egyaránt meg kell felelnie, és fontos az is, hogy az együttműködés során a *kölcsönösség és a visszajelzés* elve megvalósuljon.

IRODALOM

Belovics Ervin – Erdei Árpád (szerk.): A büntetőeljárási törvény magyarázata. HVG-ORAC Lap- és Könyvkiadó Kft., Budapest, 2018

Bócz Endre (szerk.): Kriminalisztika I–II. BM Kiadó, Budapest, 2004

Bói László: Az utazó bűnözés és a sorozatbűncselekmények kapcsolata. In: **Gaál Gyula – Hautzinger Zoltán (szerk.):** Modernkori veszélyek rendészeti aspektusai. Pécs, 2015 [Pécsi Határőr Tudományos Közlemények XVI.] http://www.pecshor.hu/periodika/XVI/boi.pdf

Garamvölgyi Vilmos – Viski László (szerk.): Kriminalisztika. Belügyminisztérium Tanulmányi és Módszertani Osztálya, Budapest, 1961

Konczer István: A visszaeső bűnözők és a szervezett jellegű bűnözés kapcsolata a fővárosban. *Belügyi Szemle,* 1986/1.

Lakatos János (szerk.): Kriminalisztikai alapismeretek. Jegyzet. Rendőrtiszti Főiskola, Budapest, 2005

Nyitrai Endre: Bűnelemzés a nyomozásban. In: **Gaál Gyula – Hautzinger Zoltán (szerk.):** Modernkori veszélyek rendészeti aspektusai. Pécs, 2015 [Pécsi Határőr Tudományos Közlemények XVI.] http://pecshor.hu/periodika/XVI/nyitrai.pdf

Nyitrai Endre: Civilnyilvántartások a nyomozásban. In: **Gaál Gyula – Hautzinger Zoltán (szerk.):** Tanulmányok a „Biztonsági kockázatok – rendészeti válaszok” című tudományos konferenciáról. Pécs, 2014 [Pécsi Határőr Tudományos Közlemények XV.] http://pecshor.hu/periodika/XV/nyitrai.pdf

Pilisi Fanni: Bűnügyi adatgyűjtés, különös tekintettel a raszternyomozásra. *Büntetőjogi Szemle,* 2012/2.

Dr. Belovics Ervin – Dr. Békés Imre – Dr. Busch Béla – Dr. Gellér Balázs – Dr. Margitán Éva – Dr. Molnár Gábor – Dr. Sinku Pál: Büntetőjog Általános rész. HVG-ORAC Lap- és Könyvkiadó Kft., Budapest, 2006

JOGSZABÁLYOK

A büntetőeljárásról szóló 1998. évi XIX. törvény (Be.)

A büntetőeljárásról szóló 2017. évi XC. törvény (új Be.)

DOI: 10.38146/BSZ.2018.7-8.8

HERÉDI ISTVÁN

Nyílt forrású adatgyűjtés az interneten

Napjainkban különleges médiafigyelem övezi az internetes közösségimédia-felületek adatkezelési gyakorlatát. A közösségimédia-szolgáltatók nyíltan hozzáférhető felületet kínálnak, amelyre regisztrálva – és alapvető személyes adatainkat megadva – szöveges vagy grafikus tartalmakat oszthatunk meg, híreket, cikkeket olvashatunk, ismerősöket gyűjthetünk, illetve figyelemmel kísérhetjük a mások által megosztott tartalmakat is.

Az okostelefonok és egyéb okoseszközök világában meg sem lepődünk azon, hogy az egyik alkalmazás használatakor közvetlenül betöltődnek egy teljesen másik alkalmazásban használt adataink, esetleg közvetlenül ezeket felhasználva regisztrálhatunk az adott szolgáltatásra. Az okoseszközök rendkívül sok kényelmi funkcióval próbálják meg kellemesebbé tenni az életünket, illetve felgyorsítani az igényelt szolgáltatások elérését – aminek felhasználói szempontból természetesen rendkívül sok előnye van, mindamellett sok járulékos, személyes adat megosztására is sor kerül ezek használatával.

Az ilyen alkalmazások, médiafelületek és szolgáltatások használata általában ingyenes, vagy relatíve alacsony előfizetési díj ellenében vehető igénybe. Természetesen ez a szolgáltatók elsődleges érdeke is, hiszen – más gazdasági társaságokhoz hasonlóan – a profitmaximalizálás egyszerű reklámelhelyezéssel nem feltétlenül kivitelezhető. A célzott marketing, illetve fogyasztói csoportok gyűjtése azonban annál több haszonnal kecsegtet. Ez csak úgy valósítható meg, ha a szolgáltatók megfelelően ismerik felhasználóikat, ez pedig minél több releváns adat begyűjtése révén lehetséges.

A begyűjtött adatok a felhasználó által is publikusan elérhetővé, megjeleníthetővé tehetők, vagy akár háttér-információként kerülhet sor a felhasználásukra a célzott marketingkommunikáció keretében. Ezt a felhasználási kört igyekszik szabályozni az új európai uniós adatvédelmi rendelet, a GDPR is, amely az utóbbi időben kiemelt médiafigyelmet kapott.

A közösségi média és egyes alkalmazások használata természetesen csak egy-egy – bár kétségkívül hatalmas – szeletét teszi ki az interneten elérhető személyes, illetve meghatározott személyekhez köthető adatoknak. Eme adatforrások felkutatása és kiaknázása a nyílt internetes adatgyűjtés elsődle-

ges célja, ami bárki számára hozzáférhető forrásokból teszi lehetővé a releváns, célszemélyhez vagy célobjektumhoz köthető információk beszerzését.

A digitális lábnyom

Az internetet böngészve hatalmas mennyiségű adatot tehetünk rendkívül gyorsan megjeleníthetővé, akár a mobileszközünkről is. A böngészési tevékenység közben azonban egy sor algoritmus dolgozik azon, hogy a megfelelő tartalom jelenjen meg az eszközünk kijelzőjén, illetve az érdeklődésünknek megfelelő további tartalmakat ajánlhasson a szolgáltató. Minden egyes kattintás vagy billentyűleütés naplózható részfolyamatként jelenik meg a szerverek oldalán, így egy egyszerű weblap megtekintése is naplóbejegyzést generál.

Az adott weboldal üzemeltetője a naplóállományok alapján tudja megállapítani, hogy mikor, milyen IP-címről, milyen eszköz és böngészőszoftver felhasználásával és milyen tartalomhoz fértek hozzá. A nyomozó hatóság tagja az ilyen szerver-naplóállományokkal elsősorban az információs rendszereket is érintő bűncselekmények esetén lefoglaláskor vagy egy-egy üzemeltetői megkeresésre adott válaszban találkozhat.

Az ilyen böngészési adatokhoz – normális esetben – csak az oldal üzemeltetője, illetve a szerverszolgáltató férhet hozzá. Azonban a „minimális internetes aktivitás” elve alapján, ha akár egyetlen egyéb e-mail-fiókkal, szolgáltatásfelhasználói hozzáféréssel vagy profillal bír, akkor valószínűsíthetően egyéb olyan online aktivitás is köthető hozzá, amely a már meglévő profilt egy másik szolgáltatáshoz társítja. Erre a legegyszerűbb példa egy webshop, hirdetési felület, hírfolyam vagy bármely alapvető szolgáltatás használata, amely e-mail-címhez kötött, így a felhasználó regisztrációkor a hozzáféréséhez társítja a levelezőfiókját.

Az online tevékenységünk során tehát egy sor olyan adat képződik, amely ha csak megfelelő hozzáférési jogosultsággal is, de visszavezethető hozzánk. Az internet böngészése során így gyakorlatilag egy digitális lábnyom keletkezik, amelyet visszakövetve a személyre vonatkozó közvetlen és közvetett információk gyűjthetők össze.

A nyílt forrású adatgyűjtés – angol szakkifejezéssel Open Source Intelligence, röviden OSINT – elsődleges célja olyan, nyílt forrásokból származó információk felkutatása és abból értékelhető adathalmazok kinyerése, ami a célszemélyre vagy célobjektumra vonatkozólag információtartalommal bír.

Az adatgyűjtés nyílt jellegére tekintettel az bárki által elvégezhető, külön szakképzettséget vagy szaktudást nem igényel, sokkal inkább gyakorlatot vagy az online szolgáltatások használatában való jártasságot feltételez.

Természetesen a nyílt forrású adatgyűjtésen elsősorban az online felkutatható adatforrásokból beszerezhető információkat értjük, hiszen a technikai fejlődés lehetővé tette ezzel a módszerrel nagy mennyiségű adat egyidejű, gyors és egyszerű beszerzését. Ennek analógiájára természetesen klasszikus offline források is kutathatók, amire a legegyszerűbb példa egy telefonkönyv. A telefonkönyvben az egyes körzetekhez – azaz településekhez – társítva személyneveket, lakcímeket, illetve az e szolgáltatási helyhez tartozó telefonszámokat találhatjuk meg. Az adatgyűjtés így csupán ennek az egy forrásnak az ismeretében is egyetlen adat – amely akár a célszemély neve, lakcíme, vagy hívószáma – vonatkozásában két további, releváns információt hordozó adat megismerését vonja maga után.

A nyílt forrású adatgyűjtés leginkább egy Rubik-kocka kirakásához hasonlítható. A különböző szolgáltatási felületeken elérhető adatokat csoportosítva, majd megfelelően rendezve felépíthető a célszemély online profilja. A személyes adatokon kívül a célszemélyhez köthető további olyan információk is elérhetők lehetnek, mint a személy ismeretségi körére, otthonára, körülményeire, családtagjaira, felhasználási szokásaira, mozgására, érdeklődési körére vonatkozó adathalmazok.

Azt, hogy egy adott személyre milyen adatok vonatkozásában kereshetünk az interneten, leginkább online aktivitása határozza meg. Ha a célszemély csupán egyetlen e-mail-fiókot használ és semmilyen más módon nem aktív az interneten, akkor valószínűleg az e-mail-fióktól eltérő források kutatása nem vezet eredményre. Ez azonban nem minden esetben igaz. Elképzelhető, hogy nem maga a célszemély osztja meg az – adatgyűjtésünk szempontjából releváns – információt, hanem valamely ismerőse, esetleg valamely harmadik fél, vagy egyszerűen nyílt módon hozzáférhető adatbázisban szerepel. A digitalizáció világában így kifejezetten ritka az az eset, amikor valakivel kapcsolatban abszolút semmilyen információforrás nem kutatható fel az interneten. Az ilyen esetek vagy tudatos és alapos távolmaradást feltételeznek, vagy a célszemély és környezete valóban nem szerepel sem szolgáltatások felhasználójaként, sem elektronikus adatbázisokban rögzített objektumként.

Az információ forrásai lehetnek tehát a nyilvános adattárak, a közösségi profilok, az online médiaszolgáltatók, a hírforrások, hirdetési felületek, saját feltöltött tartalmak, illetve összességében bármely, a tartalomszolgáltatók által rendelkezésre bocsátott felületeken nyílt módon elérhető adathalmaz is.

Felderítési lehetőségek

A nyílt forrású adatgyűjtés nem közvetlenül a kiberbűncselekmények felderítéséhez köthető járulékos cselekménysor, hiszen az a „klasszikus” bűncselekményeket elkövető személyek esetében hasonló hatékonysággal végezhető.

Az elsődleges felderítés a legtöbbször valamely kezdeti információ vagy annak töredéke birtokában kezdődik, és közvetlen célja a rendelkezésre álló információhalmaz bővítése. A folyamatban lévő eljárások bármely szakaszában bevezethető cselekménysorról beszélhetünk, hiszen akár annak kezdeti szakaszában, akár később az eljárás folyamán bármikor szükség lehet a releváns információk összegyűjtésére.

Az adatgyűjtés elsődleges célja a célszemély vagy személyi kör, esetleg más releváns személyek vagy célobjektum beazonosítása, és róluk a lehető legtöbb információ összegyűjtése. Az így beszerzett információk tekintetében megkereséssel élhetünk akár a tartalomszolgáltatók, akár a hírközlési szolgáltatók irányába, így lehetővé válik a már személyhez köthető internet-előfizetés beazonosítása is. Az elvégzett adatgyűjtési tevékenység után további nyomozati cselekmények végrehajtása válhat szükségessé, amelynek során a beszerzett információk vonatkozásában aztán újabb, illetve további adatgyűjtésbe kezdhetünk. A folyamat addig ismétlődhet, amíg az eljárásban azonosítandó valamennyi személy, esemény, objektum és körülmény beazonosítása megtörténik.

Fontos tehát kiemelni, hogy a nyílt forrású adatgyűjtés nem csupán önmagában, hanem más, „klasszikus” eljárási cselekmények egyidejű alkalmazásával érheti el hatékonyságának legmagasabb fokát, hiszen a nyílt módon beszerezhető információk tekintetében a hatóságot megilleti az a „luxus”, hogy azokat nyilvántartásokban ellenőrizze, illetve azok tekintetében megkereséssel éljen.

Az információ forrása gyakorlatilag bármi lehet. Az egyes tartalomszolgáltatók felületén elérhető keresési opciók bemutatása külön leiratot igényelne, hiszen mind a felületek számának növekedésével, mind pedig a megosztott információk és tartalmak egyre intenzívebb megjelenítésével az elérhető keresési lehetőségek száma is drasztikusan emelkedett.

A keresések legjelentősebb részét nagy valószínűséggel a személyes közösségi profilok teszik ki, hiszen az adatgyűjtések nagy része fókuszál célszemélyek beazonosítására. Az ilyen keresések végrehajtásához leginkább gyakorlat, semmint különleges szakértelem szükséges. Az elérhető keresési opciók azonban gyakran változnak, hiszen a tartalomszolgáltatók is fejlesztik szolgáltatásaik motorját, így azt rendszeresen érdemes figyelemmel kísérni.

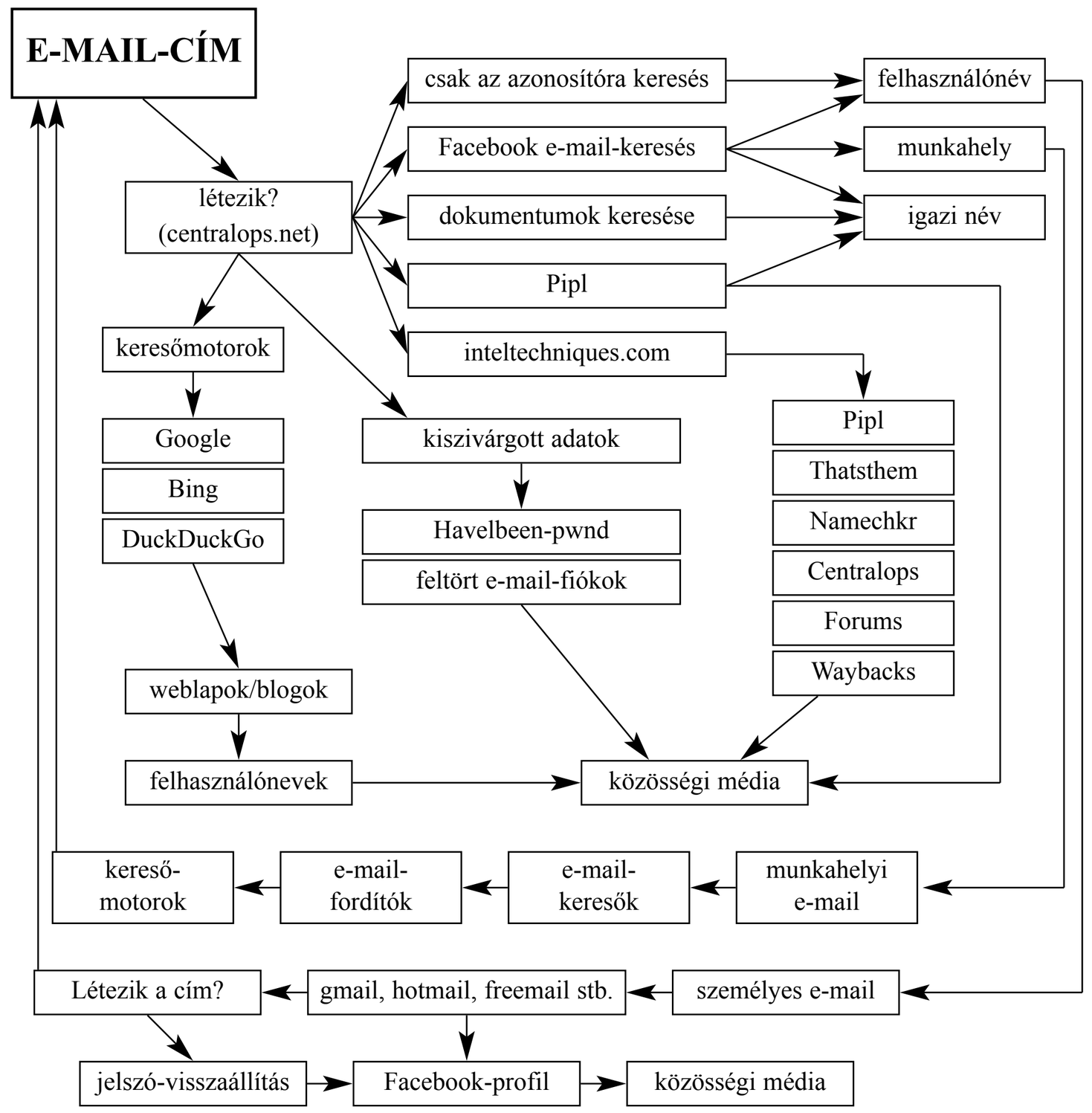
Aktív és passzív felderítés

Az interneten elérhető tartalmak többsége mára dinamikus tartalommá vált, ennek keretében nem csupán statikus jellegű weblapok jeleníthetők meg, hanem az egyes felületek akár felhasználónként is külön-külön személyre szabhatók. Ennek következménye, hogy nem ugyanazok a hirdetések jelennek meg mindenki számára a közösségi médiában – hanem leginkább az érdeklődési körünknek megfelelő, célzott reklámok –, illetve hogy az ilyen médiafelületeken különböző, személyre szabható profilokat lehet létrehozni.

A technológia előnye azonban egyben az adatgyűjtés bizonyos szempontú hátrányát is jelenti számunkra, hiszen korlátozható az elérhető, megjeleníthető tartalmak köre. Ha a célszemélynek privát vagy részben privát profilja van, csak akkor érhetjük el a lehető legtöbb informatív tartalmat, ha kapcsolatba kerülünk a profiltulajdonossal. A kapcsolatba kerülés itt jelentheti az adott profil követését, illetve akár azt is, hogy a személyt meg kell jelölnünk ismerősként. Semmi sem garantálja, hogy az elérhető tartalmak köre változni fog, nagyobb információmennyiség lesz elérhető, vagy hogy ezek közül bármelyik is releváns lesz az adatgyűjtés szempontjából. Az azonban teljesen biztos, hogy erről az aktivitásról a felhasználó értesítést kap. Ez az a lépés, ami az aktív és a passzív adatgyűjtés határát jelenti. A passzív adatgyűjtés során a célszemély nem értesül arról, hogy személye tekintetében információgyűjtés folyik. Az aktív adatgyűjtés esetében azonban már közvetlen vagy közvetett értesítéssel kell számolni, ami akár az adatgyűjtés dekonspirációjához is vezethet.

Az adatgyűjtés megkezdése előtt érdemes áttekinteni, hogy a célszemélynek milyen profiljai vannak, milyen információforrások állnak rendelkezésre, és az egyes forrásokból beszerezhető információk aktív vagy passzív tevékenységet feltételeznek-e. Külön ki kell térni arra a döntésre is, hogy a kizárólag aktív módszerrel beszerezhető információk „értéke” felülmúlja-e az adatgyűjtési tevékenység esetleges kompromittálódását.

A legegyszerűbben folyamatábrák felhasználásával lehetséges célirányos és tervezett adatgyűjtést végezni. A folyamatábra a felderítési vonatkozások és körülmények függvényében egyedileg alakítható ki – azonban természetesen léteznek általános érvényű munkafolyamatok is. Az *ábra* az e-mailek tekintetében végezhető adatgyűjtés gyakorlati algoritmusát mutatja. A vázlat megértéséhez természetesen szükséges az alapvető keresési lehetőségek ismerete is, azonban itt sokkal inkább a keresési folyamat szemléltetése a lényeg, amellyel a keresés így minden esetben mechanikus folyamat része lesz, így a hiba kockázata minimálisra csökkenthető.



Az elérhető adatok köre szolgáltatónként és felületenként is más és más, így azok kidolgozása, illetve a módszerek felderítése is külön figyelmet igényel. Fontos azonban, hogy információtartalmat nem csak a képi és szöveges adatok hordozhatnak. A célszemély megosztási szokásaiból közvetlen következtetéseket vonhatunk le egyéb online jelenlétére, online aktivitására is. Az információ hiánya is sok esetben árulkodó lehet, hiszen az használaton kívüli profilt, nem létező személyt fedő vagy egyéb konspirált tevékenységet folytató személyt feltételezhet. Az egyes adatgyűjtési lehetőségek kihasználása során így a beszerezhető információkon kívül a beszerzés, illetve a fellelhetőség körülményeire vonatkozóan is érdemes következtetéseket levonni, azzal kapcsolatban pedig verziókat felállítani.

Különös figyelemmel kell eljárni az olyan saját tartalmak esetében, mint amilyenek az egyedi weblapok, dinamikus tartalmak, átirányított hivatkozások, mivel ezek esetében az oldal üzemeltetője, illetve a tartalom tulajdonosa rendelkezhet webnaplókkal, amelyek rögzítik a beérkezett kéréseket. A legtöbb ilyen naplóállomány a digitális lábnyomnak megfelelően nemcsak az eszközről, de az internetkapcsolatról, illetve az esetleges átirányításokról is rögzít adatokat. Ilyen esetekben a kapcsolat és az eszköz elfedése tekintetében célszerű VPN-[1] vagy proxyszolgáltatások alkalmazása.

A felderítés passzív jellege csak konspirált hálózati kapcsolat, operációs rendszer, illetve online profil használatával biztosítható. Ha ezek közül az elemek közül bármelyik esetében nem gondoskodunk megfelelően online azonosságunk elfedéséről, akkor – módszertől függően eltérő mértékben ugyan, de – az adatgyűjtésünk felderíthetővé, így kompromittálóvá válik.

Adatgyűjtés a deep és dark weben

A nyílt interneten végezhető adatgyűjtés mellett egyre jelentősebb szerepet kap az internet „sötét oldalán” – a köznyelvben *dark weben* – végzett felderítőmunka. Ahhoz azonban, hogy eredményes adatgyűjtő munkát végezhessünk a *dark weben,* fontos tisztában lenni annak működési elvével, alapvetői fogalmaival is.

A nyílt internetes tartalom a *world wide web* mindenki által hozzáférhető, különböző doméncímeken elhelyezett adattartalmak összessége, amelyek megnyitásához több, ingyen hozzáférhető böngészőszoftver áll rendelkezésre. A domén- vagy IP-cím ismeretében e böngészők segítségével bármely – nyíltan hozzáférhető – felület megnyitható, tartalma böngészhető.

Ha a keresett adatokat tartalmazó weboldal pontos címét nem ismerjük, különféle keresőszolgáltatások felhasználásával rákereshetünk a számunkra releváns elemeket tartalmazó webhelyekre. A keresőmotorok olyan összetett algoritmusok, amelyek egy korábban már felállított indextartományon belül keresnek, majd a releváns kulcsszavakat tartalmazó találatokat megjelenítik a felhasználónak. Az indexelés keresőbotok felhasználásával történik, amelyek minden egyes nyíltan hozzáférhető weboldalt megnyitnak, majd az azo-

1 A VPN *(Virtual Private Network)* egy virtuálisan létrehozott privát hálózat, amelyhez kapcsolódva a hálózaton kívülre irányuló forgalom átirányítására titkosítva kerül sor az adatforgalom lebonyolításáért felelős szerveren keresztül. Használatával az internetes felületeken – normál körülmények között – csak a virtuális hálózatot kiszolgáló szerver fizikai és hálózati adatai jeleníthetők meg.

kon található összes hivatkozást tovább követve mintegy végigpásztázzák az internet teljes tartalmát.

Az egyes webhelyek rendszergazdáinak természetesen lehetőségük van arra is, hogy ezt a fajta indexelést, az oldal végigpásztázását letiltsák. Ez egyetlen fájl[2] webgyökérkönyvtárban történő elhelyezésével megoldható, és ez után a keresőbotok az oldalra jutva azt egyszerűen átugorják. Ezek az oldalak tehát a pontos domén- vagy IP-cím ismerete nélkül nem lesznek betölthetők, és az egyes keresőszolgáltatásokon keresztül sem lehetséges azokat elérni. Így alakul ki az internetes tartalmaknak az a tartománya, amelyet *deep webnek,* azaz *„sötét webnek”* neveznek.

A *dark net* bármely olyan hálózatot magában foglal, amely nem érhető el egyszerű, nyílt hozzáféréssel bárki számára. A *dark web* ezzel szemben az a webes tartalom, amely csak külön célszoftverrel – külön erre a célra programozott böngészők segítségével – nyitható meg. Az előbbi terminológiát alkalmazva a dark web a deep web része, azonban a kettő nem azonos egymással. A fogalmak elhatárolása fontos lépés, hiszen mind az adatgyűjtés technológiája, mind pedig annak módszerei különbözők a két eltérő felületen.

Az elérési útvonalak meghívására a dark web esetében nem a megszokott rendben, domén- vagy IP-cím alapján kerül sor, hanem a hivatkozások internetes felületen vagy egyéb módon történő közvetlen megosztásával.

Az ilyen tartalmak megnyitása nem lehetséges a hagyományos internetes böngészők segítségével, ahhoz külön célszoftverre van szükség. Attól függően, hogy melyik hálózathoz tartozó tartalmakat kívánjuk megnyitni, beszélhetünk egyebek között a *Tor-,* az *I2P-,* illetve a *Freenet-hálózatokról.* A legnépszerűbb felület az előzők közül a *Tor-hálózat,* amelynek megtekintéséhez, illetve webes felületének használatához a *Tor böngésző* szükséges.

A Tor böngésző egy – az ingyen hozzáférhető, szabadon szerkeszthető – Mozilla böngészőből átalakított speciális böngészőszoftver, amelynek segítségével az *.onion végződésű* hivatkozási címek megnyithatók.

Leegyszerűsítve a Tor-hálózat egy önkéntes alapon szerveződő hálózat az interneten belül, amelynek mára mintegy hétezer átirányítási pontja van. A hálózat lényege, hogy az arra kapcsolódó felhasználó egy átirányítási soron keresztül a világ különböző pontjain elhelyezkedő számítógépeken áthidalva kapcsolatát egy másik számítógépen – *a kilépési ponton* – keresztül kommunikál

---

2 A webgyökérkönyvtárban a „robots.txt” elnevezésű fájlt helyezik el, amely felsorolásszinten tartalmazza a letiltott könyvtárak jegyzékét. A fájl így információval szolgálhat arra, mely könyvtárakat nem szeretne az oldal üzemeltetője láthatóvá tenni a keresési felületeken.

az internetes szerverekkel. Az adatcsomagok a kiindulási és a kilépési pont között titkosítva közlekednek, ezáltal is növelve a felhasználó anonimitását.

A Tor-hálózat használatát egyes szolgáltatások jelzik, hiszen a Tor használata tényének elfedésére nem kerül sor. Ha a célszemély ezt a módszert használja, akkor csak az általa kilépési pontként használt számítógép IP-címét lehetséges egyszerű módszerekkel beazonosítani.

A dark weben megjeleníthető tartalmak köre teljes egészében megegyezik a nyílt internetes felületeken tapasztaltakkal, hiszen az oldalak ugyanúgy, böngészőben megjeleníthető statikus és dinamikus elemekből és objektumokból épülnek fel. A megosztott tartalmak jellege azonban eltérő. A nyílt interneten érvényesülnek az adott állami szabályozások a megjeleníthető tartalmak tekintetében, ezekre tekintettel nemzetközi egyezmények is születtek. A jogsértő tartalmakat így legtöbbször eltávolítják, illetve azok eltávolíthatók. A jogsértő tartalmak tekintetében is beszélhetünk azonban megtűrt, illetve meg nem tűrt tartalmakról. Előbbi kategóriába tartozik például a különböző hangfelvételek vagy filmek „kalózmásolatainak” megosztása, amely jogsértő tartalomnak minősül ugyan, mégsem minden esetben vonja maga után az eltávolítást és a közvetlen felelősségre vonást. A meg nem tűrt jogsértő tartalmak – amely például a gyermekek szexuális kizsákmányolásához kötődő grafikus elemek, illegális kábítószer- vagy fegyverkereskedelemhez köthető hirdetések – ellenben sokkal aktívabb ellenérzést váltanak ki, így eltávolításukról a legtöbb esetben gyorsan intézkednek. Az ilyen illegális tartalmaknak kínál kiváló lehetőséget a dark web, hiszen az oldal, illetve azok üzemeltetőinek beazonosítása jóval nehezebb, így anonim módon és relatíve egyszerűen válhatnak hozzáférhetővé a jogsértő tartalmak.

Természetesen a dark weben sem csupán jogsértő tartalmakkal találkozhatunk, azonban a relatíve szűkített felhasználószám kevéssé teszi kifizetődővé jogszerű tartalmak ilyen felületen történő elhelyezését. Az adatgyűjtés tehát itt a legtöbb esetben illegális tartalmak köré összpontosul, amely lehet akár megosztott jogsértő tartalom, akár eladásra kínált tiltott termék – amelyre a piacterek kínálnak kiváló lehetőséget. A dark weben – a felhasználók egyszerű beazonosítását elkerülendő – a legtöbb esetben nem szükséges sem a regisztrációhoz, sem az egyes tartalmak felhasználásához nyílt internetes hivatkozott tartalom, például e-mail-fiók. A felhasználó egy név–jelszó-páros megadásával egyszerűen férhet hozzá az itt elhelyezett tartalmakhoz, illetve oszthat meg saját tartalmakat.

Így a beazonosítás az ilyen felületeken nehezebb, mint a nyílt interneten. Az elsődleges cél így az adatgyűjtés nyílt internetes felületekre terelése, azaz

minél több olyan információ beszerzése, amelynek relevanciája lehet a „klasszszikus” weben. Ezek lehetnek a célszemély által használt felhasználónév, a publikus PGP-kulcsból[3] visszafejthető e-mail-cím, a profilban megadott profilkép, illetve bármilyen más megosztott tartalom. A beszerzett adatok tekintetében aztán a nyílt interneten folytatott adatgyűjtésnek megfelelően következhetnek az egyes felderítési lépések.

A beszerzett információk értékelése

Az interneten elérhető információk sok esetben nem valós tartalmúak. Az adatgyűjtés során mindenképpen figyelembe kell venni az információ és az információ forrásának megbízhatóságát is. A felderítési munka tekintetében tehát fel kell állítani a

– megbízható és megerősített;
– megbízható, de meg nem erősített;
– nem megbízható, de megerősített;
– nem megbízható és meg sem erősített; valamint
– a bizonytalan informatív tartalmú információk kategóriáját.

Az egyes információforrásokat, illetve magukat az információkat is természetesen további megbízhatósági csoportokba lehet sorolni – akár a már jól ismert kategóriák szerint –, ami alapján a besorolási kategória is szélesedik.

Az adatgyűjtés jelentéssel vagy jegyzőkönyvvel zárul, amelyben a felderítési technikákat nem, csak a már beszerzett információkat, illetve azok forrását tüntetik fel. Mind a forrás, mind pedig az információtartalom tekintetében célszerű a megbízhatósági osztályok felállítása, és az annak megfelelő besorolás elvégzése, így a jelentést kézhez kapó személy átfogó képet kaphat az adatgyűjtésről. Az értékelés soha nem szubjektív értékítélet alapján történik, hanem az objektív besorolás alapján, amelyeket összegezve a jelentés egésze is megbízhatósági jelöléssel látható el.

Az egyes információforrások, illetve az egyes célobjektumokat érintő adatgyűjtési tevékenységek akár jegyzőkönyvszerűen megalkotott jelentéssablonban is megjeleníthetők, ami rendkívül felgyorsítja a beszerzett információk későbbi feldolgozását, elemzését, illetve értékelését.

FELHASZNÁLT IRODALOM

Akhgar, Babak – Bayerl, P. Saskia – Sampson, Fraser: Open Source Intelligence Investigation. Springer, Cham, 2016

Bazzell, Michael: Open Source Intelligence Techniques. 6th ed. Amazon Fulfillment, London, 2018

DOI: 10.38146/BSZ.2018.7-8.9

HALÁSZ VIKTOR

A bitcoin működése és lefoglalása a büntetőeljárásban

„Az elektronikus pénznek egy teljességgel egyenrangú felek között működő változata lehetővé tenné a küldő és a fogadó fél közötti közvetlen online fizetést bármiféle pénzintézet közbeiktatása nélkül.”[1]

Az idézett felvetéssel indul a bitcoin működését leíró tanulmány, amely a 2008-as gazdasági világválság közepén jelent meg a világhálón.[2] A tanulmány egy olyan több évtizedes problémára adott megoldást, ami már a nyolcvanas évek óta foglalkoztatta a világ kriptográfusait: hogyan lehetséges olyan fizetési rendszert alkotni, amelyben a felek közvetlenül továbbíthatnak értéket egymásnak anélkül, hogy ehhez meg kellene bízniuk egy harmadik, közvetítő félben?[3]

A mindennapi élet online térbe áthelyeződésével szükségszerűen felvetődött a digitális értéktovábbítás mikéntjének kérdése is. Az információ digitális továbbítása során valójában ugyebár sosem az eredeti adat kerül egyik helyről a másikra, hanem csupán másolat készül az adatról az új helyen is. Az esetek túlnyomó részében ez nem okoz gondot, hiszen – például – egy kép küldése során az egyetlen cél, hogy az a fogadó félnél megjelenjen, és emellett nem bír jelentőséggel, hogy a kép egy eredeti példánya a küldő félnél továbbra is rendelkezésre áll.

Értékkel bíró dolog átruházása során azonban az értékhordozó – dolog vagy adat – többszöröződése fel sem vetődhet, hiszen akkor kétszer lehetne elkölteni. Fizikai dolgok átruházása esetén a probléma soha nem is volt jelen, hiszen egy pénzérme (bankó, kötvény, aranytömb stb.) egyszerre csak egy helyen létezhet. A javak fizikai értékhordozók nélküli, „virtuális” továbbítása esetén pedig – már az első, bankszerű intézmények ókori megjelenése óta – szükség volt egy közvetítő félre, akiben mindannyian megbíztak, és aki nyilvántartotta és hitelesen tanúsította a felek rendelkezésére álló vagyon mindenkori mértékét.

---

1 Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System. 2008, p. 1. https://bitcoin.org/bitcoin.pdf

2 A tanulmány készítőjének valódi személyazonosságára sosem derült fény; a külvilággal csupán e-mailek és online fórumok útján kommunikált, jó pár éve pedig egyáltalán nem adott életjelet magáról. Valós kilétével kapcsolatban számos nyomozás indult az évek során, lásd például Who is Satoshi Nakamoto? https://blockonomi.com/who-is-satoshi-nakamoto/

3 Andreas M. Antonopoulos: Mastering Bitcoin: Unlocking Digital Cryptocurrencies. 2015, pp. 2–3.

A XX. század vége felé a pénzintézetek – értve ezen nem csupán a bankokat, hanem minden olyan intézményt, amely bármilyen közvetítő szerepet tölt be pénzmozgások terén – tevékenysége is átvándorolt ugyan a digitális térbe, azonban a működésük alapjául szolgáló rendszer gyakorlatilag változatlan maradt.[4] Annyi történt csupán, hogy az addigi papíralapú, vaskos főkönyvek adatai átkerültek egy elektronikus szerverre, ahonnan gyorsabban lehetett ugyan elérni őket, ám a közvetítő felek iránti igény ugyanúgy nem változott.

A bitcoin éppen arra szolgáltatott megoldást, hogy az értéktovábbítás során a láncolatból kiiktassa a közvetítő pénzintézetet, ekképpen pedig olyan rendszert hozzon létre, amelyben a felek csupán egymással állnak kapcsolatban.

A pénzintézet legfőbb funkciója az elektronikus utalások lebonyolítása során, hogy hitelesen igazolja a tranzakciók érvényességét. Mivel minden tranzakciót a pénzintézet kezel, így nem fordulhat elő, hogy ugyanazt az összeget kétszer utalják el egy számláról. A pénzintézet ekképp garanciát szolgáltat a feleknek arra vonatkozóan, hogy a nekik küldött összegeket valóban meg fogják kapni.

A bitcoin esetében nincs semmilyen központi szerv, amely a tranzakciókat ellenőrizné. A pénzintézet ezen alapvető funkcióját itt az úgynevezett blokklánc biztosítja, egy világméretű, nyilvános főkönyv, amely tartalmazza az összes, valaha végrehajtott bitcointranzakciót. Legfontosabb tulajdonságai: decentralizált, anonim, maradandó és utólag megváltoztathatatlan.[5]

Kérdés, hogy ki vezeti ezt a főkönyvet. A bitcoin forradalmiságát éppen az jelenti, hogy a főkönyv vezetése nem egy a hálózat fölött őrködő intézmény felelőssége, hanem a bitcoinhasználók összessége közösen tartja nyilván, hogy kinek hány bitcoinja van éppen – ezért nevezzük ezt a rendszert decentralizáltnak.

Ha valaki szeretne bitcoincímhez jutni, csupán le kell töltenie egy bitcoinklienst[6], amellyel ez után bármilyen mennyiségben generálhat magának címeket. A címek – ha a bankok analógiáját használjuk – a bankszámlaszámoknak felelnek meg, ugyanis ezek tartják nyilván a bitcoin mennyiségét, és ezek ismerete szükséges az egymás közötti utalások lebonyolításához. Minden címhez tartozik egy úgynevezett privát kulcs is, ami egyfajta jelszóként

4 Robleh Ali – Roger Clews – James Southgate: Innovations in payment technologies and the emergence of digital currencies. Bank of England Quarterly Bulletin, vol. 54, iss. 3, 2014, p. 262.

5 Zheng Zibin – Xie Shaoan – Dai Hong-Ning – Wang Huaimin – Xiangping Chen: Blockchain Challenges and Opportunities: A Survey. International Journal of Web and Grid Services, December, 2017, p. 9.

6 Ennek ma már számos változata létezik, azonban a legelső – és azóta is folyamatosan fejlesztett – kliens a https://bitcoin.org/en/bitcoin-core/ webcímen érhető el.

fogható fel: a privát kulcs ismerete szükséges ahhoz, hogy az adott címen lévő bitcoin felett rendelkezhessünk. A bankszámlaszámokkal ellentétben a címek létrehozásához azonban semmilyen adat megadása nem szükséges (hiszen nem is lenne, aki kezelje ezeket az adatokat), így a blokkláncon rögzített tranzakciók mindegyike anonim.

A kliens letöltésével együtt letöltődik a blokklánc is az addig történt összes utalással együtt. Ha valaki új utalást akar kezdeményezni, a tranzakció adatai (milyen címről, milyen címre, mikor és mekkora mennyiségű bitcoin utalása történt) bekerülnek egy nagyobb blokkba, majd az így összegyűlt tranzakciókat átlagosan tízpercenként – egy kriptográfiai folyamat nyomán – hitelesítik, és hozzákapcsolódnak az előző blokkhoz. Ilyen módon a blokkok láncolata jön létre (innen ered a technológia elnevezése is), ami megtalálható az összes felhasználó számítógépén. Az ilyen számítógépek a csomópontok (*node*-ok).

Mivel a blokklánc értelemszerűen folyamatosan változik – új tranzakciókkal bővül –, ezért természetesen csak azok láthatják a teljes blokkláncot, akiknek a számítógépe állandó online kapcsolatban van. Ha a kapcsolat megszakad, akkor a következő indításnál az azóta keletkezett blokkokat utólag le kell tölteni. Éppen ezért azokat, akik egy adott időpillanatban az aktuálisan teljes blokkláncra rálátnak, teljes csomópontoknak (*full node*-oknak) nevezik.[7] A mindenkori teljes csomópontok hálózata felel tehát a blokklánc folyamatos nyilvántartásáért. A blokkláncban foglalt adatok elvesztése csak olyan módon fordulhatna elő, ha a világ legkülönbözőbb részein lévő teljes csomópontok mindegyike egyszerre semmisülne meg. Máskülönben, ha csupán egy csomópont is megmarad, az újonnan csatlakozó kliensek letölthetik belőle a teljes blokkláncot, újabb és újabb teljes csomópontokat hozva létre – ez garantálja tehát a blokklánc maradandóságát.

A tranzakciók említett, blokkonkénti hitelesítését nem a csomópontok végzik – ők csupán gyűjtik a tranzakciókat, majd a hitelesítés után hozzákapcsolják az elkészült blokkokat a lánc végéhez. A hitelesítés egy számításigényes művelet, amit az úgynevezett bányászok végeznek (a bányászathoz szintén nincs szükség másra, mint egy erre szolgáló program letöltésére, amely ez után automatikusan kapcsolódik a blokklánchoz, és felhasználja az adott számítógép erőforrásait). Ennek során a bányászok összegyűjtik az adott blokkban tíz perc alatt felhalmozódott – hitelesítésre váró – tranzakciókat, majd egymással ver-

7 Ezek nagyságrendje folyamatosan nyomon követhető (lásd például https://bitnodes.earn.com/). Jelenleg minden időpillanatban átlagosan tízezres nagyságrendű teljes csomópont található szerte a világon.

senyezve megoldanak egy kriptográfiai feladványt[8], amelynek bemeneti értékeit e tranzakciók adatai, illetve egy további, még az előző blokkban rögzített adatsor szolgáltatja. Az a bányász, aki elsőként számolja ki a feladvány megoldását, megszerzi a jogot, hogy az így kapott értékkel hitelesítse az adott blokkot, majd azt ellenőrzésre felajánlja a csomópontoknak. Bár a feladvány megoldása nagy számítási teljesítményt igényel, annak ellenőrzése egy pillanat alatt elvégezhető, így ha a csomópontok megfelelőnek találják a megoldást, hozzákapcsolják a blokkot a lánc végéhez, és az egész folyamat elölről indul.[9]

A kriptográfiai folyamat funkciója az, hogy szavatolja a blokkok tartalmának utólagos megváltoztathatatlanságát (másképpen fogalmazva: hogy egy korábban már elutalt bitcoint senki se „költhessen el" újra). Ahhoz ugyanis, hogy ez megtörténjen, a „csalónak" meg kell változtatnia az adott tranzakció adatait, ami szükségszerűen hatással lesz az adott blokkra vonatkozó egész feladványra, amit így újra kell számolni. Ez azonban önmagában még mindig nem elég; mivel a feladvány része az előző blokk végeredménye is, így a megváltoztatott blokk után újra kell számolni az összes többi, ez után keletkezett blokkot is. Mivel átlagosan tízpercenként keletkezik egy újabb blokk, ezért a csalónak egy egynapos tranzakció megváltoztatásához is több száz blokkot kellene egyedül megoldania. Természetesen ez nem lehetetlen (bár valószerűtlenül sok számítási kapacitást igényel), azonban a csomópontok mindig a leghosszabb láncot fogadják el érvényesnek.

Mivel a csaló szükségképpen hátrányból indul (egy múltbeli blokkot akar megváltoztatni), mindeközben pedig tízpercenként újabb blokkok is keletkeznek, ezért csak akkor lenne esélye utolérni és megelőzni az eredeti láncot, ha az összes bányász által biztosított számítási kapacitás legalább több mint a felével rendelkezne.[10]

---

8 A kriptográfiai probléma egy úgynevezett hash függvény kiszámolását jelenti. A hash függvények lényege, hogy segítségükkel bármilyen mennyiségű adatból (ami esetünkben a hitelesítendő tranzakciók és az előző blokk adatai) képezhető egy meghatározott hosszúságú, ámde rövid hash érték, ami egyfajta ujjlenyomatként is értelmezhető (ugyanazon adathalmaznak mindig ugyanaz lesz a hash értéke). A blokk hitelesítése a kiszámolt hash értékkel történik.

9 Konstantinos Christidis – Michael Devetsikiotis: Blockchains and Smart Contracts for the Internet of Things. IEEE Acces, vol. 4, 2016, pp. 2293–2294.

10 Ez pedig gyakorlatilag lehetetlen, ugyanis jelenleg nem létezik a földön olyan egységes entitás (vállalat, kormány stb.), amely ilyen méretű erőforrásokat birtokolna. A bitcoint bányászó számítógépek összes energiafogyasztása jelenleg megegyezik egy közepes méretű európai ország energiafogyasztásával (Bitcoin's Energy Consumption Can Power An Entire Country. https://www.forbes.com/sites/shermanlee/2018/04/19/bitcoins-energy-consumption-can-power-an-entire-country-but-eos-is-trying-to-fix-that/#1a5b90301bc8), így egy teljes ország az összes energiáját csak és kizárólag bitcoin-bányászatra kellene, hogy fordítsa a sikerhez.

Fontos megérteni tehát, hogy a számításigényesség nem a rendszer szükségszerű velejárója; a tranzakciók akár bányászok nélkül is blokkokba foglalhatók lennének, ha feltételeznénk, hogy a rendszer minden tagja becsületes, és soha senki nem próbálna meg utólag megváltoztatni egy már végbement utalást. Mivel azonban ilyen feltételezésre természetesen nincs mód, ezért a rendszert úgy alkották meg, hogy a blokkok elkészítését szándékosan kriptográfiai műveletek megoldásától tegye függővé, és így a csalás rendkívül energiaköltséges művelet legyen – ily módon valósul meg a blokklánc megváltoztathatatlansága.[11]

Látható, hogy a bitcoin működéséhez két összetevőre van szükség; a blokkláncot nyilvántartó teljes csomópontokra, illetve a hitelesítést nyújtó bányászokra. Jogosan vetődik fel a kérdés, mi késztet bárkit is arra, hogy a rendszer működését valamely szerepben önként fenntartsa (hiszen a bitcoint semmilyen központi szerv nem működteti, az csak a felhasználók önkéntes hozzájárulásával létezhet).

Nos, a teljes csomópont üzemeltetése nem igényel különösebb számítási kapacitást, csupán a blokklánc tárolásához szükséges tárhely és minimális sávszélesség. Ilyen módon önmagában az a tény, hogy valakinek bitcoinja van, érdekeltté teszi őt egy teljes csomópont és ezáltal a rendszer fenntartásában. Ez az elmélet a bitcoin születése után a gyakorlatban is igazolódott (hiszen a rendszer fennmaradt), azóta pedig széles körű infrastruktúra is kiépült a bitcoin köré, így egyre több és több gazdasági szereplőnek is érdekévé válik a fennmaradása.

A bányászat ugyanakkor rendkívül energiaigényes folyamat, így a számítási kapacitás önkéntes biztosítása már a bitcoin indulásakor sem lett volna reálisan elvárható. Éppen ezért a rendszert úgy alkották meg, hogy egy-egy blokk helyes megfejtését elsőként megtaláló bányászt bitcoinnal jutalmazza. Ez egyben választ ad arra a kérdésre is, hogy ki bocsátja ki a gazdasági körforgásban lévő bitcoin „érméket”; az új bitcoinokat a rendszer hozza létre, majd jutalomként kiosztja a sikeres bányászoknak, akik ez után szabadon rendelkezhetnek velük. A jutalom mértéke fix, azonban 210 ezer blokkonként (hozzávetőleg négyévente) feleződik; a rendszer indulásakor egy blokk megfejtéséért még ötven bitcoin járt, ma már csak ennek negyede (12,5 bitcoin), a következő felezés pedig 2020-ban várható.[12]

11 Todor Todorov: Bitcoin: An innovative payment method with a new type of independent currency. Trakia Journal of Sciences, vol. 15, suppl. 1, 2017, p. 164.

12 Nicolas Houry: The Bitcoin mining game. 2014, p. 2. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2407834

Ez a metódus megakadályozza, hogy a valuta értéke túlzottan inflálódjon, hiszen idővel egyre kevesebb és kevesebb új bitcoin kerül be a gazdasági körforgásba.[13] Mindemellett az utalások során az utaló feleknek egy bizonyos mértékű tranzakciós díjat is fel kell ajánlaniuk, amire szintén a blokkot hitelesítő bányász válik jogosulttá.[14]

Összefoglalva, tehát a blokklánc egy nyilvánosan elérhető, a hálózat egyenrangú tagjai által közösen vezetett (decentralizált)[15], anonim bejegyzéseket tartalmazó, maradandó és utólag megváltoztathatatlan főkönyv, amely lehetővé teszi annak nyomon követését, hogy kinek milyen mennyiségű bitcoinja van. Ha az internetre úgy tekintünk, mint az információ világméretű hálójára *(world wide web)*, akkor a blokklánc nem más, mint az értékek világméretű főkönyve.[16]

Mi is valójában egy bitcoin?

A bitcoint gyakran ábrázolják fényes érmeként, ami érthető, hiszen az emberi elmének sosem árt egy kapaszkodó, ha valamilyen absztrakt fogalmat kell elképzelnie. És bár mindenki számára nyilvánvaló, akinek legalább csak érintőlegesen is vázolták a bitcoin működését, hogy a rendszerben valódi érmék nem találhatók, a bitcoin mibenlétéről így is sok tévhit kering.

Mint korábban említettem, a bitcoinhálózatban való részvételhez szükség van egy bitcoincímre, illetve a hozzá tartozó privát kulcsra. A cím a bitcoin „tárolására” szolgál, a privát kulcs pedig a címen lévő bitcoinnal való rendelkezéshez szükséges (egyfajta jelszóként). Az előző mondatban időzőjelbe tettem a tárolás szót, ám ha egyszerűen szeretném megfogalmazni a bitcoincímek funkcióját, akkor más kifejezéssel sem jutottam volna sokkal közelebb

13 Ha pedig a csökkenés ütemét függvényként ábrázoljuk, látható, hogy az összes bitcoin mennyisége sosem haladhatja meg a 21 milliót.

14 Nicolas Houry: The economics of Bitcoin transaction fees. 2014, p. 2. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2400519

15 Megjegyzendő, hogy a decentralizáltság kapcsán az utóbbi időben egyesekben aggályok merültek fel, ugyanis a rendszer egyre nagyobb energiaigényével párhuzamosan a bányászat az otthoni felhasználóktól egyre inkább áttevődik nagyobb bányászvállalatok kezébe, amelyek így egyre nagyobb önálló szeletet hasítanak ki a bitcoin működtetéséből. Bár a rendszer ettől függetlenül még decentralizált, azonban a folyamat mindenféleképpen egyfajta centralizációnak is tekinthető. Lásd Arthur Gervais – Ghassan O. Karame – Srdjan Capkun – Vedran Capkun: Is Bitcoin a Decentralized Currency? IEEE Security & Privacy, vol. 12, no. 3, 2014, p. 56.

16 Don Tapscott – Alex Tapscott: Blockchain Revolution – How the technology behind Bitcoin is changing money, business, and the world. Penguin Canada, 2016, p. 7.

a valósághoz. A címen ugyanis valójában nem található semmilyen elektronikus érme, vagy más adatcsomag, amit bitcoinnak nevezhetnénk. Egy-egy cím csupán a bitcoinhálózaton a legelső naptól kezdve végrehajtott tranzakciók bizonyos láncolatának éppen aktuális végső eredményét rögzíti, a privát kulcs pedig lehetőséget ad az ismerőjének ezen eredmény – egy újabb tranzakcióval történő – megváltoztatására.

Téves tehát az a széles körben elterjedt nézet, amely szerint a bitcoin valamiféle számítógépes fájl vagy más elektronikus adat.[17] A bitcoin – a megtestesített érték oldaláról vizsgálva – csupán egy absztrakt fogalom, amivel bizonyos tranzakciók láncolatának végeredményét jelöljük[18], és amire nyilvánvalóan szükség van ahhoz, hogy a mindennapok során beszélni tudjunk a rendszer működéséről.

Ha pedig a birtoklás oldaláról szeretnénk megfogni a bitcoin lényegét (mit jelent az, hogy valakinek bitcoinja van?), akkor pedig a privát kulcsot kell a definíció középpontjába helyeznünk: bitcoinja annak van, aki ismer egy (nem „üres") címhez tartozó privát kulcsot, hiszen a bitcoinnal való rendelkezéshez semmi egyébre nincs szüksége. A bitcoin birtoklása tehát nem jelent mást, mint a privát kulcs tudatában lehetőséget[19] arra, hogy valahol az „éterben" létező, és emberek tízmilliói által[20] hiteles értéknyilvántartóként elfogadott főkönyvet, a blokkláncot egy apró szeletében megváltoztassuk.

Való igaz, hogy a címek és a hozzájuk tartozó privát kulcsok alapesetben a bitcoinkliens által létrehozott fájlban tárolódnak a létrehozó személy számítógépén, amelyet tárcának *(wallet)* nevezünk. Azonban mivel a privát kulcs egy egyszerű karaktersor, így a fájlból kinyerhető és bármilyen egyéb formában is tárolható (akár egy papírlapra is felírható, vagy egyszerűen meg is tanulható), és emiatt semmiképpen sem definiálhatjuk elektronikus adatként. Az elektronikus tárolás csupán egy lehetőség a számtalan tárolási mód közül – éppúgy, mint bármilyen adat esetében.

---

17 Lásd például *„A bitcoinok számítógépes fájlok, hasonlóan egy szöveges vagy mp3 fájlhoz, és éppúgy megsemmisíthetők vagy elveszthetők, mint a papírpénz."* M. Nikolei Kaplanov: Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against its Regulation. 25 Loyola Consumer Law Review, vol. 25, iss. 1, 2012, p. 116.

18 Florian Tschorsch – Björn Scheuermann: Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. IEEE Communications Surveys & Tutorials, vol. 18, iss. 3, 2016, p. 2088.

19 Szándékosan nem a „jogosultság" szót használom, ugyanis a blokkláncnak édesmindegy, hogy valaki jogosan, vagy adott esetben teljesen jogtalanul jutott hozzá egy privát kulcshoz.

20 A bitcoinhasználók száma – a rendszer anonimitásából és azon tényből kifolyólag, hogy bárki bármennyi címet használhat – nem határozható meg pontosan, azonban nagyságrendjük megbecsülhető. Lásd például How Many People Use Bitcoin? https://www.bitcoinmarketjournal.com/how-many-people-use-bitcoin/

Fontos megjegyezni továbbá, hogy a címek és a hozzájuk tartozó privát kulcsok egymással matematikai összefüggésben állnak: a privát kulcsból bármikor egy pillanat alatt kiszámolható a cím.[21] A címet jelentő karaktersor tárolása így nem is feltétlenül szükséges, illetve olyan sem fordulhat elő, hogy „elveszítjük" a privát kulcsunkhoz tartozó címet. Fordítva ez természetesen nem igaz; a címből nem számolható ki a privát kulcs, hiszen akkor bárki bármilyen címről szabadon utalhatna. Ennek tudatában tehát fokozottan is igaz, hogy a bitcoin birtoklása csupán a privát kulcs ismereteként definiálható.

A kriptovaluták tárolóeszközként történő használata

A kriptovaluták már részletezett tulajdonságai tökéletesen alkalmassá teszik őket bármilyen vagyoni érték elrejtésére, ezért a bűncselekményből származó vagyon kriptovaluták útján történő tárolása a bűnözők által is előszeretettel alkalmazott módszer.

A gyakorlati munka során gyakran szembesülünk azzal, hogy a bűnelkövetők az általuk elkövetett – bármilyen – bűncselekményből származó vagyont igyekeznek mielőbb bitcoinra váltani. Minderre az elkövetőknek jó okuk van, hiszen – mint említettem – ez után már csak arra kell figyelmet fordítaniuk, hogy a címhez tartozó privát kulcsot megőrizzék.

A privát kulcs nem más, mint egy 51 karakter (és ebben az esetben 5-ös számmal kezdődik), vagy pedig egy 52 karakter (ebben az esetben pedig az első karakter L vagy K betű) hosszúságú karaktersor, ami a következőképpen nézhet ki (bitcoin esetén):

5K9sk2YjAhA6Vvcah7oJJJenpB3SeTn9cUepihCj2GWrKwZrztE.

A bitcoincímek ezzel szemben 26–35 karakter hosszúságúak, és 1-es számmal, 3-as számmal, vagy pedig „bc1" karaktersorral kezdődhetnek. A fenti privát kulcshoz tartozó cím a következő[22]:

1C4TAcm5AADfomDCGhbssUajm5F2wjTatP.

21 A rendszer itt is hash függvényeket használ.

22 A különböző formátumok oka, hogy az ilyen címek részben különböző tulajdonságúak (például beállítható, hogy egy címhez való hozzáféréshez egyszerre több kulcs ismeretére legyen szükség), vagy pedig a bitcoinprotokoll újabb verziói alatt készültek. Ennek mélyebb technikai ismerete a jelen téma szempontjából nem fontos.

Mint már említettem, a privát kulcsból a cím bármely klienssel kiszámolható, így annak megőrzése nem is feltétlenül szükséges. Megjegyzendő továbbá, hogy más kriptovaluták esetén a címek és privát kulcsok formátuma is más, azonban ezek jellemzői is minden nehézség nélkül kideríthetők.

Alapvetően – ha az elkövető bitcoinklienst használ a cím generálásához – a privát kulcs egy fájlban tárolódik a program által létrehozott mappában (a fájl neve kliensenként eltérő, azonban általában tartalmazza a „wallet” megnevezést, a kiterjesztése pedig „.dat”, ami az egyszerű adatfájlokhoz tartozó legáltalánosabb kiterjesztés).[23] Ez után a tulajdonosa a fájlt külső adathordozóra mentheti, feltöltheti egy felhőbe, vagy bármilyen egyéb módon tárolhatja, ami elektronikus adatok tárolása esetén felvetődhet. Természetesen annak sincs akadálya, hogy a fájlt bármilyen erre szolgáló programmal titkosítsa, így pedig az elrejtésével sem kell bajlódnia, hiszen elég csupán megjegyeznie a jelszót.

Léteznek továbbá olyan titkosító eszközök – kriptográfiai algoritmusokat használó hardverkulcsok –, amelyek lehetővé teszik, hogy egy adott címről csak a hardverkulcs birtokában lehessen elutalni az összeget. A hardverkulcsot (amely egy pendrive-ra hasonlít) ilyenkor csatlakoztatni kell a számítógéphez, ugyanis a privát kulcsot a megfelelő kliens csak a hardverkulcson tárolt adatok birtokában képes kiszámolni (ezek az adatok a hardverkulcsból semmilyen módon nem nyerhetők ki). Mindez azt jelenti, hogy a cím felett csak az rendelkezhet, akinek ténylegesen is a birtokában van egy ilyen kulcs.

Az előbbi esetekben azonban az elkövetőnek vállalnia kell annak a kockázatát, hogy ha a fájlt tartalmazó összes adathordozó vagy a hardverkulcs megsemmisül, akkor elveszti a hozzáférést a kriptovalutához. Ennek kiküszöbölése érdekében megteheti, hogy a fájlból egyszerűen kinyeri a privát kulcsot, majd azt kinyomtatja, vagy más – nem elektronikus – adathordozón tárolja. Ha a kriptovalutát később el szeretné költeni, nincs más dolga, mint bármelyik kliensbe újra begépelni a privát kulcsot.

Utóbbi módszerrel azonban azt kockáztatja a tulajdonos, hogy a privát kulcsot más is megismerheti, hiszen elég, ha az adathordozóról akár csak egy fényképet készít (nem beszélve arról, hogy az adathordozó természetesen ebben az esetben is megsemmisülhet vagy elveszhet).

A legbiztosabb módja tehát a bitcoin tárolásának, ha valaki megjegyzi a privát kulcsot, majd pedig törli azt minden olyan adathordozóról, amely va-

---

23 Szigorúan véve ezt a fájlt nevezzük tárcának, ami tehát több címet is tartalmazhat (és általában tartalmaz is). A köznyelvben azonban gyakran – pontatlanul – magára a címre is tárcaként hivatkoznak, illetve az online szolgáltatóknál létrehozott fiókokat is tárcának nevezik.

laha tartalmazta. Ily módon a privát kulcs csak a bitcoin tulajdonosának tudatában létezik, és azt tőle megszerezni semmilyen módon nem lehet (ha csak ő maga el nem árulja). Természetesen egy privát kulcsot megjegyezni – ha nem is lehetetlen, ám nyilvánvalóan – nem egyszerű feladat, és az sem zárható ki, hogy valaki több év után elfelejti a pontos karaktereket. Már pedig egyetlen karakterben való tévedés is használhatatlanná teszi a kulcsot.

Mivel azonban a privát kulcs lényegében nem más, mint egy matematikai függvény eredménye, így bármilyen adatból képezhető. Mindez azt jelenti, hogy bármilyen értelmes szóból vagy mondatból is generálható privát kulcs, és ebben az esetben csupán ennek a megjegyzése szükséges.[24] Mivel egy függvény azonos bemeneti érték esetén mindig ugyanazt az eredményt adja, így a privát kulcs bármikor újragenerálható a szó ismeretében.[25]

A példaként mutatott privát kulcsot és címet a Nemzeti Közszolgálati Egyetem kifejezésből számítottam ki, így ha erre a címre utalnék bitcoint, elég lenne ennek a tényét megjegyeznem az örök időkig tartó birtoklásához. Természetesen ez azzal a kockázattal jár, hogy ha másnak is eszébe jut ugyanebből a kifejezésből privát kulcsot generálni, akkor ő is elköltheti a címen lévő bitcoint.[26] Mindazonáltal könnyű belátni, hogy megfelelő bonyolultságú kifejezés használata esetén igen kevés esély van arra, hogy más is éppen ugyanazt a kifejezést választja majd. Az ilyen típusú tárolást a köznyelvben *brain wallet*nek hívják (a kifejezés az agy és tárca szavakból áll, magyar megfelelője nincs).

Könnyen belátható, hogy ha az elkövető *brain wallet*et használ, akkor egy házkutatás nyilvánvalóan nem vezethet semmiféle eredményre, hiszen csupán az emberi tudatban létező információt semmilyen kényszerintézkedéssel nem lehet megszerezni.

---

24 Nemcsak szavakból generálható természetesen privát kulcs, hanem más adatból is (így akár zenéből, képből, vagy bármilyen egyéb adatállományból), hiszen az informatika világában minden fájl lefordítható egyesek és nullák sorozatává. Ennek azonban sok gyakorlati haszna nincs (hiszen ilyen esetben a fájlt is meg kell őrizni).

25 Mivel matematikai műveletről van szó, mindez papírral és ceruzával is kiszámolható, azonban természetesen bármikor találhatók erre szolgáló programok és weboldalak az interneten (például https://www.bitaddress.org).

26 Ha megnézzük az 1-es számból generált címhez tartozó forgalmat a blokkláncon, láthatjuk, hogy az évek során több mint ezer tranzakció kapcsán volt érintett ez a cím. Nyilvánvalóan ennek az oka, hogy a bitcoint használók milliói közül egymástól függetlenül többnek is eszébe jutott az a „nagyszerű” ötlet, hogy az 1-es számból generáljon magának bitcoincímet. Ha valaki türelmesen figyelné a fenti cím forgalmát, akkor a következő utalásnál az érkező bitcoint minden további nélkül továbbutalhatná magának.

Kimondhatjuk tehát, hogy a bitcoinnal létrejött az emberi történelem során az első olyan vagyontárolási mód, amikor is egy információ önmagában – a materiális világban megjelenő minden más dolog közrehatása nélkül – értékkel bír.

Leginkább csak ahhoz hasonlítható ez, mint amikor elásunk egy láda kincset, aminek egyedül mi ismerjük a helyét; viszont az információ értékét végső soron ebben az esetben is a kincs biztosítja, ez pedig elenyészhet, vagy megtalálhatja más. A bitcoin esetén a „kincs" a blokklánc, ami viszont elenyészni nem fog (hiszen a csomópontok képében minden pillanatban egyszerre tízezer helyen van jelen a világon, és ez a szám csak egyre nő), illetve „megtalálni" sem fogja más (ugyanis a privát kulcs címből való kiszámítása gyakorlatilag lehetetlen[27]). Mindemellett a kincsesládánkhoz csupán azon az egy helyen férhetünk újra hozzá, ahol azt elrejtettük, míg a blokklánchoz történő hozzáférés a világ bármely pontjáról lehetséges, ahol van internetkapcsolat.

Mindez azt is jelenti, hogy ha az elkövető a *brain wallet* létrehozása során nem követ el olyan hibát, ami által a privát kulcs napvilágra kerülne, akkor a nyomozó hatóság a bitcoin (vagy más kriptovaluta) megszerzése érdekében semmit sem tehet. Ilyen módon a bűnöző a bűncselekményt követően minden további nélkül megvárhatja akár azt is, hogy a cselekménye elévüljön (vagy ha elfogták, a büntetése leteljen), majd nyugodtan elköltheti az így tárolt vagyont. Mindezen idő alatt pedig a bűncselekményből származó vagyon pontos helye mindenki számára látható lesz a blokkláncon, azonban ahhoz hozzáférni senki sem tud.

Az említett körülmények egyértelműen olyan új helyzet elé állíthatják majd a nyomozó hatóságokat, amire korábban sosem volt példa a büntetőeljárások során.

A bitcoin lefoglalása

A következőkben az kívánom bemutatni, hogy ha az eljárás folyamán bármely okból szükségessé válik az elkövető birtokában lévő bitcoin lefoglalása, akkor ez milyen gyakorlati lépések alapján tehető meg. Bár a címben csupán a lefoglalásról teszek említést, természetesen az elképzelt szituáció egy házkutatással egybekötött lefoglalásra vonatkozik, nem pedig arra az esetre, ha az elkövető önként „adná át" a nyomozó hatóság tagjának a kriptovalutát.

27 Ignacio Mas – David Lee Kuo Chuen: Bitcoin Like Protocols and Innovations. David Lee Kuo Chuen (ed.): Handbook of Digital Currency. Academic Press, 2015, p. 420.

Ennek okán a lépések részletezésekor kitérek a házkutatáskor szem előtt tartandó elvekre is.

Végül fel kívánom hívni a figyelmet arra, hogy álláspontom szerint a bitcoin megfelelő tárolásához a nyomozó hatóság részéről központi szintű lépések meghozatalára – egészen pontosan egy megfelelően beállított hatósági tárca létrehozatalára – van szükség, ez azonban csupán hosszabb folyamat eredménye lehet. A lefoglalás azonban nyilvánvalóan nem képzelhető el anélkül, hogy a lefoglalt bitcoint valamilyen módon ne tárolnánk. A lefoglalás lépéseit leíró részt ezért olyan szellemben készítettem el, hogy annak alkalmazásával egy nyomozó akár már holnap képes legyen bitcoint lefoglalni, és a *körülményekhez képest* megfelelően tárolni. Optimálisnak viszont értelemszerűen azt tartanám, ha egy jövőbeli időpontban megvalósulnának a tárolás kapcsán általam indokoltnak vélt lépések, és onnantól fogva a nyomozás során lefoglalt bitcoin egy központi tárcába kerülne.

A bitcoin lefoglalásának lépései

Az eddig kifejtettek alapján nyilvánvaló, hogy bitcoin esetében zár alá vételnek és hasonló jellegű intézkedéseknek még elméletben sincs értelme, ugyanis nincs semmilyen szerv, amely végrehajthatná a hatóság határozatát. A bitcoin feletti rendelkezési jogot kizárólag a tulajdonossal szemben közvetlenül alkalmazott kényszerintézkedéssel, mégpedig egy kikényszerített tranzakcióval lehet felfüggeszteni, amely során a lefoglalandó bitcoint a tulajdonos címéről a hatóság címére utaljuk.

A következőkben összefoglalom azokat a főbb lépéseket, amelyeket a nyomozó hatóság tagjának ezen eljárás során ajánlatos végrehajtania. Annak érdekében, hogy mindez valóban alkalmazható is legyen a gyakorlatban, a lépéseket nem csupán elméleti jelleggel, hanem egy konkrét bitcoinkliens alkalmazásán keresztül mutatom be.

Megismételvén a korábban elmondottakat: ha a hatóságnak már a rendelkezésére áll egy központi cím, akkor a lefoglaláshoz szükséges cím létrehozására vonatkozó lépések értelemszerűen kihagyhatók.

A lefoglalás – a tranzakció kikényszerítése – a következő nyolc lépésben hajtható végre. Az első három lépés a lefoglalás előkészületének, míg a többi a tényleges végrehajtásának tekinthető.

– A tranzakcióhoz szükséges számítógép előkészítése.
– A fogadásra szolgáló cím elkészítése.
– A fogadásra szolgáló címhez tartozó privát kulcs biztonságba helyezése.

– A lefoglalást szenvedő privát kulcsának felkutatása.
– A privát kulcsok kinyerése a tárcából.
– A privát kulcsok importálása a tranzakcióhoz használandó számítógépre.
– A tranzakció végrehajtása.
– A tranzakció ellenőrzése.

A tranzakcióhoz szükséges számítógép előkészítése

Az első lépésben elő kell készítenünk egy olyan hordozható, internetkapcsolattal bíró számítógépet, amellyel a kikényszerített utalást végre fogjuk tudni hajtani a helyszínen.

Bár a tranzakció elvileg végrehajtható az eljárás alá vont számítógépének használatával is, azonban ez könnyen akadályokba ütközhet. Elképzelhető, hogy a kérdéses számítógépen nincs internetkapcsolat, vagy jelszóval védett bitcoinklienst telepítettek rá, esetleg a privát kulcsra végül csupán egy egyszerű szöveges fájlban vagy egy papírlapon rögzítve bukkanunk. Utóbbi esetekben nem is áll majd rendelkezésünkre megfelelő kliens vagy számítógép.

Az előkészítés során telepíteni kell egy bitcoinklienst a használni kívánt számítógépre. Bár ebből többfajta is létezik, azonban a lefoglalás szempontjából megfelelő kliensnek jellemző tulajdonságai kell hogy legyenek.

A kliensnek értelemszerűen ismernie kell a teljes blokkláncot, hiszen máskülönben nem tudná ellenőrizni a tranzakciók hitelességét. A teljes blokklánc mérete azonban több száz gigabyte – ami természetesen folyamatosan növekszik –, így letöltése egyrészről hosszabb ideig is eltarthat, másrészről pedig minden indításnál újabb frissítésre van szükség. E problémák kiküszöbölése érdekében ajánlatos olyan klienst használni, amely nem tölti le a teljes blokkláncot, hanem annak adatait egy olyan távoli szerver útján ellenőrzi, amelyen az már rendelkezésre áll. Mindemellett természetesen a kliensnek megbízható forrásból is kell származnia, máskülönben akár adathalász vírust is tartalmazhat.

Az említett feltételeknek megfelelő kliensnek tekinthető az Electrum, amely a https://electrum.org/#download címen érhető el. Az említett címen az Electrum több verziója is megtalálható. Ezek közül – feltételezve természetesen, hogy Windowst használunk – a *Portable version* használható a legegyszerűbben, ugyanis ez nem igényel semmiféle telepítést.

A letöltés után a programban létre kell majd hoznunk egy tárcát, amelybe később a lefoglalást szenvedőtől megszerzett privát kulcsokat importáljuk a tranzakció végrehajtásához (ezt részletesen *A tranzakció végrehajtása* alcím

alatti részben mutatom be). A lefoglaláshoz azonban egy másik számítógépen létre kell hoznunk egy másik tárcát is, amelyben majd az utalás fogadásához szükséges címet generáljuk. Mivel mindkét tárca létrehozásának lépései azonosak, ezért ezt csupán egyszer (e második tárca kapcsán) mutatom be a következő pontokban.

A fogadásra szolgáló cím elkészítése

A lefoglaláshoz tehát létre kell hoznunk egy másik tárcát is, amely majd tartalmazza azt a hatósági címet, amelyre a lefoglalandó bitcoint utalni szándékozunk. Bár ilyen címet az előző pontban említett tárcával együtt is létrehozhatnánk, biztonsági megfontolásból azonban ez mégsem indokolt.

A tranzakció végrehajtásához mindenképpen internetkapcsolatra van ugyanis szükség, így ha a hatósági címhez szükséges tárcát ugyanazon a számítógépen készítenénk el, fennállna a veszélye, hogy a számítógépen lévő esetleges adathalász vírusok az újonnan létrehozott privát kulcsokat megszerzik.[28]

Az előbbiek kizárása érdekében a bitcoinklienst fel kell telepíteni egy internetre nem rákötött számítógépre is, és a bitcoinok fogadására szolgáló tárcát ezen kell létrehozni.

A tárcában lévő címek és a hozzájuk tartozó privát kulcsok elkészítéséhez nincs szükség internetkapcsolatra, hiszen ezek csupán matematikai műveletek eredményei. Az így alkotott címek természetesen nem is fognak megjelenni a blokkláncban mindaddig, amíg egy tranzakció során nem adjuk meg azokat az utalás céljaként. Bár elviekben akár előfordulhatna, hogy időközben véletlenül valaki más is ugyanazt a címet generálja magának, ám a karaktersor bonyolultsága miatt ez gyakorlatilag kizárt, a lehetséges bitcoincímek száma 2^{160} lehet.[29] Azonban ezzel együtt is, a blokkláncot nyilvántartó oldalakon[30] közvetlenül a tranzakció megkezdése előtt bármikor ellenőrizhetjük, hogy az adott cím nem szerepel-e már véletlenül a blokkláncban.

Ha az eljárás későbbi szakaszában a lefoglalt bitcoint tovább kell utalnunk – vagy a lefoglalás megszüntetése miatt, vagy mert az eljárás befejeztével az állam tulajdonába kerül és értékesíteni kell –, akkor a tárcát elég csupán közvetlenül az utalás előtt online számítógépre másolnunk.

---

28 Ennek lehetősége ugyanis sosem zárható ki teljesen egy internetkapcsolattal bíró számítógépen.

29 Ez azt jelenti, hogy ha egymilliárd ember használna a földön bitcoint, és mindegyik tíz címet generálna, két cím egyezésének az esélye akkor is csak 0.00000000000000000000000000000000000007 százalék lenne.

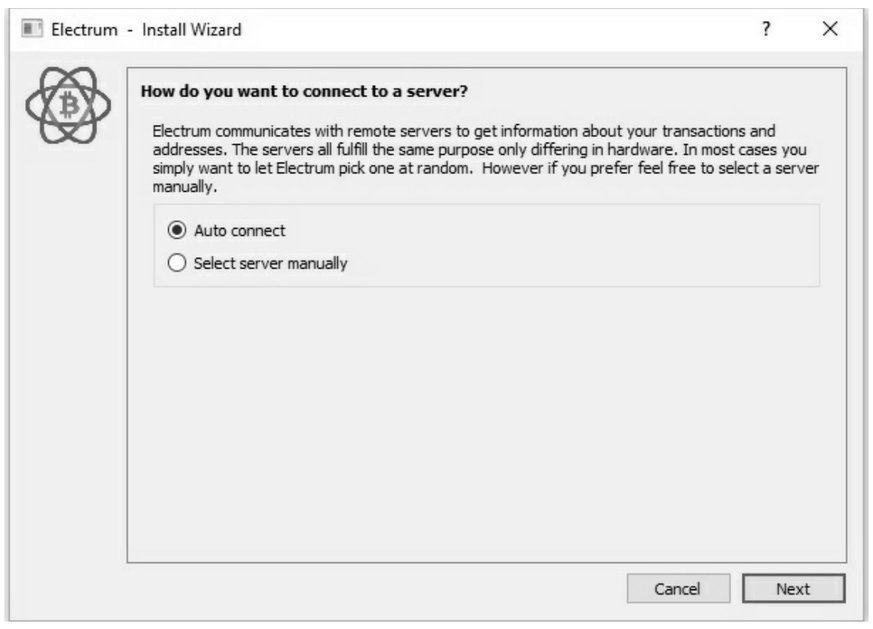
30 Mint például a https://blockchain.info/

Nyilvánvalóan célszerű minden lefoglalást szenvedő esetén külön címet generálni, azonban a címek számát egyéb célszerűségi okok is meghatározhatják (külön címek a külön bűncselekményekből származó bitcoinok biztosítására stb.).

A tárca létrehozásának lépései a következők.

Az első indítás után be kell állítanunk, hogy a kliens milyen módon csatlakozzon a blokkláncot tartalmazó szerverhez. A beállítást hagyjuk az alapértelmezettként felajánlott *Auto connect* lehetőségen, majd kattintsunk a *Next* fülre! *(1. számú ábra)*

1. számú ábra



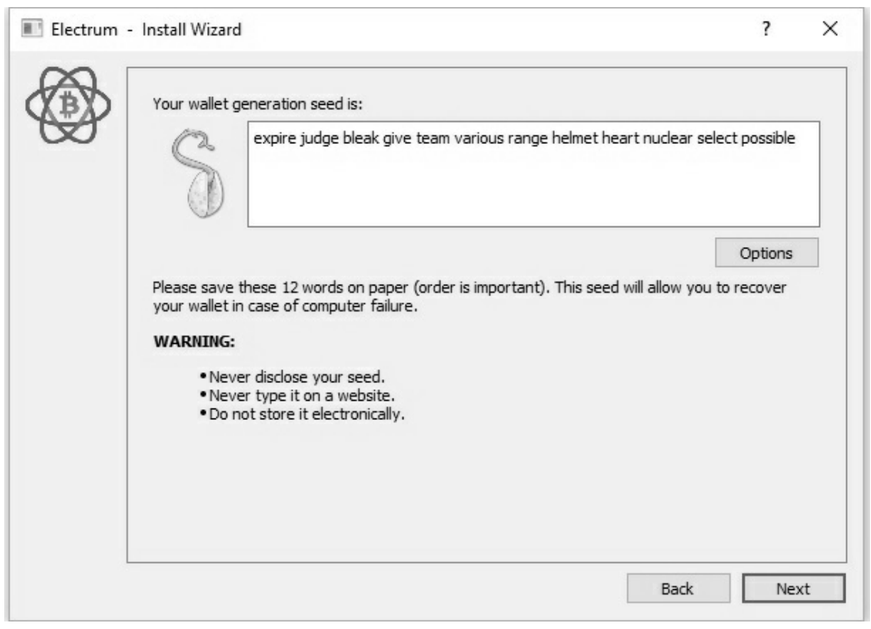
Ezt követően a kliens létrehoz egy *electrumdata* elnevezésű mappát ugyanazon a helyen, ahonnan a letöltött klienst elindítottuk. Ez a mappa fogja tartalmazni a *wallets* almappában *defaultwallet* néven a létrehozott tárcafájlt (ha csak nem változtatjuk meg a tárca nevét a következő ablakban).

Az ez után felugró három fülben a felajánlott lehetőségek közül sorban válasszuk ki a *Standard wallet, Create new seed, Standard* opciókat, hogy a következő ablakhoz jussunk.

Az előbbi ablakban a program egy *seed*nek (magnak) nevezett, 12 véletlenszerű szóból álló listát fog feltüntetni, amit fel kell jegyeznünk, és a következő ablakban ugyanilyen formában kell majd megadnunk. *(2. számú ábra)*

Ez egy biztonsági megoldás, ugyanis a *seed* ismeretében (ami gyakorlatilag egy kriptográfiai művelet alapjaként szolgál) később bármikor visszaállíthatnánk a tárcában lévő összes címet és privát kulcsot, ha valamilyen okból elvesztenénk azokat.

2. számú ábra



Minderre a jelen eljárási rendben nem lesz szükségünk, az opció azonban sajnos nem kerülhető meg. Másoljuk tehát ki a szavakat, majd a következő ablakban adjuk meg őket újból.

Ha ezt megtettük, a kliens fel fogja ajánlani, hogy készítsünk jelszót is a tárcához. Ha állítanánk be jelszót, az a privát kulcsok kliensen belüli megjelenítéséhez és ezáltal az utalások végrehajtásához lenne szükséges. Mivel azonban a tárcát – mint azt a későbbiekben kifejtem – a lefoglalás után a programból törölni fogjuk, így e biztonsági lépcső közbeiktatása felesleges.

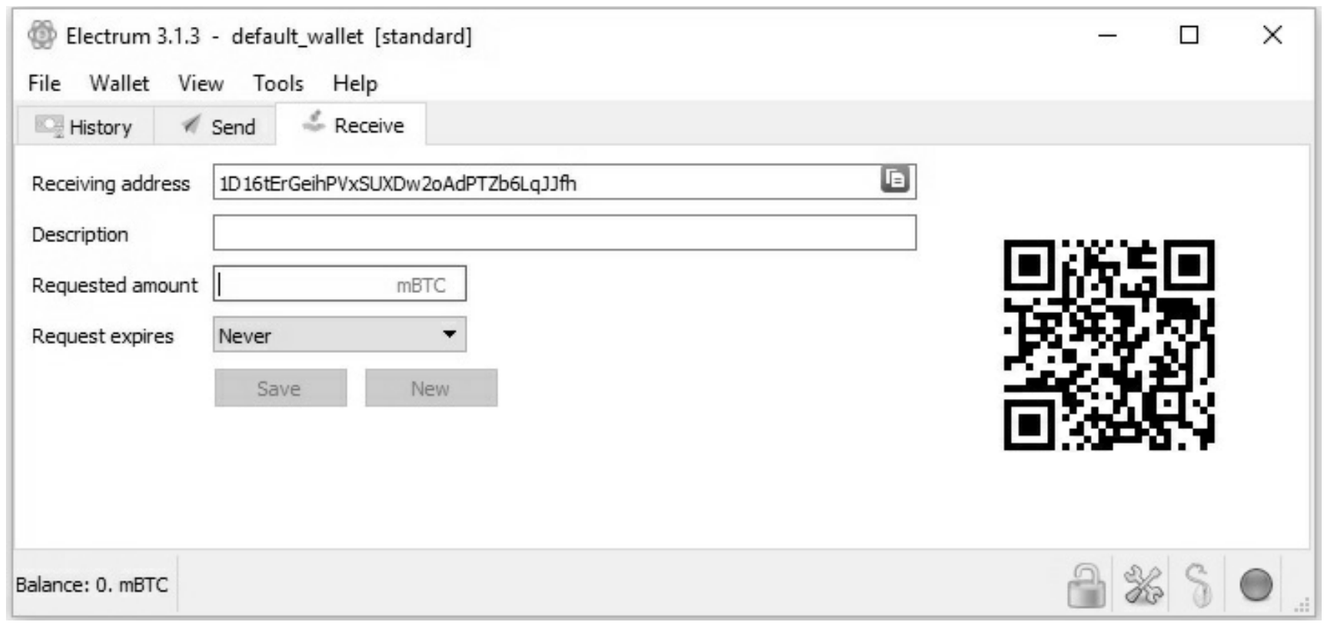
A mezőket üresen hagyva lépjünk tehát tovább, majd hasonló megfontolásból a *seed*ről készült előző feljegyzésünket is semmisítsük meg (arra a továbbiakban nem lesz szükségünk, ha azonban illetéktelen kezekbe kerülne, akkor a tárca újragenerálásával a lefoglalt bitcoinhoz más is hozzáférhetne).

Az előbbiek után a program létrehoz egy tárcát, amelybe belépve a *Receive* fül alatt láthatjuk is az első címünket a hozzá tartozó QR-kóddal.[31] *(3. számú ábra)*

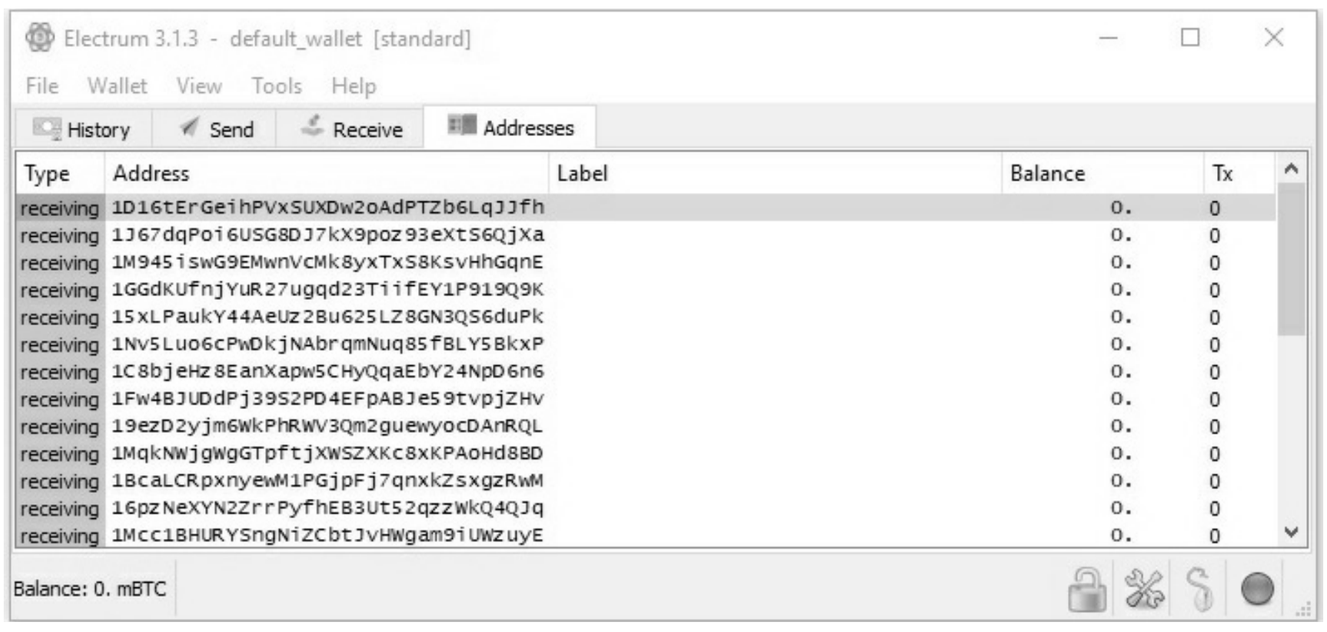
A tárcában azonban valójában ezzel egyidejűleg több cím létrehozására is sor kerül, amelyeket a *View* és a *Show Addresses* opciókra kattintva, majd pedig a megjelenő *Addresses* fülre lépve láthatunk. A *Balance* oszlop jelöli az adott címekhez tartozó bitcoin mennyiségét, amely jelen esetben mindenhol nulla. *(4. számú ábra)*

31 A QR-kódok lényege, hogy hosszabb szövegeket (mint amilyen egy bitcoincím is) grafikus formában tárolnak, így a megfelelő applikációkkal olvasva őket nem kell begépelni vagy átmásolni az adott szöveget. A mobilra letölthető tárcák legtöbbje képes QR-kódot beolvasni, így ez kényelmi funkciónak tekinthető.

3. számú ábra



4. számú ábra



A következő lépésben a szükséges mennyiségű címet egy külső adathordozó segítségével át kell másolnunk a tranzakcióhoz előkészített gépre, hogy a lefoglalás előtt majd célként meg tudjuk adni a kliensben. Bár a címet le is gépelhetjük, célszerű másolást alkalmazni, ugyanis bármely karakter elütése esetén a tranzakció nem jön létre (a karaktersor egyaránt tartalmaz kis- és nagybetűket, illetve számokat).

A címekhez tartozó privát kulcsokat természetesen nem kell átmásolnunk a másik számítógépre, ugyanis a bitcoin fogadásához azokra nincs szükségünk.

Jobb gombbal valamelyik címre kattintva, a *Copy Address* paranccsal másoljuk vágólapra bármelyik általunk választott címet, ezt követően illesszük azt egy egyszerű szöveges fájlba, és egy – lehetőleg előzőleg formatált – pendrive segítségével másoljuk át a tranzakcióhoz használandó számítógépre.

A fogadó címhez tartozó privát kulcs biztonságba helyezése

A tárca létrehozása után digitális mentést fogunk készíteni az előző pontban kimásolt címekhez tartozó privát kulcsokról. *(5. számú ábra)*

5. számú ábra

A privát kulcsot az adott címre jobb gombbal kattintva a *Private Key* parancscsal jeleníthetjük meg (mint korábban említettem, a privát kulcs jelen esetben az L karakterrel kezdődik, a „p2pkh” csupán a kulcs létrehozása során alkalmazott script típusát jelöli, ami esetünkben irreleváns).

Mind a címet – az előző pontban kifejtettek szerint –, mind a hozzá tartozó privát kulcsot másoljuk át egy egyszerű szöveges fájlba, amit ezt követően másoljunk külső adathordozóra (valamilyen optikai lemez használata javasolt).[32] A fájlt indokolt továbbá jelszóval is védeni, amelynek legegyszerűbb módja annak tömörítése WinRAR-ral, jelszó megadása mellett (természetesen még a lemezre másolás előtt).

A jelszót természetesen szintén úgy kell tárolnunk, hogy illetéktelen személy azt ne ismerhesse meg. Erre megfelelő módszer lehet, ha azt – annak érdekében, hogy átvilágítással se lehessen kifürkészni – egy kartonlapra írva, zárt borítékban tároljuk az adathordozótól elkülönítve.

Az adathordozót a bűnjelekhez hasonlóan kell csomagolnunk szintén olyan módon, hogy a bűnjelzacskó felnyitása állagsérelem okozása nélkül ne legyen lehetséges. Az adathordozót ez után elhelyezhetjük a bűnjelkamrában, míg a jelszót az eljárás során egy másik helyiségben indokolt őrizni.

32 Bár a címek a hozzájuk tartozó privát kulcsokból visszafejthetők ugyan, praktikus okokból azonban indokolt azokat is a privát kulcsok mellett feltüntetni.

Az adathordozó tárolásánál figyelemmel kell lennünk arra is, hogy megsemmisülése vagy elvesztése esetén végleg elveszítjük a lefoglalt bitcoin feletti rendelkezés lehetőségét, ajánlott ezért egyidejűleg egy biztonsági másolatot is létrehozni (és hasonló módon tárolni).

A mentések elkészítése után a tárcafájlt (ami a már említett mappában található *defaultwallet* néven) törölnünk kell a létrehozáshoz használt számítógépről, hogy később senkinek se legyen módja megismerni a privát kulcsokat. Ügyeljünk arra, hogy az adatokat végleg töröljük a merevlemezről, hogy azok erre szolgáló programok segítségével se legyenek visszaállíthatók. Ilyen célra egyszerűen és ingyen használható a File Shredder nevű alkalmazás.[33]

A lefoglalást szenvedő privát kulcsának felkutatása

A házkutatás megkezdése előtt mindenképpen indokolt adatgyűjtést folytatnunk arra vonatkozóan, hogy a célszemély milyen módon tárolhatja az eljárás tárgyát képező bitcoint. Ehhez vegyük igénybe blokklánc segítségét is, ugyanis könnyen kiderülhet, hogy a keresett bitcoint elutalták egy online tőzsdéhez, pénztárca-szolgáltatóhoz, vagy egyéb más szolgáltatóhoz (ezek címei általában egyszerű Google-keresés alapján is azonosíthatók). Különösen árulkodó lehet, ha az adott címen nagy összegű bitcoin fordult meg, vagy rendkívül gyakoriak az utalások. Ilyen esetben máris tudhatjuk, hogy a házkutatás során nem a privát kulcsok, hanem az e szolgáltatókhoz tartozó bejelentkezési adatok felkutatása lesz a fő cél (természetesen ilyen esetben az utalást is e szolgáltatók felületén kell majd végrehajtanunk).
Ha nem találtunk olyan adatokat, amelyek az inkriminált címre vonatkozóan különösebb iránymutatással szolgálnának, vagy egyáltalán nem is ismerünk címet, akkor a házkutatás során kell a privát kulcsokra utaló nyomokat felkutatnunk.

A házkutatás megkezdésekor arra kell törekednünk tehát, hogy az eljárás alá vont a számítógépét ne tudja a kényszerintézkedés megkezdése után kikapcsolni. Ajánlott természetesen a házkutatást is olyan időpontban foganatosítani, amikor feltételezzük, hogy a számítógépet bekapcsolt állapotban találhatjuk (nem indokolt tehát ilyen esetben a hajnali órákban kopogtatni, célszerűbb abban az időszakban felkeresni az eljárás alá vontat, amikor délutáni vagy esti pihenését tölti).

33 http://www.fileshredder.org/

Az adatok lefoglalására irányuló házkutatások során általában a nyomozó hatóság igyekszik lefoglalni a helyszínen talált eszközöket, amelyekről aztán a lefoglalás után mentést készít az adattartalom későbbi vizsgálata céljából.

Hogyha azonban a kényszerintézkedés bitcoin felkutatására irányul, akkor az effajta késlekedésre nincs mód; a megtalált elektronikai eszközöket a helyszínen kell átvizsgálni addig, míg lehetőségünk van az eljárás alá vont személyt felügyelet alatt tartani. Máskülönben a távozásunk után azonnal lehetősége nyílna más címre utalni a bűncselekmény tárgyát képező bitcoint, még ha egyébként a privát kulcsok megtalálhatók lettek volna később a lefoglalt eszközökön is.

Ha sikerült a számítógépet bekapcsolt állapotban találnunk (vagy az nem volt jelszóval védve), akkor tehát azonnal meg kell kezdenünk felkutatni a számítógépen lévő klienseket (alapértelmezés szerint ugyanis a tárcafájlok általában e programok gyökérkönyvtárában találhatók). A kliensek felkutatása azért is indokolt, mert a tárcából a privát kulcsok kinyerése legkönnyebben a lefoglalást szenvedő által használt programmal lehetséges. Bár az Electrum képes lehet a más típusú kliensek által létrehozott tárcafájlokat is megnyitni, azonban könnyen felléphetnek kompatibilitási problémák is. A tárcafájlok pontos helye felkutatásának megkönnyítése érdekében végezhetünk internetes keresést is, ez alapján ugyanis gyorsan megállapíthatjuk, hogy egy-egy adott kliensnek mi az alapértelmezett mentési helye és tárcaneve. Hogyha a számítógépen nem találunk bitcoinklienst, akkor a meghajtókon egyszerű keresést kell végeznünk a *„wallet, private key, seed”* és egyéb olyan szótöredékekre, amelyekről feltételezzük, hogy a privát kulcsokhoz vezethetnek minket.

A meghajtók tartalmának átvizsgálása mellett ellenőriznünk kell a böngészési előzményeket és könyvjelzőket is. Ennek során akkor is fel kell jegyeznünk az előzményekben talált váltókat és egyéb szolgáltatókat, ha hozzájuk bejelentkezési adatokat nem sikerült megállapítanunk, ugyanis az eljárás későbbi szakaszában megkeresést küldhetünk részükre a célszemélyre vonatkozóan. Ugyanez vonatkozik a felhőszolgáltatókra is, ugyanis a privát kulcsok náluk is tárolhatók. A böngészési előzmények mellett érdemes ellenőriznünk továbbá a sütiket is, ugyanis ezeket a felhasználók – az előzményekkel ellentétben – hajlamosak nem törölni.

A számítógépek mellett természetesen – ugyanilyen elvek alapján – ellenőriznünk kell a célszemély birtokában lévő összes egyéb elektronikai eszközt is (tabletek, mobiltelefonok), az ilyen eszközökön szokásos tárcák után kutatva.

Természetesen lehetséges, hogy az eljárás alanya papír alapon, vagy más külső adathordozón tárolja a privát kulcsokat, így nem csupán a számítógépeket, telefonokat (stb.) kell felkutatnunk. Az elektronikus és hagyományos iratok átvizsgálása során figyelemmel kell lennünk az olyan iratokra is, amelyek egymástól független szavakat tartalmaznak, ugyanis nem kizárt, hogy a célszemély feljegyzést készített a tárcájához tartozó *seed*ről. Ha nem bitcoint keresünk, akkor még a házkutatás előtt érdemes tájékozódni afelől, hogy az adott kriptovaluta privát kulcsai milyen formátummal bírnak.

Szintén figyelemmel kell lenni a QR-kódokat tartalmazó iratokra is, ugyanis ezek is jó eséllyel takarhatnak bitcoin címeket éppúgy, mint hozzájuk tartozó privát kulcsokat. Ne feledkezzünk meg továbbá a hardverkulcsok felkutatásáról sem, ha feltételezzük, hogy a gyanúsított ilyet használt a bitcoinjai megőrzése érdekében (tartsuk szem előtt azonban, hogy ezen eszközök PIN-kóddal is elláthatók).

A manapság legelterjedtebb hardverkulcsok a *6. számú ábrá*n láthatók:

6. számú ábra

A *7. számú ábrá*n láthatóhoz hasonló, papíralapú tárcát kell keresnünk jellemzően abban az esetben, amikor az alany ATM-en keresztül vásárolt bitcoint (új tárca létrehozása esetén az ATM-ek ugyanis kinyomtatnak egy címet és privát kulcsot is tartalmazó papírtárcát). Az erre vonatkozó információk felderítése során szintén igénybe vehetjük a blokkláncot, ugyanis az ATM-ek címe is legtöbbször ismert.

Amennyiben a helyszínen nem voltunk képesek felkutatni a privát kulcsot, még nem tekinthetünk el automatikusan az eszközök lefoglalásától, ugyanis lehet még esélyünk azok megtalálására a benti, alaposabb vizsgálat során is. Természetesen éppúgy bízhatunk abban is, hogy az elkövetőnek nincs másolata a privát kulcsairól (így a lefoglalás esetén sem fogja tudni a bitcoint továbbutalni), mint ahogy egyébként tartanunk kell tőle, hogy igen.

7. számú ábra

Az is előfordulhat továbbá, hogy egy nyomozás során nem is számítunk arra, hogy a célszemély rendelkezik bitcoinnal, azonban a lefoglalt eszközei átvizsgálása során később mégis erre vonatkozó adatokat találunk (bitcoinkliens, elmentett privát kulcs stb.). Ha az eljárásban indokolt lehet az így talált bitcoin lefoglalása is (például a kár megtérülésének biztosítása érdekében), ezt szintén a lehető legrövidebb időn belül kell megtennünk.

Ilyen esetekben természetesen külön kell lefoglalnunk a később feltárt bitcoint – már csak a tranzakció pontos dokumentálása és a jogorvoslati jog biztosítása érdekében is –, a lefoglalást pedig indokolt egy szemle keretében végrehajtani. A szemlejegyzőkönyvben így – a lefoglalás mellett – dokumentálhatjuk azt is, hogy miként tekintettük át az adathordozót, ezt a korábbi kényszerintézkedés során miért nem végeztük el helyben (időhiány, az adatok nagy mennyisége stb.), és eközben hol és hogyan bukkantunk olyan adatokra (például privát kulcs, tárcafájl), amelyek felhasználásával a lefoglalást végrehajtjuk. Ebben az esetben természetesen elegendő, ha a szemlét és a lefoglalást hatósági tanú jelenlétében végezzük el, befejeztével pedig haladéktalanul értesítjük az érintett személyt, akit utólag nyilatkoztatunk a panasztételi szándékáról (hiszen, ha még a lefoglalás előtt értesítenénk, akkor ezzel esetleg lehetőséget adnánk neki a bitcoin továbbutalására).

A privát kulcsok kinyerése a tárcából

A privát kulcsok azonosítására a legegyszerűbb módszer, ha a tárcát az elkövető által használt programmal nyitjuk meg. Ebben az esetben láthatjuk az elkövető által létrehozott címeket és az azokon szereplő összegeket is. Ilyen

esetben a privát kulcsokat az erre szolgáló funkcióval – a tranzakcióhoz előkészített számítógépre történő másolás céljából – egy szöveges fájlba menthetjük. Bár minden program felépítése más, az Electrumhoz hasonlóan általában *Private key* elnevezésű gombot kell keresnünk a privát kulcs megjelenítéséhez (amennyiben nem boldogulunk, használjuk a program súgóját vagy keressünk rá az interneten a funkció előhívásának mikéntjére az adott kliensben).

Ha valamilyen okból a program segítségével nem sikerült megjelenítenünk a privát kulcsokat, vagy nem is találtunk erre szolgáló programot a gépen, különálló tárcafájlt vagy privát kulcsokat azonban igen, akkor egyszerűen ezeket másoljuk át a tranzakcióhoz előkészített számítógépre.

A privát kulcsok importálása a tranzakcióhoz használandó számítógépre

Természetesen ha a házkutatás során feltárt klienssel, vagy webes alkalmazással el tudjuk utalni a bitcoint a hatósági címre, akkor tegyük ezt meg. Hogyha azonban csak egy különálló tárcafafájlt vagy privátkulcsot találunk, vagy más okból nem tudjuk a tranzakciót végrehajtani (például a vizsgált eszköz nem csatlakozik az internethez), akkor az általunk ebből a célból előkészített számítógépet kell igénybe vennünk az utaláshoz.

Tárcafájl esetén a fájlt másoljuk a korábban említett *electrumdata\wallets* mappába, ami után jó eséllyel az Electrum felismeri majd és megjeleníti az abban szereplő címeket az *Addresses* fül alatt (ehhez nem árt újraindítanunk a programot, majd ezt követően a *File/Open* paranccsal megnyitni a tárcát).

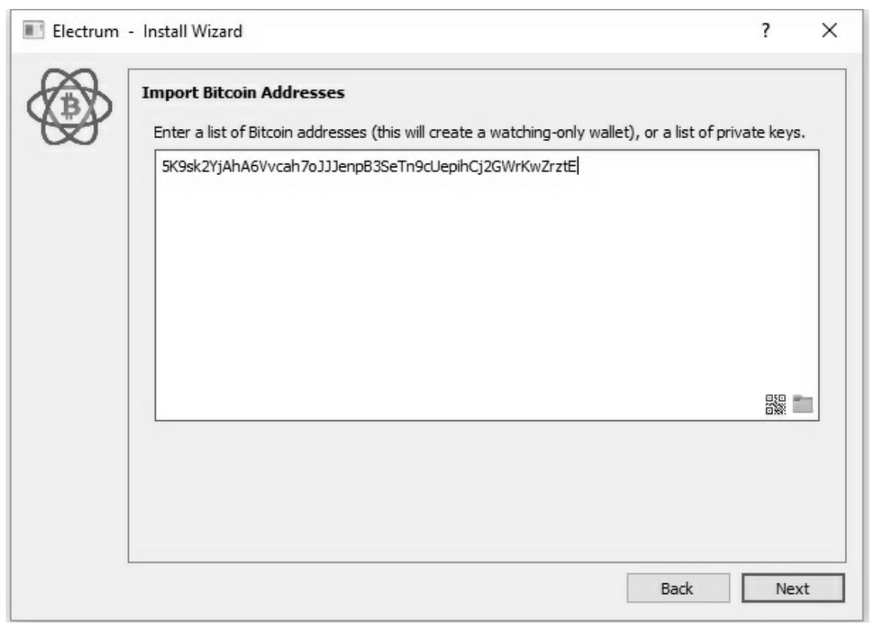
Ha ez után nem jelennek meg a tárcában lévő címek az *Addresses* fül alatt, akkor a tárcafájl nem kompatibilis az Electrum programmal. Ilyen esetben próbáljuk meg kideríteni, milyen programmal készült a tárcafájl, majd a letöltés és telepítés után nyerjük ki a privát kulcsokat *A privát kulcsok kinyerése a tárcából* című részben írtak szerint (ha a lefoglalást szenvedő nem hajlandó elárulni a kliens nevét, akkor erre vonatkozóan internetes kutatást végezhetünk a fájl elnevezése alapján, vagy megpróbálhatunk felkutatni telepítő fájlokat a számítógépen és a lomtárban).

Mielőtt azonban ezt megtennénk, kíséreljük meg egyszerűen Notepaddel is megnyitni a fájlt, ugyanis – egyszerű adatfájl lévén – jó eséllyel kaphatunk értelmezhető adatokat. Ha a privát kulcsot közvetlenül nem találjuk is meg így, lehet esélyünk akár a *seed* megismerésére, amit ezt követően csupán be kell emelnünk az Electrumba (a fogadásra szolgáló címek elkészítéséről szó-

ló pontban megismert lépések keretében) és ilyen módon újragenerálni a privát kulcsokat.

Ha csak különálló privát kulcsokat tudtunk felkutatni, akkor ezek importálására lesz szükség (ebben az esetben azonban már nem kell kompatibilitási problémáktól tartanunk). Ehhez a *File* legördülő menüben a *New/Restore* parancsra kattintva meg kell adnunk egy nevet az újonnan létrehozandó tárcának, majd ezt követően a fogadásra szolgáló címek létrehozása során már ismert ablakok tárulnak elénk. Most azonban a *Standard wallet* helyett az *Import bitcoin addresses or private keys* lehetőséget válasszuk. A megjelenő ablakban most a mag helyett a megszerzett privát kulcsokat kell az erre szolgáló mezőbe másolnunk. Egyszerre több privát kulcsot is megadhatunk, illetve a mező jobb alsó sarkában lévő mappa ikonra kattintva akár ki is jelölhetjük az általunk korábban létrehozott szöveges fájlt (a program automatikusan felismeri a benne lévő kulcsokat). Bár a program felajánlja, jelszót megint nem szükséges megadnunk.

8. számú ábra



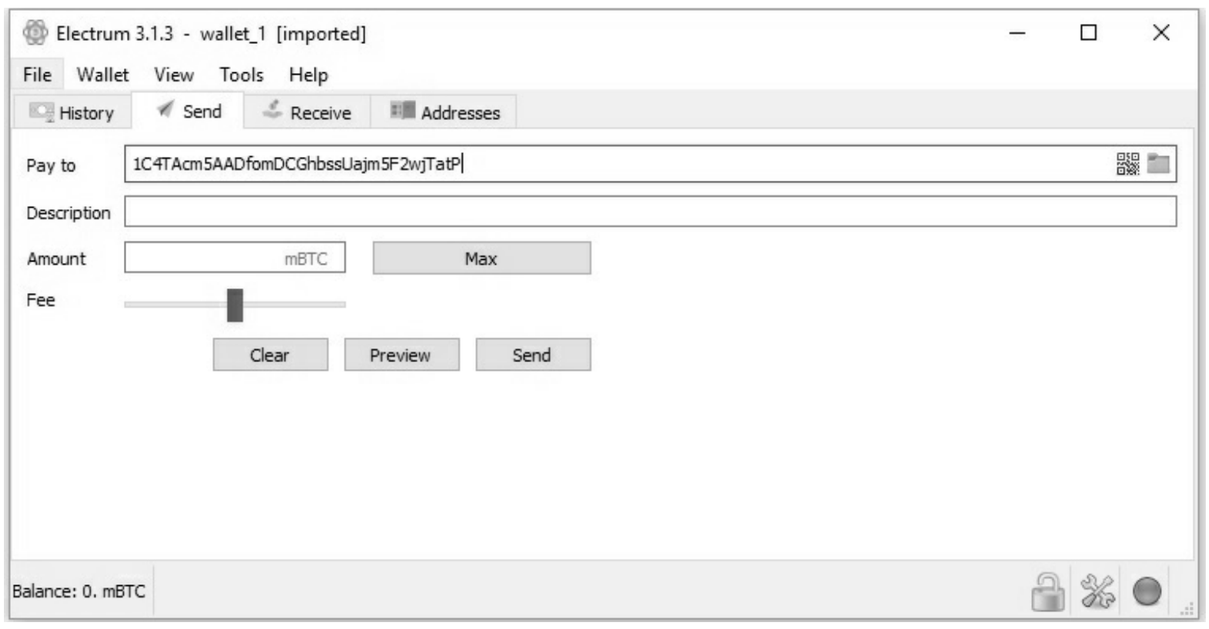
Ha a privát kulcsokat papír alapon találtuk meg, akkor kénytelenek vagyunk azokat manuálisan begépelni a fenti mezőbe. Ilyenkor különösen ügyeljünk a pontosságra, valamint a kis- és nagybetűk különbözőségére.

Az importálás után a kliens egy új tárcafájlt hoz létre, amely csak az importált címeket tartalmazza (ezek ekkor generálódnak a privát kulcsokból). Egy új Electrum-ablakban az *Addresses* fül alatt jelennek meg a címek, és az azokhoz rendelt bitcoinösszegek. A címre jobb gombbal kattintva, a *Private key* paranccsal akár meg is győződhetünk róla, hogy valóban az általunk korábban megadott privát kulcshoz tartozik a cím.

A tranzakció végrehajtása

A tranzakció végrehajtása előtt ellenőriznünk kell az internetkapcsolatot a tranzakcióhoz használt számítógépen, hiszen enélkül az utalás nem jöhet létre (a kapcsolat meglétét egyébként a kliens jobb alsó sarkában található zöld kör is jelzi). *(9. számú ábra)*

9. számú ábra



Ezt követően kattintsunk a *Send* fülre, majd a *Pay to* mezőbe a korábban létrehozott valamely hatósági címet másoljuk be. Ügyeljünk arra, hogy a karaktersort pontosan adjuk meg, hiszen ellenkező esetben nem jön létre a tranzakció. Az *Amount* mezőben kell megadnunk az elküldendő bitcoinösszeget.

Előfordulhat – sőt, valószínű –, hogy a lefoglalást szenvedő egyszerre több címen is tárol bitcoint. Ilyen esetben a tranzakció összegének az összes címen tárolt bitcoin együttes összegét adjuk meg, ha nincs különös indokunk a más-más címekre történő utalásra (mint tudjuk, egyszerre több címről is küldhetünk bitcoint egyetlen tranzakció során). A küldő címeket nem kell kijelölnünk, a program automatikusan levonja a rendelkezésre álló címekről a szükséges összeget. Természetesen összeadogatnunk sem kell az összegeket, elég, ha ehhez a *Max* gombra kattintunk (praktikus is ezt a módszert alkalmazni, hiszen így a félreszámolás veszélye nélkül „üríthetjük ki” egyszerre a lefoglalást szenvedő összes címét).

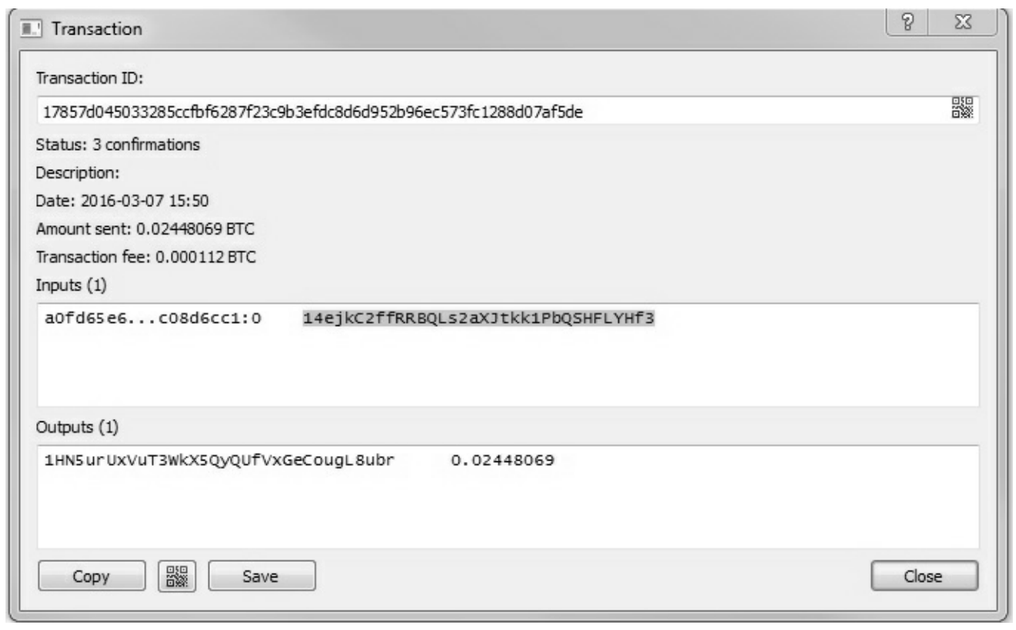
Az előbbi adatok megadása után kattintsunk a *Send* gombra (ha az Electrum nem ismerte fel a tárcafájlt és ezért kénytelenek voltunk az adott fájlnak megfelelő klienst letölteni, akkor természetesen a menüpontok eltérők lehetnek, azonban lényegében ugyanezen adatokat kell megadnunk).

A tranzakció végrehajtásához tranzakciós díjat kell fizetnünk, ez azonban elhanyagolható mértékű. Bár ennek összege hatással lehet a blokkba foglalás sebességére, ajánlott elfogadni az alapértelmezett mértéket (a tranzakciós díj nagyságát egyébiránt a *Tools/Preferences/Fees* menüpontban tudjuk módosítani).

A tranzakció ellenőrzése

A küldést követően néhány másodpercen belül megjelenik a *History* fül alatt a tranzakció, ezzel párhuzamosan pedig a címeken lévő bitcoinok összege nullára csökken. A tranzakcióra jobb gombbal kattintva, majd a *Details* parancsot választva előhívhatjuk a tranzakció részleteit tartalmazó ablakot.

10. számú ábra



A *Status* bejegyzés mellett láthatjuk, hogy a tranzakciót hány alkalommal erősítették meg *(confirmation)* a bányászok. Elméletileg előfordulhat, hogy a hatósági tranzakció elindítását követően a lefoglalást szenvedő is indít egy tranzakciót ugyanarról a címről, és – ha magasabb jutalékot ad meg – a bányászok az ő tranzakcióját erősítik meg előbb.

Ez csak úgy előzhető meg, ha a lefoglalást szenvedőt felügyelet alatt tartjuk mindaddig, míg a tranzakció legalább egy – de inkább két – megerősítést nem kap (ergo a blokkba foglalást követően már egy újabb blokkot is kibányásztak). Két megerősítést követően már közel lehetetlen egy tranzakciót felülírni a blokkláncban, így a lefoglalást sikeresnek tekinthetjük.

Mivel a tranzakció ekkor már a nyilvános blokklánc része, ezért az ellenőrzést akár bármely erre szolgáló weboldal segítségével is elvégezhetjük. A

példában szereplő tranzakció a https://blockchain.info/ oldalon az előbbiek szerint néz ki.

Ha mindezt végrehajtottuk, akkor már „csak” azt kell megoldanunk, hogy az utalásban érintett címekhez tartozó privát kulcsokat a továbbiakban is biztonságban őrizzük.

A bitcoin tárolása az eljárás során

Bár a lefoglalás lépéseinek bemutatásakor egyben ajánlást adtam arra vonatkozóan is, hogy milyen módon történjen a lefoglalt bitcoin tárolása, azonban ez a módszer csak abban az esetben alkalmazandó, ha nem áll rendelkezésre erre vonatkozóan központi megoldás.

Mindenekelőtt fontos leszögezni, hogy a bitcoint a lefoglalást követően a hatóság nem értékesítheti abból a célból, hogy az eljárás végéig pénzként tárolja azt a letéti számláján (a kapcsolódó konferenciák során gyakran hallok erre vonatkozó „javaslatokat”). Bár ez elsőre talán kézenfekvő megoldásnak tűnhet, azonban több akadálya is van.

Egyrészről a 11/2003. (V. 8.) IM–BM–PM együttes rendelet alapján letéti számlára csak lefoglalt pénzt lehet befizetni – magyar pénzt a hatóság által kezelt, külföldi pénzt pedig a Magyar Államkincstár által vezetett letéti számlára –, a bitcoin pedig jogilag nem tekinthető pénznek.

Másrészről pedig a lefoglalt dolgok előzetes értékesítéséhez szükséges feltételek[34] egyike sem igaz a bitcoinra – a bitcoin ugyanis nem romlandó, nem alkalmatlan huzamos tárolásra, az nem jár jelentős költséggel, illetve az sem jelenthető ki, hogy a hosszú tárolás miatt értéke biztosan csökkenne.[35] Márpedig ezek a törvényben taxatíve felsorolt feltételek, az előzetes értékesítésnek más esetköre nincs.[36]

Érdemes megjegyezni továbbá, hogy ha nem lennének jogi akadályai az előzetes értékesítésének, az akkor sem lenne indokolt. A bitcoin árfolyama ugyanis rendkívül nagy ingadozást mutat (néhány éves története során az értéke több ezerszeresére növekedett, majd újból csökkent), és ha a lefoglalás után az értéke újból növekedne, akkor a számlán lévő forintösszeg már nem

34 Be. 156. § (1) bekezdés

35 Az utolsó pont kapcsán meg kell jegyezni, hogy a bitcoin értéke a tárolás során valóban csökkenhet ugyan, ám éppúgy nőhet is, a törvény pedig csak akkor teszi lehetővé az előzetes értékesítést, ha a csökkenés bizonyosan bekövetkezik a hosszú tárolás miatt.

36 E feltételek az új Be.-ben is változatlanok [új Be. 319. § (3) bekezdés].

fedezné az értékét. Ha valamely okból a lefoglalás megszüntetésére kerülne sor, akkor a bitcoin tulajdonosát érdeksérelem érhetné, amiért akár jóval kisebb pénzösszeget kap vissza, mint amit a bitcoinjai egyébként érnének.

Mivel a bitcoin lefoglalására jellemzően nem a bizonyítás (hiszen arra tökéletesen alkalmas a blokklánc), hanem a vagyonelkobzás későbbi biztosítása érdekében kerül sor, így a hatóság a lefoglalást arra való hivatkozással sem szüntetheti meg, hogy arra a bizonyítás érdekében már nincs szükség. A lefoglalt bitcoin ezért jellemzően az eljárás végéig a hatóság őrzésében kell hogy álljon, amíg az eljárást valamilyen okból meg nem szüntetik, vagy ítélettel a vagyonelkobzást a bíróság meg nem állapítja.[37]

Fel kell készülni tehát arra, hogy a bitcoin őrzéséről hosszú ideig kell a hatóságnak gondoskodnia. És bár ez csak a privát kulcsok megőrzését jelenti, azonban amennyire mindez egyszerűnek hangzik, egyúttal éppoly bonyolult is.

A privát kulcs megismerése esetén ugyanis bárki, a lebukás rendkívül kis kockázatával képes lehet megszerezni a bitcoint, ami sajnos súlyos veszélyt jelent. Bár szeretnénk azt hinni, hogy a hatóság tagjai feddhetetlenek, azonban a büntetőeljárás során lefoglalt dolgok jellemzően sok kézen mennek keresztül a nyomozás során, és egyszerűen csak megbízni e kezek feddhetetlenségében túlzott könnyelműség lenne.[38]

Kézenfekvőnek látszik, hogy a privát kulcsok elkészítését és őrzését bízzuk csupán egyetlen személyre, hiszen ilyenkor egyértelmű, hogy a bitcoin eltűnése esetén ki a felelős. Ilyenkor azonban számolnunk kell azzal a kockázattal, hogy ha ezzel a személlyel később történik valami, vagy egyszerűen csak elveszti a kulcsokat, és rajta kívül senki nem fér hozzájuk, akkor a hatóság maga veszíti el a rendelkezés lehetőségét. Két személy esetén viszont már sosem lehetünk biztosak benne, hogy melyikükben keressük a felelőst.

Látható tehát, hogy meg kell találni a kényes egyensúlyt a privát kulcsok illetéktelen kezekbe kerülésének, illetve azok elvesztésének kockázata között olyan módon, hogy számottevően egyik tényező miatt se kelljen aggódnunk.

---

37 Érdekes kérdés, hogy az új Be.-ben megjelenő megváltás intézménye (318. §) miként jelentkezik majd a gyakorlatban a bitcoinlefoglalások során. Egyes nyugati országokban régóta gyakorlat, hogy a bitcoin lefoglalását követően a lefoglalást szenvedőt írásban nyilatkoztatják, hogy mi a kívánsága: a hatóság adja el rögtön a bitcoint az adott árfolyamon, vagy pedig bitcoinként őrizze azt továbbra is az eljárás végéig. Hasonló módszerre akár a megváltás intézménye is lehetőséget adhat, azonban itt a tulajdonosnak kell visszavásárolnia a lefoglalt bitcoint a hatóságtól, és ennek engedélyezése is ez utóbbitól függ.

38 Találhatunk példát arra vonatkozóan, amikor éppen a csábításnak ellenállni nem tudó nyomozó tulajdonította el az eljárás során lefoglalt bitcoint. FBI Agent Admits to Stealing Silk Road Bitcoins Seized by U.S. Marshals. https://news.bitcoin.com/rogue-silk-road-agent-admits-to-stealing-bitcoins-seized-by-u-s-marshals/

Az általam vázolt megoldás ideig-óráig használható ugyan, hosszú távon azonban nyilvánvalóan nem fenntartható. Egyrészről mindenképpen bele kell helyeznünk a teljes bizalmunkat abba a személybe, aki a privát kulcsokat létrehozza, hiszen semmilyen módon nem ellenőrizhetjük, hogy azokat a folyamat során nem másolja le. Másrészről a privát kulcsok adathordozón való tárolása a bűnjelkamrában nem olyan megoldás, amit a bitcoin megszerzése érdekében elszánt személy ne tudna feltétlenül kijátszani, főként hogy valószínűsíthetően az esetleg létrehozott jelszót tartalmazó papír is pontosan ugyanebbe a bűnjelkamrába kerülne. Harmadrészről irreális azt feltételezni, hogy a rendőrségen belül ma a kapitányságok nagy részében hajlandók lennének elkülöníteni egy külön számítógépet csak azért, hogy azon bitcoincímeket hozzanak létre, és semmi másra ne használják (márpedig másképpen nem biztosítható, hogy a címek biztosan ne kompromittálódhassanak a készítés során). Negyedrészről pedig számításba kell venni azt is, hogy a nyomozók nagy részének nincsenek mélyebb ismeretei arról, hogy mi is pontosan a bitcoin, és milyen hibalehetőségekre kell különösen odafigyelni egy privát kulcs létrehozása és tárolása során, így – akár rendelkezésére áll egy útmutató, akár nem – a véletlen hibázás lehetőségével is számolni kell.

Mindezen tényezők egyesével is jókora kockázatot hordoznak magukban, így összességükben pedig mindenképpen azt feltételezik, hogy a biztonságos tárolás fenntartása hosszú távon csak központi intézkedés útján lehetséges.

A blokklánc jellegéből adódóan azonban semmi akadálya nincs annak, hogy a rendőrségen központi szinten, a szükséges szakértelemmel és biztonsággal elkészítsenek egy megfelelően őrzött címet, amit ezt követően minden alsóbb szerv egyformán használhat az összes lefoglalás során. Ezzel egyrészről levesszük a hibázás kockázatának terhét az alsóbb szintű nyomozó szervek dolgozóiról, másrészről nem terheljük őket a hosszú megőrzés jelentette felelősséggel sem, harmadrészről pedig nem is tágítjuk ki azon személyek körét, akikben kénytelenek vagyunk vakon megbízni.

Nem kell attól tartani, hogy az így létrehozott címen a különböző helyekről érkező lefoglalt bitcoinok „összekeverednek”, hiszen a blokklánc elvégzi helyettünk a „jegyzőkönyvezést”, és pontosan nyilvántartja, hogy mikor, honnan és mekkora összeg érkezett a címre.

Felvetődik azonban a kérdés, hogy kit bízzunk meg az így létrehozott címhez tartozó privát kulcs őrzésével. Mint láttuk, egy személy megbízása is kockázatos (a kulcs elvesztésének veszélye miatt), és több személy sem jelent megnyugtató megoldást (a felelősség megállapításának nehezülése miatt).

Szerencsére azonban a bitcoinprotokoll lehetővé teszi olyan címek létrehozását is, amelyek fölötti rendelkezéshez egyszerre több privát kulcs együttes megléte szükséges (ezeket hívják *multisignature* – több aláírást igénylő – címeknek vagy tárcáknak).

E *multisignature* címek valódi előnye azonban abban rejlik, hogy az aláírások szükségességének bármilyen kombinációja beállítható: minden további nélkül meghatározhatjuk például, hogy egy adott címhez három privát kulcs tartozzon, és az utalás kezdeményezéséhez ebből a háromból bármely kettő együttes meglétére legyen csupán szükség.[39]

Mindez tökéletes megoldást nyújt az előbb említett problémára, hiszen ennek a módszernek az alkalmazásával megbízhatunk két különböző személyt a rendőrség szervezetén belül egy-egy privát kulcs őrzésével, és a kiutalásokat egyikük sem fogja tudni a másik hozzájárulása nélkül kezdeményezni. Ugyanakkor attól sem kell tartanunk, hogy valamelyikük a privát kulcsot elveszíti és ezzel a bitcoinhoz való hozzáférést ellehetetleníti, ugyanis ilyen esetben még mindig rendelkezésre áll a harmadik – addig akár letétben tartott – privát kulcs is.

Mivel a közös címről történő kiutalásokra csak az eljárások legvégén kerül sor, így várhatóan csak viszonylag ritkán lesz szükség utalások végrehajtására. Ebből kifolyólag elképzelhető megoldás lehet akár az is, hogy a privát kulcsok egyikét a rendőrség, míg a másikat az ügyészség őrizze, a minimálisra csökkentve ezzel a lehetséges összejátszás veszélyét.

Álláspontom szerint – bár a bitcoinlefoglalások jelenleg még nem részei a nyomozó hatóságok mindennapi munkájának – az új büntetőeljárási törvény hatálybalépésével és a bitcoinnal kapcsolatos bűncselekmények számának folyamatos növekedésével a jövőben igenis számolni kell az effajta esetek megjelenésével. Mindehhez pedig elengedhetetlen egy olyan biztonságos rendszer létrehozása, amely lehetővé teszi a nyomozó szervek mindegyike számára a megőrzés egyszerű, átlátható és biztonságos módon történő végrehajtását.

39 Pedro Franco: Understanding Bitcoin: Cryptography, engineering, and economic. Wiley, 2014, pp. 136–137.

DOI: 10.38146/BSZ.2018.7-8.10

BENEDEK ZOLTÁN

Digitális adatok a helyszínen

A bűnügyi helyszínen mára nemcsak a klasszikus értelemben vett nyomok és anyagmaradványok találhatók meg, hanem a különböző elektronikai eszközök által tárolt, külső szemlélő elől rejtett adatok is, amelyeknek kiemelkedő bizonyító erejük lehet. A szakértői tevékenység bővülése következtében a szemlebizottság már „nem sétál el” az elektronikai eszközök mellett, hanem egyre nagyobb számban foglalják le őket, tartalmukat pedig igazságügyi informatikus szakértő vizsgálja meg. Nem is jelenthető ki, hogy csak egy bizonyos bűncselekménytípusnál javasolt lefoglalni ilyen eszközöket, gondoljunk csak arra, hogy akár egy mobiltelefon is rejthet olyan felvételt, amely múltban lejátszódó releváns történéseket rögzített videófelvétel vagy fénykép formájában. Legyen szó informatikai rendszer útján elkövetett csalásról, vagy kábítószer-kereskedelemről, számtalan olyan helyzet adódhat a gyakorlatban, ami a számítógépek, adathordozók, telekommunikációs eszközök lefoglalását teszi szükségessé.

A helyszínen nemcsak az elektronikai eszközök által tárolt digitális adatok felkutatásának, rögzítésének van kiemelkedő szerepe, hanem a bűnüldöző hatóságok által alkalmazott olyan eszközöknek is, amelyek a digitális technika segítségével rögzítik a helyszíni állapotokat.

A digitális adat megszámlálhatatlan formában létezik. A technika rohamos fejlődése nyomán szinte évente jelennek meg újabb és újabb eszközök, amelyeket a nyomozó hatóságok a bizonyítás szolgálatába tudnak állítani. Különbséget lehet tenni azon eszközök között, amelyekkel a helyszínen találkozunk, illetve alkalmazunk, valamint azok között, amelyeket a szakértők alkalmaznak a begyűjtött nyomok és anyagmaradványok vizsgálata során. A parttalanság elkerülése érdekében az eszközök közül a dolgozatomban csak néhányat tudok bemutatni, azonban megemlíthető a digitális hangazonosítás, a képanyagelemzés, az íriszazonosítás, a rekonstrukciós szoftverek, a biometrikus szkennelés vagy a rádiófrekvenciás helyazonosítás, amelyek a legújabb technikai fejlődés vívmányai.[1]

1 Fenyvesi Csaba: A kriminalisztika tendenciái. Dialóg Campus Kiadó, Budapest–Pécs, 2014, 68. o.

Ezek mindegyike kiemelt szerepet kap manapság a bűnüldözés eszköztárában. A digitális hangazonosítás lényege, hogy a rossz minőségű felvételeket ma már képesek vagyunk feljavítani, így megállapíthatjuk az elkövető hangját, leszűrhetjük a zavaró háttérzajt, így akár képesek vagyunk meghatározni a helyszínt.[2] A képanyagelemzés során a szakértők képesek az adott személy mozgását folyamatosan figyelni, megállapítani, hogy tart-e magánál fegyvert vagy egyéb tárgyat.[3] A biometrikus szkennelés mind a bűnmegelőzésben, mind a felderítésben kiemelt szerepet kap, ahogy a rádiófrekvenciás helyazonosítás is, hiszen mind az elkövető, mind a sértett mozgása modellezhető és ellenőrizhető.[4]

Digitális adatok felkutatása

A bűncselekmény helyszínén a nyomok és anyagmaradványok mellett lefoglalás tárgya lehet maga a számítógép is, a hozzá tartozó adathordozókkal együtt, pontos rögzítésük és későbbi vizsgálatuk bizonyítékként felhasználható. Ha a számítógéphez nyomtató is csatlakozik, indokolt lehet a nyomtató, és az általa kinyomtatott dokumentumok lefoglalása is, hiszen bizonyos bűncselekményfajtáknál relevánsak lehetnek.[5]

A számítógépes környezetben elkövetett bűncselekmények relatíve gyorsan és anonimitást kínálva segítik az elkövetőket. A helyszíniszemle-bizottság többnyire a kézzelfogható nyomok és anyagmaradványok felkutatására koncentrál, de az elektronikus bizonyítékok felkutatásáról sem lehet megfeledkezni. Ha sikerrel végzünk ilyen irányú kutatást, akkor is nagy körültekintéssel kell eljárni, mivel egy elektronikus bizonyíték olyan sérülékeny, mint egy ujjnyom.

Elektronikus bizonyítékokra lelhetünk például internetes levelezésben, böngészési előzményekben, felhasználónevekben, fényképekben, videókban, híváslistákban vagy akár GPS-előzményekben és koordinátákban is.

Hogyha számítógépet foglalunk le, akkor beszélhetünk látható bizonyítékokról (például CD-k), azonban nagyobb számban vannak jelen láthatatlan elemek is. Ilyenek például a gépben lévő memóriakártyák, telefonok esetében a híváselőzmények, PDA-készülékekben, tabletekben lévő adatok, okostele-

2 Uo. 68–69. o.
3 Uo. 69–70. o.
4 Uo. 71. o.
5 Ken Lidstone –Vaughan Bevan – Clare Palmer: Bevan and Lidstone's The Investigation of Crime. A Guide to Police Powers. Second Editon, Butterworths, 1996, p. 143.

fonokban lévő képek, videók, szervereken tárolt adatok, nyomtatókban tárolt információk, merevlemezek és szkennerek.

A rögzítésük során gondosan dokumentálni kell az elhelyezkedésüket, típusukat, darabszámukat, azonosítási számaikat, majd nem statikus zacskóba kell csomagolni őket. Ha nyomkutatás válik szükségessé például egy CD-n vagy merevlemezen, akkor kerülni kell a mágnespor használatát az elektronikus bizonyítékok károsodásának megelőzése érdekében.[6]

A számítógépes környezetben elkövetett bűncselekmények tipikus formája a különböző vírusok küldése, másolóprogramok használata, adathalászat, hamis adatok szolgáltatása, blokkolóprogramok küldése, logikai bombák használata a számítógép megbénítása érdekében, és számtalan más módszer. Ezek feltárása, bizonyítása és az elkövető kilétének a felderítése szakértő segítségével lehetséges, ami az esetek nagy részében meglehetősen nehéz, egyes esetekben pedig lehetetlen.[7]

A digitális bizonyítékoknak napjainkban egyre nagyobb jelentőségük van, ezért a helyszíni szemlénél a bizottságnak nagyobb figyelmet kell rájuk fordítania. A számítógépes környezetben elkövetett bűncselekmények lehetősége egyre szélesebb, gondoljunk akár a csalásra, a kábítószer-kereskedelemre, vagy a prostitúció esetére. A számítógépes világ folyamatosan változik és fejlődik, ezért a bizonyítás során a nyomozó hatóságoknak is készen kell állniuk arra, hogy sikerrel vegyék fel a harcot ezek ellen.

A digitális bizonyítékok láthatatlanok, mint az ujjnyom vagy a DNS, könnyen elrejthetők, megsemmisíthetők és meg is semmisülhetnek. A digitális bizonyítékok felkutatása esetén gondot kell fordítani az összegyűjtésre, a biztosításra és a szállításra.

Fontos az azonosításuk, méretük és feltalálási helyük dokumentálása, majd a csomagolásuk és a szállításuk. Ennek során figyelemmel kell lenni a megfelelő helyszínbiztosításra, az adatok megváltoztatatlanságára. Ennek során, amennyiben a számítógép bekapcsolt állapotban van, nem szabad megnyitni a különböző fájlokat, nem szabad kikapcsolni szakértő segítsége nélkül. Fontos, hogy ha a képernyő is bekapcsolt állapotban van, le kell fényképezni a képet, ha pedig egy törlőprogram futását észleljük, azonnal áramtalanításra van szükség.

Számítógépek esetében beszélhetünk különféle adattároló eszközökről, amelyek lefoglalása nagymértékben hozzájárulhat a keresett adatállomány

6 Ngaire Genge: The Forensic Casebook. The Science of Crime Scene Investigation. Ballantine Books, New York, 2002, p. 201.

7 Michael D. Lyman: Criminal Investigation. 8th Editon. Pearson, Columbia College of Missouri, 2016, p. 487.

megtalálásához. Ilyenek lehetnek például a külső és belső merevlemezek, USB-porton keresztül használható adattároló eszközök és memóriakártyák. Az adattároló eszközök lefoglalásán kívül fontos megemlíteni a billentyűzetet, az egeret, valamint a gépházat is, amelyeken szintén jó eséllyel találhatók ujjlenyomatok, vagy emberi eredetű biológiaianyag-maradványok.[8]

A különböző tárgyak csomagolása esetén pontosan kell dokumentálni a folyamatot, számozást kell alkalmazni, illetve fényképfelvételeket kell készíteni. Ennek során nem szabad elfelejteni, hogy az eszközök esetleg különböző anyagmaradványokat hordozhatnak, ezért nagy odafigyeléssel kell eljárni a minták megsemmisülésének vagy szennyeződésének elkerülése érdekében. A csomagolóanyagnak egy nem statikus papírzacskónak kell lennie, de az egyes tárgyak eredeti tárolódobozát is használható. Biztosítani kell, hogy a tárgyak ne sérüljenek, ne rongálódjanak meg a művelet folyamán, illetve a szállításkor. Ha mobiltelefon lefoglalására kerül sor, azt kikapcsolt állapotban, az akkumulátorát és a benne található SIM- és memóriakártyákat kiszedve kell csomagolni.

Szállítás során a digitális adatokat tartalmazó eszközöket óvni kell a fizikai behatásoktól, valamint az elektromos és mágneses mezőktől. Itt fontos megjegyezni, hogy a tárgyra kedvezőtlenül hat a rendőrautóban lévő szolgálati rádió által gerjesztett elektromágneses mező.

Mobiltelefonok, GPS- és PDA-készülékek lefoglalása esetén jó eséllyel lehet hívásadatokhoz, helyszínekhez és különböző útvonalakhoz információt gyűjteni. Itt megemlíthető a bejövő- és kimenőhívás-lista, hívó és hívott adatok, cellainformációk és elmentett útvonaltervek.[9]

Szakértő bevonása

A szakértő bevonásának szükségessége nem szerepel a jogszabályban, mindig az adott eset határozza meg, szükség van-e szakértő bevonására. Ez alapesetben akkor szükséges, ha a bizonyítandó tény megállapításához különleges szakértelem kell, illetve kötelező szakértőt kirendelni, ha a személyazonosítást biológiai vizsgálattal végzik.[10] A digitális adatokról különösen elmondható, hogy már a legelső intézkedések megtételekor javasolt szakértő jelenléte, köz-

8 Kevin Lothridge: Crime Scene Investigation: A Guide for Law Enforcement. National Forensic Science Technology Center, 2013, p. 113.

9 Aric W. Dutelle: An Introduction to Crime Scene Investigation. Second Editon. Jones & Bartlett Learning, 2014, p. 401.

10 A büntetőeljárásról szóló 1998. évi XIX. törvény 99. §.

reműködése. A szakértő jelenlétében, javaslatainak figyelembevételével sokkal eredményesebben kutathatjuk fel, illetve rögzíthetjük az adatokat. A szakértő adott esetben már a helyszínen is meg tudja állapítani, hogy az adott eszköz lefoglalása szükséges-e, ezzel megelőzve a felesleges dolgok elvonását a tulajdonos birtokából. Álláspontom szerint a szakértő aktív közreműködése átveszi az adott szakasz irányítását, iránymutatásával, javaslataival nagyban hozzájárulhat a helyszín minél alaposabb átvizsgálásához. Például egy informatikus szakértő – ha rendelkezésére állnak a megfelelő eszközök – már a helyszínen is átvizsgálhatja a memóriakártyák, merevlemezek, mobiltelefonok tartalmát, ezzel meggyorsítva, megkönnyítve az eljárás e szakaszát.

Ha a szakértő az eljárási cselekménynél nincs jelen, vagy egyéb módon – telekommunikációs eszközön keresztül – nem segíti a munkát, akkor a bizonyítás során határozni kell a szakértő kirendeléséről. A szakértő a részére megküldött kirendelő határozatban foglalt kérdések figyelembevételével vizsgálja át az informatikai eszközöket, adathordozókat, e művelethez speciális keresőprogramok segítik.

A legfőbb szakértői rendszerek közül megemlíthető a Belkasoft[11], a Mobiledit[12], az Autopsy és The Sleuth Kit[13], az Andriller[14], a Caine[15] és az UFED[16]. Ezek a szakértői rendszerek gyakorlatilag ízekre szedik az eszközöket, legyen az számítógép vagy okostelefon, legyen az Windows- vagy Linux-, iOS- vagy Android-alapú. Teljes körű listát képesek összeállítani az eszközökben szereplő adatokról (rejtett fájlokról is), azok keletkezési idejéről, sőt a GPS-koordináták és hívásadatok, cellaadatok segítségével még az eszköz korábbi tartózkodási helyei is megállapíthatók. A programok még a törölt állományokról is tudnak információkkal szolgálni, ezek adott esetben visszaállíthatók. Az igazságügyi szakértő a felsorolt automatikusan működő programok segítségével térképezi fel a digitális adatokat, majd a feltett kérdések megválaszolásával alakítja ki véleményét. Ha az adatállomány birtoklása jogszabályba ütközik (például gyermekpornográfia esetében), a szakértő törölheti, vagy ideiglenesen hozzáférhetetlenné teheti őket.[17]

11 https://belkasoft.com/ec
12 http://www.mobiledit.com/products/
13 http://www.sleuthkit.org/index.php
14 http://www.andriller.com/
15 http://www.caine-live.net/
16 http://www.cellebrite.com/Mobile-Forensics/Solutions/ufed-pro-series
17 A büntetőeljárásról szóló 1998. évi XIX. törvény 158/B §.

Digitális eszközök alkalmazása a szemlén

A bűnügyi helyszínen a hatóság is alkalmazhatja a rendelkezésére álló legújabb kriminalisztikai eszközöket. A számtalan eszköz közül azokat mutatom be, amelyek a magyar gyakorlatban megtalálhatók. Megítélésem szerint a Nemzeti Szakértői és Kutatóközpont a legfrissebb eljárások kidolgozásának, eszközök tesztelésének centruma. A központon kívüli helyi szervek elvétve alkalmazzák a bemutatott eszközöket, ennek főként a szűkös pénzügyi keret és a megfelelően kiképzett szakemberhiány az oka.

A drón alkalmazása

A drón mint szó, leginkább pilóta nélküli repülőgépet jelent. Napjainkban igen nagy szerephez jut, hiszen nemcsak a civil szektorban, hanem a bűnüldözésben és a rendvédelemben is kiemelt szerepet kap. Elsősorban katonai, illetve hírszerzési feladatok ellátására alkották meg őket, később azonban más területeken is elkezdték alkalmazni.[18] A magyar rendvédelmi szervek is használnak drónokat, alkalmazásukat a jövőben több területre kívánják kiterjeszteni, például rendezvénybiztosításkor, tömegkezelési feladatoknál, a közlekedési helyzet megfigyelésére, terepkutatásnál, elfogásoknál, rajtaütéseknél és szemléknél.[19] A drón alkalmas megfigyelésre olyan területeken, ahol más technikai eszköz alkalmazása nem lenne megoldható, emellett nemcsak nappal, de éjszaka is használható.[20] Kiválóan alkalmazható katasztrófavédelmi feladatok ellátására is, tűzfelderítésre vagy épp kárfelmérésre.[21] Hatótávolság alapján több csoportba sorolhatók, így beszélhetünk csak látótávolságig vezérelhető eszközökről, rádió-távirányítással működő, wifi támogatott és GPS-eszközökről.[22]

Jelenleg nincs olyan magyar jogszabály, amely meghatározná a drónok alkalmazását, hiszen ezeknek jelenleg nem lajstromjelük sincs.[23] A légi közle-

18 Nagy Attila: Pilóta nélküli légi járművek – a technológia bemutatása, aktualitásai, jogi háttere. Szakmai Szemle, 2015/2., 116. o.

19 Petrétei Dávid: A drónok kriminál technikai és rendészeti felhasználása. Magyar Bűnüldöző, 2015/1–3., 3. o.

20 Petrétei Dávid: Kriminalisztikai fényképészet – helyszínek fényképes dokumentálása. In: Szabó Gyula (szerk.): Munkabaleseti helyszínek dokumentálása. Óbudai Egyetem, Budapest, 2014, 11–12. o.

21 Vránics Dávid – Üveges András: Pilóta nélküli légi járművek fejlődése. Felderítő Szemle, 2015/2., 130. o.

22 Uo. 128. o.

23 Petrétei Dávid (2014): i. m. 4. o.

kedésről szóló 1995. évi XCVII. törvény hatálya alá tartoznak, és használatukra a Nemzeti Közlekedési Hatóság Légügyi Hivatalától kell engedélyt kérni.[24] Természetesen történik próbálkozás a jogi háttér megteremtésére, hiszen ez mind a civil szektor, mind a rendvédelem szempontjából elengedhetetlen, így példa lehet hazánk számára az Egyesült Államokban vagy épp Németországban alkalmazott szabályozás.[25] A drónok alkalmazása természetesen több veszélyt is rejt magában, hiszen szándékos jogellenes cselekmények elkövetésére is felhasználható, így minden esetben szükség van a kockázatok felismerésére, és ezek szabályozására, akár úgy, hogy engedélyhez kötjük az alkalmazásukat.[26]

A drónok jövőbeni szélesebb körű alkalmazása megjelenhet egyebek között a gyanúsítottak megfigyelésében, felkutatásában (akár infrakamera segítségével), védett személyek és területek biztosításában, wifihálózat ellenőrzésében vagy zavarásában, valamint a határvédelem terén. Drónokat nemcsak a hatóságok vethetnek be, hanem akár az elkövetők is. Gondolhatunk akár az embercsempészés bűncselekményére, ahol az elkövetők is megfigyelhetik a járőrök mozgását a határterületen. A drón esetleges lefoglalása is segítséget nyújthat a bizonyítás során, hiszen GPS-adatokat tárolhat, e koordináták térképre illesztése megmutatja az eszköz korábbi mozgásának helyszínét.

3D térszkenner

A 3D térszkenner napjainkban a térbeli adatszerzés legjobb módszere, hiszen gyorsan, több millió pont koordinátáiból megállapítható egy objektum geometriai adata.[27] A körbeforgó lézer gömbhéjszerűen letapogatja a környezetet, akár olyan sűrűséggel, hogy ötven méter távolságban minden négyzetmilliméterre jut egy sugár. A szoftver a kész gömbpanoráma-felvételt ráilleszti a fénypontfelhőre. A különböző álláspontokból felvett fénypontfelhőket és gömbpanoráma-képeket a szoftver hibátlanul összeilleszti. Abból a célból, hogy használható legyen a kész anyag, elegendő álláspontból kell a felvételeket elkészíteni, nehogy valamely terület kimaradjon. A térszkenner magassága fix, a lézersugár pedig egyenes. A helyszínen kell meghatározni, hogy

24 Nagy Attila: i. m. 117. o.

25 Petrétei Dávid (2014): i. m. 6–8. o.

26 Beck Attila: Az UAV-k polgári alkalmazásának kockázatai, és kezelésük lehetséges módszerei terrorelhárítási és személyvédelmi szempontból. (T)error&elhárítás, 2015/2., 3. o. http://epa.oszk.hu/02900/02932/00008/pdf/ EPA02932_terror_elharitas_2015_2_01.pdf

27 Pásztor László: A 3D térszkenner működése, tapasztalatok, lehetséges további felhasználási területek. Belügyi Szemle, 2016/7–8., 65. o.

hol legyenek az egyes álláspontok, illetve egyáltalán hány álláspontból szükséges felvételt készíteni. A kész kép térben elforgatható, így szinte beleélhetjük magunkat a helyszínbe.[28]

A 3D térszkenner megfelelően használható műemlékvédelem, ipari alkalmazás, eszközgyártás, katasztrófavédelem, igazságügy, valamint a bűnügyi nyomozás során.[29] Maga az eszköz alkalmas metszetek készítésére, rekonstrukcióra.[30] Eltérő változatai vannak, így beszélhetünk állványos 3D lézerszkennerről, fogászati szkennerről vagy kézi szkennerről. Míg a térszkenner fontossága az összképrögzítésnél ragadható meg, addig a kézi szkenner a nyomrögzítésnél kap meghatározó szerepet.[31] A 2015. július 11-én, Tatabányán, lőfegyverrel elkövetett emberölés helyszínén a térszkenner segítségével megállapíthatóvá vált az elkövető helyzete a lövés pillanatában, illetve az, hogy célzottan történt-e az elkövetés.[32]

Talajradar

A talajradart 2014 óta alkalmazzák a bűnügyi helyszíni szemléknél.[33] A talajradar képes felismerni a talaj összetételétől eltérő objektumokat, és ezáltal megmondani azok pontos helyét és mélységét. A talajradarral történő vizsgálat kétféle módon történik, az egyik módja a helyszíni mérő és jelölő módozat, míg a másik a rácshálós módszerrel történő feltérképezés és vizsgálat.[34] A talajradar bűnügyekben való alkalmazását jelentős eredmények támasztják alá, így indokolt a jövőbeni alkalmazás. Gyakorlati példát említve a talajradart akár elrejtett, elásott holttestek felkutatására is használni lehet.

Képalkotás

A képalkotás jelentőségét véleményem szerint nem kell hangsúlyozni, hiszen a krimináltechnika egyik fő szakterülete. A képkészítés az idők folyamán jelentős fejlődésen ment keresztül, amíg eljutott a ma ismert és alkalmazott eljárásokig. Míg az 1950-es években sztereofényképek készültek, napjainkban

28 Petrétei Dávid (2014): i. m. 107. o.
29 Pásztor László: i. m. 66. o.
30 Uo.
31 Petrétei Dávid: Háromdimenziós képalkotás a kriminalisztikában. Belügyi Szemle, 2016/7–8., 84. o.
32 Pásztor László: i. m. 67. o.
33 Mama Sándor – Gárdonyi Gergely: A talajradar használatának gyakorlati tapasztatai a hazai bűnügyi helyszínelésben. Belügyi Szemle, 2016/7–8., 70–71. o.
34 Uo.

a digitális képek uralják a világot, ezek közé sorolható a helyszínelésnél alkalmazott gömbpanorámakép.[35]

A modern gömbpanorámakép-rögzítők (például PanoScan, SpheronVR) méretarányos digitális képeket hoznak létre, amelyeken utólagos mérések is végezhetők. Továbbá a számítógép segítségével elkészített gömbpanoráma gyakorlatilag szabadon mozgatható-forgatható, így háromdimenziós modell lesz. A megörökített virtuális helyszín fényképminőségű részleteihez a programban hozzárendelhetünk helyszíni fényképeket, jegyzőkönyvrészleteket, vagy videófelvételeket. A legfejlettebb háromdimenziós képalkotó rendszer jelenleg a háromdimenziós lézeres térszkenner.[36]

Pásztázó elektronmikroszkópia

Az első elektronmikroszkópot 1935-ben alkották meg, azóta számos példány készült belőle, jelentőségét pedig annak köszönheti, hogy egyrészt a minta előkészítése egyszerű, másrészt a legjobb adatokat ismerhetjük meg általa.[37] A pásztázó elektronmikroszkópnak alapvetően két fő része van, az egyik a torony, a másik a vezérlő egység, a tápegység, a kép létrehozásához pedig fókuszált elektronsugarat alkalmaznak.[38] A pásztázó elektronmikroszkóp leginkább felületek letapogatására, valamint preparátumok megvizsgálására, anyagösszetétel megállapítására alkalmas. Lényegét és működését tekintve elmondható, hogy *„az e-nyaláb – minta kölcsönhatásból származó jeleket detektáljuk, majd erősítés után képalkotásra használjuk”.* Az elektronmikroszkóppal a képalkotásra több lehetőség is van, alkalmazhatjuk a visszaszórt elektronmódszert, a szekunder elektronmódszert vagy a próbaáramos rendszert. Fontos megjegyeznünk, hogy jelentőségét nemcsak annak köszönheti, hogy kis mintáról ad számunkra információt, hanem a felület összetételének megállapítására is alkalmas.[39] Gyakorlati alkalmazása az anyagmaradványok vizsgálatára terjed ki, különösen a csappantyú-anyagmaradványok felkutatására.[40]

---

35 Petrétei Dávid (2016): i. m. 77–79. o.

36 Petrétei Dávid (2014): i. m. 106. o.

37 Havancsák Károly – Dankházi Zoltán: Pásztázó elektronmikroszkópia. ELTE anyagfizikai tanszék, Budapest, 2016, 1. o. http://metal.elte.hu/oktatas/alkfizlab/meresleirasok/SEM3.pdf

38 Tóth Zsolt: A Hitachi S4700 pásztázó elektronmikroszkóp bemutatása és kezelési útmutatója. Szeged, 2006, 1–2. o. http://www.muszeroldal.hu/measurenotes/S4700_utmutato.pdf

39 Szakács Hajnalka – Varga Csilla – Nagy Roland: Polimerek méréstechnikája. Pannon Egyetem, Budapest, 2012, 1. o.

40 https://leb.fbi.gov/2011/may/the-current-status-of-gsr-examinations

Röntgen

A post mortem radiológia segítségével a testről olyan átvilágító, feltérképező felvételeket készíthetünk, amelyek támpontot adhatnak az elkövetés körülményeiről. A röntgensugárzás nagy energiájú elektromágneses sugárzás, amelynek hullámhossza a néhányszor 10 nanométer és a néhányszor 10 pikométer közé esik. Legfontosabb felhasználási területei az orvostudomány és a kristálytan. A röntgensugárzásban terjedő röntgenfoton energiája élettanilag veszélyes. A röntgensugarak biológiai hatása – gondos adagolás és ellenőrzés esetén – sok betegség gyógyításánál előnyösen alkalmazható (röntgenterápia rosszindulatú daganatos megbetegedéseknél). Az eljárás kifejlesztése *Wilhelm Conrad Röntgen* német tudós nevéhez köthető (1895). Napjainkban a radiológiát a személyazonosításban, a kormeghatározásban és a halál okainak vizsgálatára is használják. Emellett az igazságügyi radiológia megtalálható a csomagok és járművek átvizsgálásánál, kábítószerek kutatásánál és művészeti tárgyakkal kapcsolatos csalásoknál.

Alkalmazása a gyakorlatban megtalálható csontok törésének megállapításában, a lövedékek károkozásának és egyéb sérülések vizsgálatában, valamint az ujjlenyomat és a DNS mellett mint kisegítő lehetőség, segítségül szolgálhat a személyazonosításban. Erre példa egy törött csontról készült röntgenfelvétel összehasonlítása az orvosi nyilvántartásokban szereplőkkel.[41]

CT

A komputertomográfia (CT) a radiológiai diagnosztika egyik ága. A tomográfia szó szeletre utal. A tomográfiás felvételeken a vizsgálat tárgya képzeletbeli szeletekre bontva látható. Az eszköz kifejlesztéséért 1979-ben *Allan M. Cormack* és *Godfrey N. Hounsfield* orvosi Nobel-díjat kapott.

A komputertomográfia a röntgen-átvilágítási technika továbbfejlesztésének tekinthető. A tomográfiás felvétel esetében vékony, síkszerű röntgensugárnyalábbal világítják át a vizsgált objektumot. Az objektum mögött elhelyezett detektor egy vonal mentén érzékeli, hogy a sugárnyalábból hol és mennyi nyelődött el. Az eljárás befejeztével a vizsgált test térbeli szerkezete feltérképezhető.[42] A modern CT-berendezések egy körülfordulás alatt egyszerre több (akár 128) szeletet térképeznek fel, és egy vizsgálat a szükséges

41 http://www.jofri.net/
42 http://www.forensicmag.com/article/2009/08/necro-radiology-postmortem-ct-scans-are-rise

számítások elvégzésével együtt néhány perc alatt elvégezhető, így alkotva meg a vizsgált objektum térbeli rekonstrukcióját.[43]

MRI

Az MRI (Magnetic Resonance Imaging) jelentése mágnesesmagrezonancia-képalkotás. A technikát elsősorban az orvosi diagnosztikában használják a test szerkezetének leképezéséhez. Emellett az agyi képalkotás területén is alkalmazzák. Előnye a komputertomográfiához képest, hogy jobb a kontrasztfelbontó képessége a lágy szövetek területén. Létezik a strukturális MRI-vizsgálat (sMRI) mellett úgynevezett funkcionális mágnesesrezonancia-vizsgálat (fMRI) is, amellyel a vizsgált szervek működéséről kapható információ. Az MRI valójában inkább eszközök gyűjteményének tekinthető, egy nagyon összetett képalkotó eljárás.[44]

MDCT

A hosszú vizsgálati idő, a számottevő sugárterhelés és a leletek gyakori értékelhetetlensége miatt szükség volt technológiai váltásra. Az orvosi berendezések folyamatos fejlődésével ma már negyedik generációs multidetektoros (többszeletes spirál) CT (MDCT) berendezések állnak rendelkezésre, amelyek előnye a magas szeletszám, a megfelelő tér- és időbeli felbontás, valamint a pácienst érő sugárterhelés mérséklődése. Ezekkel a modern berendezésekkel ma már akár egy-két másodperc alatt elvégezhető a vizsgálat. Megjegyzendő, hogy bár néhány perc alatt több ezer képet készíthetünk, ezek kiértékelése nyilván sokkal több időt vesz igénybe. A 2005-ben bemutatott két sugárforrású dual-source CT (DSCT) – amilyet a Pozitron-diagnosztika Központ is használ – ilyen készülék. A DSCT felépítése abban különleges, hogy a berendezésben két különálló 64 szeletes felvételező rendszer van egymáshoz képest 90 fokban elforgatva, elhelyezve, amelyekkel negyed fordulat alatt leképezhető a teljes látómező.[45]

A bűnügyi célú ujj- és tenyérnyomat-felvételi munkaállomás

A bűnügyi nyilvántartásba vétel során számos ujj- és tenyérnyomatok felvételét elősegítő eszköz alkalmazható.

---

43 http://www2.le.ac.uk/departments/emfpu/imaging/brief-history
44 http://emedicine.medscape.com/article/1785023-overview
45 http://emedicine.medscape.com/article/1785023-overview#a2

A LiveScan berendezés szoftvere az ujj- és tenyérnyomatokat elektronikusan rögzíti és dolgozza fel. A rendszer tökéletesen illeszkedik a Cogent automatizált ujjlenyomat-azonosító rendszerhez (CAFIS). A munkaállomás a bűnügyi célú ujj- és tenyérnyomat-rögzítés teljes folyamatát lefedi, alkalmas a nyomok rögzítésére, az adatbevitelre, a nyomatlap nyomtatására és a rögzített adatok továbbítására. Az ujj- és tenyérnyomatok rögzítéséhez a CS500P élőolvasó szkenner szükséges. A termék az FBI által hitelesített.
A nyomatrögzítés a személyes adatok bevitele után három fázisból áll:

– a tízujjas sík nyomatok levétele;
– a tízujjas átforgatott nyomatok levétele; valamint
– a tenyérnyomatok levétele.

A nyomatok levétele előtt meg kell győződni arról, hogy az alany keze és a LiveScan üveglapja tiszta és szennyeződésmentes. Ha az alany bőre túlságosan izzadt vagy túl meleg, a nyomat túl sötét lesz. Ebben az esetben az alany kezének megtisztítása szükséges. Ha az alany bőre túl száraz, vagy túl hideg, a nyomat túlságosan világos lesz, ez esetben nedvesítésre van szükség. Ha a sík ujjnyomok gyenge minőségűek, a rendszer folyamatosan hibaüzenetet jelenít meg, amikor az átforgatott ujjnyomok fázisában vagyunk, mert nincs összehasonlításra alkalmas, megfelelő nyomat. Ha a rendszer egy ujjnyomatot annak gyenge minősége miatt vagy a helytelen sorrend miatt elveti, figyelmeztet, hogy rögzítsük újra az adott ujjnyomatot.

A LiveScan egy átforgatottujjnyomat-rögzítő ablakot kínál fel minden egyes ujj számára. Ebben a szakaszban a rendszer nemcsak a képek minőségét ellenőrzi, de a helyes sorrend érdekében összeveti őket a már meglévő sík ujjnyomatok képeivel.

A tenyérnyomat levételénél külön figyelmet kell fordítani a tenyér felső részének erős nyomására (interdigitális terület), mert ez a rész a tenyérnyomat kiértékelésénél jelentős információkkal szolgál a szakértőknek. Ha sérülés vagy amputáció van valamelyik kézen, ez bejelölhető a rendszerben.

A nyomatvétel után a küldés gomb megnyomásával a szoftver az adatokat automatikusan továbbítja a központi nyilvántartásnak, amely minden tranzakcióra válaszüzenetet küld.[46]

46 LiveScan Bűnügyi célú ujj- és tenyérnyomat felvételi munkaállomás felhasználói kézikönyv. ORFK, Budapest, 2011

Az Alphonse személyleírási rendszer

A bűncselekményt elkövető személyt némely esetben tanúk látják. A tanúk – ideértve a sértettet is – kihallgatásakor nemcsak a cselekmény lefolyásáról szükséges kikérdezni, hanem az elkövető személyére vonatkozóan is, különösen akkor, ha nincs térfigyelő kamera, az elkövető elhagyta a helyszínt, illetve személyazonossága ismeretlen. Mára lehetőség nyílt az elkövetőről adott személyleírást számítógépes program segítségével feldolgozni és megjeleníteni, ami nagyban segíti a hatóságokat.

A rendszert *Alphonse Bertillon*ról, az antropometria és az első személyleírási rendszer megalkotójáról nevezték el. A fényképfelvételek, az ujj- és tenyérnyomatok, valamint a DNS-profilok mellett a személyleírásnak is nagy jelentősége van az azonosításban. A rendőrségi programba integrált (Robotzsaru Neo) modul lehetővé teszi, hogy az elkövetőt észlelő személy minden olyan külső tulajdonságot megadjon, amely azonosíthatóvá teszi a terheltet. A program lehetőséget nyújt, hogy lépésről lépésre, tetőtől talpig felvigyék azokat az elkövetőt jellemző ismérveket a járástól kezdve a piercingig.

A személyleírási rendszer kidolgozásában részt vettek orvos szakértők, antropológusok, nyelvészek, tetoválóművészek, fodrász és piercingszakértők is abból a célból, hogy a legátfogóbb fogalmakat és képi megjelenítési módokat integrálják a rendszerbe. Ennek köszönhetően a legapróbb részletekig leírható, hogy az elkövetőnek milyen volt például az orra, a szája, a járása, a tetoválása, a bőrszíne és még sok más jellemzője.

A rendszerbe vitt adatok segítséget nyújtanak abban, hogy a nyomozó hatóságok keresést hajtsanak végre benne, ezáltal összekapcsolhatóvá válhatnak helyszínek, elkövetők, bűncselekmények. Például segítséget nyújthat abban az esetben, ha Budapesten elkövetnek egy rablást, majd a szemtanúk a tettes testfelépítéséről, vagy akár tetoválásáról részletes leírást adnak. Ebben az esetben a rendszerbe szükséges az adatokat bevinni, majd keresést végrehajtani, amelynek eredményeképp egy korábban nyilvántartásba vett személy kerülhet látótérbe.[47]

IRODALOMJEGYZÉK

Beck Attila: Az UAV-k polgári alkalmazásának kockázatai, és kezelésük lehetséges módszerei terrorelhárítási és személyvédelmi szempontból. *(T)error&elhárítás,* 2015/2.

47 Az ORFK Bűnügyi Értékelő-Elemző Osztály 8/E/2016/5876-os számú akkreditált képzési programja. Budapest, 2016

Dutelle, Aric W.: An Introduction to Crime Scene Investigation. Second Editon. Jones & Bartlett Learning, 2014

Fenyvesi Csaba: A kriminalisztika tendenciái. Dialóg Campus Kiadó, Budapest–Pécs, 2014

Genge, Ngaire: The Forensic Casebook. The Science of Crime Scene Investigation. Ballantine Books, New York, 2002

Havancsák Károly – Dankházi Zoltán: Pásztázó elektronmikroszkópia. ELTE anyagfizikai tanszék, Budapest, 2016

Lidstone, Ken – Bevan, Vaughan – Palmer, Clare: Bevan and Lidstone's The Investigation of Crime. A Guide to Police Powers. Second Editon, Butterworths, 1996

Lothridge, Kevin: Crime Scene Investigation: A Guide for Law Enforcement. National Forensic Science Technology Center, 2013

Lyman, Michael D.: Criminal Investigation. 8th Editon. Pearson, Columbia College of Missouri, 2016

Mama Sándor – Gárdonyi Gergely: A talajradar használatának gyakorlati tapasztatai a hazai bűnügyi helyszínelésben. *Belügyi Szemle,* 2016/7–8.

Nagy Attila: Pilóta nélküli légi járművek – a technológia bemutatása, aktualitásai, jogi háttere. *Szakmai Szemle,* 2015/2.

Pásztor László: A 3D térszkenner működése, tapasztalatok, lehetséges további felhasználási területek. *Belügyi Szemle,* 2016/7–8.

Petrétei Dávid: A drónok krimináltechnikai és rendészeti felhasználása. *Magyar Bűnüldöző,* 2015/1–3.

Petrétei Dávid: Háromdimenziós képalkotás a kriminalisztikában. *Belügyi Szemle,* 2016/7–8.

Petrétei Dávid: Kriminalisztikai fényképészet – helyszínek fényképes dokumentálása. In: **Szabó Gyula (szerk.):** Munkabaleseti helyszínek dokumentálása. Óbudai Egyetem, Budapest, 2014, 11–12. o.

Szakács Hajnalka – Varga Csilla – Nagy Roland: Polimerek méréstechnikája. Pannon Egyetem, Budapest, 2012

Tóth Zsolt: A Hitachi S4700 pásztázó elektronmikroszkóp bemutatása és kezelési útmutatója. Szeged, 2006

Vránics Dávid – Üveges András: Pilóta nélküli légi járművek fejlődése. *Felderítő Szemle,* 2015/2.

DOI: 10.38146/BSZ.2018.7-8.11

RÁDI NORBERT – CZÁR ZSANETT

A csengelei ügy tapasztalatai

Csengele egy 60,66 négyzetkilométeren szerényen meghúzódó, átlagos, nyugodt, csendes, szerethető kisközség a Dél-Alföldön, Csongrád megye északi részén, a Kisteleki járásban. 2033 fős lakossága főként a mezőgazdaságban tevékenykedik az év minden napján. A település mellett halad el az M5-ös autópálya, amelynek a 128-as kilométerénél található egy pihenőhely.

Hajnali ébresztés – a kezdet

2017. december 5. az a nap, amellyel Csengele a bűnügyi híradások fókuszába került, a nap, amikortól a kisközség nevének hallatán nemcsak a helyiekben, hanem az egész országban egy bűntény emlékképe rémlik fel.

Hajnalban csörög a készenlétes nyomozók, vizsgálók és a technikus telefonja. Az ügyelet közli, hogy a legrövidebb időn belül a szolgálati helyre kell vonulniuk, mert lövöldözés volt az autópályán, a Csengele pihenőnél.

Azonnali ébredés, villámgyors készülődés, irány a helyszín. Három csapat alakul: ki bent, a rendőrségen az irodájában várja a híreket, ki a helyszínre indul, mások a Csengele pihenőnél gyülekeznek.

Két külföldit lőttek le pisztollyal, egyikük halott, a másik életveszélyesen megsérült. Kezdődik a verziók felállítása. Mi lehet az emberölés indítéka? Pénz? Szerelemféltés? Leszámolás? Maffiagyilkosság? Embercsempészés? Sok kolléga, sok elmélet, mindenki ötletel.

Elindul a rendőri munka, a helyszíni szemle, a nyomok felkutatása, a lehetséges tanúk kihallgatása, adatgyűjtés, kamerakutatás.

Siralmasan kevés az elsődleges kapaszkodó: senki sem látott semmit. Néhány lőszerhüvely, egy keréknyom a havas aszfalton, egy kamera, amely talán működik. Így kezdődött.

Szigorú tények – ami történt

Egy ismeretlen férfi 2017. december 5-én, 3 óra 20 perckor segélyhívást kezdeményezett, amit az Országos Rendőr-főkapitányság hívásfogadó központja fogadott. A férfi zaklatott volt, német és román nyelven mondta el, hogy a hívás előtt nem sokkal az M5-ös autópálya egyik pihenőjén fegyveresek megtámadták; a barátja meghalt, ő pedig megsérült.

A Csongrád Megyei Rendőr-főkapitányság tevékenységirányítási központja azonnal riasztotta az Országos Mentőszolgálatot, továbbá két rendőri egységet küldött a helyszínre, amelyek a bejelentés valódiságát ellenőrizték, valamint információt gyűjtöttek a további szükséges intézkedésekhez.

A Bács-Kiskun Megyei Rendőr-főkapitányság tevékenységirányítási központját is tájékoztatták – mivel a pontos helyszín és egyéb körülmények ekkor még nem voltak ismertek –, onnan további járőrpárt indítottak.

A járőrök a kiérkezés után azonnal jelentették, hogy a bejelentés valós. Elmondták, hogy 3 óra 15 perckor az M5-ös autópálya Szeged felé vezető oldalán, a Csengele pihenőhelyen egy ismeretlen férfi több lövést adott le egy osztrák honosságú Ford Galaxy típusú gépjármű vezetőjére és utasára. A sofőr, egy 39 éves bolgár férfi a támadás után meghalt, 56 éves osztrák utasa pedig életveszélyes hasi sérülést szenvedett. Az ismeretlen elkövető a helyszínt gépjárművel hagyta el.

Megállapították továbbá azt is, hogy a segélyhívást egy román férfi kezdeményezte a sérült utas telefonjáról. A bejelentő a bűncselekményt nem látta, de az áldozatokra ő talált rá.

Elsődleges intézkedések

A helyszínre érkezett a Csongrád Megyei Rendőr-főkapitányság bűnügyi osztályának vezetője is, akit a „forró nyomon” üldözés parancsnokának jelöltek ki. Három csoport alakult.

A bizottság orvos és fegyverszakértővel kiegészülve megkezdte a helyszíni és halottszemlét, a berendelt bűnügyi állomány további nyomozói pedig a pihenőben tartózkodó lehetséges tanúk felkutatását és adatgyűjtést végeztek.

A második csoport – mivel mind a sértettek, mind pedig a tettes az autópályán érkezett a bűncselekmény elkövetésének helyszínére – a pihenőhelyek és a pálya menti üzemanyagtöltő állomások biztonsági és térfigyelő kamerái által rögzített felvételek kimentésére intézkedett.

A harmadik csoport – elemző-értékelő tisztekkel kiegészülve – a főkapitányságon hajtotta végre az adatbázisokból a lekéréseket, a rendszeradatok ellenőrzését és a kapott információk elemzését.

A helyszíni és halottszemle egyszeri és megismételhetetlen, az annak során rögzített nyomok a bizonyítás során kiemelkedő jelentőségűek. Rendkívül aprólékos, pontos, precíz és szakszerű szisztematikus tevékenységet igényel, emiatt azonban hosszan tartó nyomozási cselekmény. Mindenképpen párhuzamos munkavégzésre volt szükség. Az elsődleges adatok alapján nem volt felkutatható olyan személy, aki az elkövető azonosításához érdemi információval birtokában lett volna, hiszen éjszaka történt az esemény, ezért a látási viszonyokat nehezítette a sötétség, másrészt pedig a pihenőben tartózkodók többsége aludt, és csak a lövésekre riadt fel. A sértettek egyike meghalt, az egyetlen szemtanú pedig – aki életveszélyesen megsérült – nem volt kihallgatható, műtéti beavatkozásra várt.

A nyomozás megkezdéséhez a kiindulópont az áldozatok által használt gépjármű forgalmi rendszáma, és az elkövetés helyszíne volt.

Mindezek alapján, a nyomozó csoport kizárólag a digitális nyomok felkutatásától, elemzésétől és értékelésétől várhatott eredményt.

Lépésről lépésre

A Csengele pihenőhelyen felszerelt térfigyelő kamerákat kezelő Alföld Koncessziós Autópálya Zrt.-t kértük, hogy a felvételeket őrizze meg, majd intézkedtünk a lefoglalásukra. A megszerzett videókat a nyomozók órákon át nézték visszza, és részletesen elemezték. A felvételeken látható volt a bűncselekmény és annak főbb mozzanatai.

Viszont indokolt volt a képminőség javítása, mivel a tettes személyazonossága és az általa használt gépjármű típusa, valamint egyéb egyedi azonosításához szükséges ismérvei nem voltak felismerhetők.

A Nemzetbiztonsági Szakszolgálat Szakértői Intézet Fotó- és Videótechnikai Laboratóriumában speciális informatikai programok felhasználásával megkezdték a felvétel minőségi javítását, ennek eredményére néhány órát várni kellett.

Ami bizonyos volt, hogy a sértettek 2 óra 47 perckor érkeztek a Csengele pihenőhelyre, majd két perccel később egy ismeretlen típusú, szürke gépjármű hajtott be utánuk, és beállt a már korábban ott parkoló kamionok mögé. Nem sokkal ezután vélhetően egy férfi szállt ki az autóból, aki a pótkocsik takará-

sát kihasználva, több alkalommal kitekintett, és szemmel tartotta a sértettek járművét. Rövid várakozás után odament áldozataihoz, akik az autójukban ültek. A sofőr és utasa pihent, aludni próbált. A támadó 3 óra 15 perckor, higgadtan, lassú léptekkel a vezetőoldalhoz sétált, megállt, majd bekopogott az ablakon. Úgy látszott, mintha egy pisztolyt tartott volna a kezében. Néhány másodperccel később szóváltás vagy egyéb előzmény nélkül, közvetlen közelről tüzet nyitott a járműben ülő férfiakra. Mindezek után higgadtan visszasétált a saját autójához, beszállt, és elhajtott a helyszínről.

A látottak alapján a nyomozó csoport azt feltételezte, hogy az elkövető ismerhette áldozatait, cselekményét személyes okok motiválhatták, és akár hosszabb ideje is követhette az autópályán haladó sértetteket. A Csongrád Megyei Rendőr-főkapitányság elemző-értékelő osztálya lekérte az M5-ös és M43-as autópályák kapuinak adatait.

Mivel a Nemzeti Útdíjfizetési Szolgáltató (NÚSZ) Zrt. által üzemeltetett informatikai rendszer adatbázishoz közvetlen hozzáférést kínáló végpontot akkor még csak a Készenléti Rendőrség Nemzeti Nyomozó Iroda érhette el, a társszervet bevontuk a nyomozásba. A részadatokat folyamatosan átadták elemzőinknek.

Az elemzést végző szakértők öt perccel a sértettek előtt és után közlekedő járművekre koncentráltak, így hat lehetséges gépjárműre redukálták az autók körét. E hat autó közül volt valamelyik összefüggésbe hozható a bűncselekmény elkövetésével.

10 óra 10 percre már hat NÚSZ- és egy VÉDA-kapu adatállományának összevetése történt meg. A kiértékelés alapján bebizonyosodott, hogy a bűncselekmény elkövetésével egy német honosságú Renault Megane típusú személygépkocsi hozható kapcsolatba.

Mindezek után a nyomozók már az inkriminált gépjárműre fókuszáltak.

A további adatlekérések szerint pontosan megállapíthatóvá vált a feltételezett elkövető és a sértettek haladási útvonala, amelyről ponttérkép készült.

Nem sokkal 23 óra után a sértettek Levélnél, az M1-es autópályán haladtak, majd feltűntek Abda–Bőny–Tata térségében. Utóbbi helyszínen 0 óra 15 perckor rögzítette a NÚSZ- és a VÉDA-rendszer az elhaladásukat, majd néhány másodperccel később követte őket a Renault Megane.

A tatai helyszín után hat további városnál telepített kapu adatai igazolták, hogy a tettes hosszasan követte áldozatait.

A bűncselekmény után a fegyveres a járművel Kecskemétnél, Ócsánál és Levélnél haladt el, végül elhagyta Magyarország területét, és Ausztriába távozott.

A sértettek és a követőjük útvonalán végighaladva szükségessé vált valamennyi biztonsági és térfigyelő kamera felvételének lefoglalása. Ennek érdekében a Győr-Moson-Sopron, a Pest és a Bács-Kiskun Megyei Rendőr-főkapitányság segítségét kértük a felvételek felkutatása és megőrzése céljából. Ellenőriztük, hogy a külföldiek megálltak-e útjuk során valahol, történt-e olyan esemény, ami a gyilkossághoz vezetett, kerestük a lehetséges motivációt.

Vélelmeztük továbbá, hogy nemcsak a sértetteknél, hanem a tettesnél is lehetett egy vagy több mobiltelefon, ezért a nyomozó csoport egy része a Csengele autópálya pihenőt lefedő bázisállomások szolgáltatóit kereste meg, részben írásos formában, részben pedig az elemző-értékelő osztály mint közvetlen lekérésre jogosult szervezeti egység segítségével. A sértetteknél a szemle során megtalált SIM-kártyák hívószámainak és híváslistaadatainak beszerzésére is intézkedtünk, azonban az elemzés után érdemi információ nem vetődött fel.

A felderítő osztály elvégezte a Csongrád megyei autópálya-szakasz többi pihenőhelyén az adatgyűjtést, de a nyomozást segítő körülmény nem vált ismertté.

Közben stabilizálták az életveszélyes sérült állapotát, de továbbra sem volt kihallgatható. Ébredése után annyit tudott elmondani, hogy az elkövető egy ismeretlen, 50 év körüli, kb. 165 centiméter magas, barna bőrű, szakállas férfi, aki fekete ruházatot és sapkát viselt. Elmondta azt is, hogy az osztrák–magyar határ után nem sokkal megálltak autópálya-matricát vásárolni.

Utóbbi információ alapján – mivel vélelmeztük, hogy az elkövető már akár indulásuktól követhette a sértetteket – megállapítottuk a vásárlás pontos helyét, majd a Győr-Moson-Sopron Megyei Rendőr-főkapitányság együttműködésével beszereztük a mosonmagyaróvári pénzváltó és e-matrica-árusító pavilon felvételét. A videón azonban csak a sértettek gépjárműve, valamint az utóbb elhalálozott sofőr vásárlása volt látható, az elkövető nem.

Az első fontos nyom

Az elemzőmunka során kiszűrt német honosságú Renault Megane volt az egyetlen olyan nyom, amely a tetteshez vezethetett. Az úgynevezett prümi rendszer adatállományában – amely a külföldi honosságú gépjárművek azonosítását segíti – a tulajdonos nem szerepelt, csak az üzemben tartó, aki egy Törökországban született 57 éves német férfi volt. Megkerestük a Hegyeshalom–Nickelsdorf közös kapcsolattartási szolgálati hely ügyeletét, valamint a

Nemzetközi Bűnügyi Együttműködési Központot, hogy tájékozódjunk a sértettekről és a Renault-ról, továbbá annak üzemben tartójáról.

Mind a német, mind az osztrák rendőrök azonnal a nyomozók rendelkezésére álltak. Közreműködésükkel beszereztük a feltételezett elkövető által használt jármű üzemben tartójának fényképét, adatait, valamint a bűnügyi előéletére vonatkozó információkat.

A férfi nemzeti elfogatóparancsának kibocsátásáról határoztunk, egyidejűleg előterjesztést tettünk a Csongrád Megyei Főügyészségen az európai nyomozási határozat kezdeményezésére. Az eljárási jogsegély keretében kértük az üzemben tartó kihallgatását, valamint lakásának átkutatását.

A német rendőrség néhány óra leforgása alatt a kért nyomozási cselekményeket elvégezte. A kihallgatott férfi elismerte, hogy ő a keresett Renault üzemben tartója. Elmondta, hogy az autóját az Ausztriában élő testvérének adta, és úgy tudja, hogy azóta is öccse használja. Ezen kívül a bűncselekmény elkövetésének időpontjára ellenőrzött alibit igazolt.

Az áttörés

A férfi vallomása alapján ismét az osztrák rendőrség segítségét kértük. A társhatóság rendőrei azonosították a testvért, megállapították a tartózkodási helyét, és átadták a kért háttér-információkat is. Az 52 éves férfi Törökországban született, Ausztriában élt, de állampolgársága német volt. Az osztrák nyomozóktól kapott fényképe alapján hasonlított a sértett által körülírt támadóra.

A Csongrád Megyei Rendőr-főkapitányság nyomozói a fénykép birtokában a kórházba mentek, majd a képet megmutatták a sérültnek. Az illető azonnal és minden kétséget kizáróan azonosította támadójukat.

A meghallgatással egy időben kutatást végeztünk a Facebookon, ahol sikerült azonosítani a lehetséges elkövető profilját. A feltöltött fényképek közül több olyat találtuk, amelyek arra utaltak, hogy a gyanúsított szoros, baráti kapcsolatot ápolt későbbi áldozatával.

Kattan a bilincs

Azonnal intézkedtünk az országos körözés elrendelésére, valamint előterjesztést tettünk európai és nemzetközi elfogatóparancs kibocsátására. Továbbá újabb európai nyomozási határozatban házkutatást és kihallgatást kértünk.

A Nemzetközi Bűnügyi Együttműködési Központ igazgatója december 6-án, nem sokkal 19 óra előtt értesítette a nyomozó csoport vezetőjét, hogy az osztrák rendőrség különleges egysége a lakóhelye közelében elfogta a bűncselekmény elkövetésével megalapozottan gyanúsítható személyt. A cselekményhez használt gépjárművet is megtalálták és lefoglalták. A személyautó átvizsgálása során a rendőrök egy rejtekhelyet fedtek fel, abban egy maroklőfegyver volt, ami – típusát tekintve – a bűncselekmény eszköze is lehetett. Ausztriában végrehajtott kihallgatáson az elfogott és előállított férfi elismerte a bűncselekmény elkövetését. Haladéktalanul intézkedtünk a terhelt magyar hatóságoknak történő átadására, a büntetőeljárás lefolytatása céljából.

Az osztrák hatóságok hozzájárultak a gyanúsított kiadásához, és az Igazságügyi Minisztérium közreműködésével 2017. december 21-én a Hegyeshalom–Nickelsdorf közös kapcsolattartási helyen megtörtént a gyanúsított átadása. A Csongrád Megyei Rendőr-főkapitányság bűnügyi osztályán végrehajtott gyanúsítotti kihallgatás során a feltételezett elkövető beismerte, hogy ő adta le a lövéseket. A nyomozás jelenlegi állása szerint haragosa volt az áldozat, és elszámolási vita is állt a háttérben.

A feltételezett támadó – akinek előzetes letartóztatását a bíróság elrendelte – megalapozottan gyanúsítható a büntető törvénykönyvről szóló 2012. évi C. törvény 160. § (1) bekezdésébe ütköző, és a (2) bekezdés f) pontja szerit minősülő – figyelemmel a Btk. 10. § (1) bekezdésére –, több ember sérelmére elkövetett emberölés bűntett kísérlete, valamint a Btk. 325. § (1) bekezdés c) pontjába ütköző, és aszerint minősülő, engedély nélkül az ország területére behozatallal elkövetett lőfegyverrel visszaélés bűntettének az elkövetésével.

Konklúzió

A csengelei ügy esettanulmánya jól példázza, hogy a nyomozó hatóságok által hozzáférhető nyilvántartások, adatbázisok, a modern kor technikai vívmányai által rögzített információk és a digitális nyomok aprólékos elemzésének és értékelésének kiemelkedő jelentősége van a bűncselekmények felderítése során.

A társszervekkel (megyei rendőr-főkapitányságok, Nemzetközi Bűnügyi Együttműködési Központ, Készenléti Rendőrség Nemzeti Nyomozó Iroda), az ügyészséggel, valamint a német és osztrák társhatóságokkal történő hatékony együttműködés eredményeként egy kiemelt tárgyi súlyú, élet elleni bűncselekmény elkövetése után, negyven órán belül sikerült megállapítani a tettes személyazonosságát és tartózkodási helyét, majd őt elfogni.

DOI: 10.38146/BSZ.2018.7-8.12

BOGDÁNY GYULA

Bűncselekmény-sorozatok megszakítása, bűnözői csoportok bomlasztása

Az ember hétköznapi tevékenységének lenyomatát hordozó digitális adatnak a kriminalisztika fejlődési útján méltán tulajdonított mérföldkő jelentőséget nagy ívű elméleti összefoglaló művében *Fenyvesi Csaba.*[1] A digitális adatok – amelyek megjelenési formáinak és felhasználási területeinek bővülése töretlen – felkutatása, rögzítése, biztosítása, rendszerezése és az igazságszolgáltatás számára történő előkészítése a bűnügyi nyomozást hivatásul választó szakemberek informatikai készségének folyamatos fejlesztését igényli. Ugyanakkor, ha az eredményes nyomozó mintaképét vázoljuk, nem rugaszkodhatunk el a személyi bizonyítékforrások (vallomások, adatközlések) kiaknázásának mesterfogásaitól sem. Hiszen mit ér egy kamerafelvételnek, egy telefon cellaadatának, esetleg egy gyanús tartalmú szöveges üzenetnek a tagadást vagy hárítást tanúsító személy elé tárása, ha az igaz vallomás elérése érdekében előzőleg nem épült fel a kihallgatás terve, azaz a lehetséges válaszokra felkészülés és az ezekből megfelelően következő kérdések azonnali feltétele. Még a terhelti vallomás hiányában is (kényszerű vagy taktikus belenyugvás a vallomás megtagadásába, halasztásába) szükséges a kihallgatónak felismernie a digitális adatok alkotta bizonyítékok elégséges mértékét.

A digitális adatok értő (informatikai jártasság) és hatékony (kriminalisztikai jártasság) felhasználásával a detektív olyan kanyarokat vághat le a nyomozás menetében, amelyekkel lényegesen csökkentheti a bűn üldözésében a rajtnál, vagyis a tudomásra jutásnál keletkezett hátrányát.

A nyomozó csoport működésében, ahol nyomozást nem egyéni teljesítménynek, hanem a nyomozó szerv meghatározott szervezeti eleme által folytatott kollektív szakmai erőfeszítésnek tekintjük, az egység munkáját irányító vezető feladata, hogy a sikeres működés érdekében a csoport tagjai közül kire-kire a legmegfelelőbb feladatot bízza.

Nyomozó csoportot kell alakítani – egyebek közt – a sorozatban elkövetett bűncselekmények vagy a forró nyomon üldözést igénylő, különösen az

1 Fenyvesi Csaba: A kriminalisztika tendenciái. A bűnügyi nyomozás múltja, jelene, jövője. Dialóg Campus Kiadó, Budapest, 2017, 69. o.

élet elleni bűncselekmények felderítéséhez. Előbbieknél a sorozatjelleg felismerése, utóbbiaknál a felfedezés késői vagy késleltetett ideje jelent hátrányt az üldözésben.

Ezeknél a bűncselekménytípusoknál elengedhetetlen a digitális adatok időszerű felkutatása és összegyűjtése, hiszen a behatárolt, akár néhány napra rövidült megőrzési idő miatt – hasonlóan a raszterekben tárolt adatok nagy részéhez – az adatok törlődnek, a felderítés esélye lényegesen csökken. Még ha nem is látható előre a sorozatjelleg kialakulása vagy nem merült is fel az élet elleni bűncselekmény gyanúja, bizonyos vagyon elleni bűncselekmények esetén (például lakásbetörés, gépjárműlopás, trükkös lopás) vagy rendkívüli halál miatti közigazgatási hatósági eljárásban, illetve eltűnés miatti körözési eljárásban – a relevancia mérlegelését megelőzve – célszerű intézkedni a számításba vehető digitális adatok megismerésére, beszerzésére.

Számolni kell ugyanakkor a beszerzési idő esetleges kitolódásával is. Nem elegendő a megkeresés sablonos kiküldése, hiszen a kézbesítéssel, ügyintézéssel, hiánypótlással vagy újabb adatkezelő megkeresésével járó időveszteség az adatok menet közbeni törlésének veszélyével jár, és ez már nyomozástaktikai hiba. Esetenként célravezetőbb a megkeresés küldése előtt vagy közvetlenül utána az adatkezelővel történő egyeztetés a kért adatok köréről, meglétéről, minőségéről, a teljesítés módjáról, sürgősségéről.

A digitális adatok megjelenési formáinak szaporodásával arányosan szélesedik a bűnüldözési célú felhasználás technikai-informatikai választéka, hiszen például a távközlési szolgáltatók, az útdíjfizetési szolgáltató, a közúti intelligens kamerahálózat adatbázisához történő közvetlen nyomozó hatósági hozzáférés, a Nemzeti Szakértői és Kutatóközpont által személyazonosság ellenőrzése vagy ismeretlen személy azonosítása érdekében végzett arcképelemzési tevékenység mind a bűnügyi munka hatékonyságának növelését szolgálják.

A nyomozásokban jelenleg leggyakrabban használt két digitálisadat-típus, a mobiltelefonnal (az azon tárolt, továbbított és a készülék detektálásával) kapcsolatos információk, valamint a közterületen és nyilvános helyeken működő térfigyelő kamerák felvételei.

A következőkben a Bács-Kiskun Megyei Rendőr-főkapitányság joggyakorlatából vett néhány példán mutatom be a digitális adatok nyújtotta felderítési lehetőségeknek a nyomozásokban történő sikeres alkalmazását.

Trófeatolvajok Érsekhalmán

Országos előfordulással, de főként a középső és a nyugati országrészben, évek óta, váltakozó gyakoriséggal fordultak elő külterületen, vadászházaknál elkövetett betöréses lopások, amelyek fő tárgyai gímtrófeák voltak. Az alkalmazott módszerben, az eszközökben és segédeszközökben, a társas elkövetésben, az elkövetőknek a helyszínen tanúsított magatartásában mutatkozó hasonlóságok alapján az esetek többségében azonos elkövetői körrel lehetett számolni. Bács-Kiskun megyét is érintették a betörések, és több szerv folytatott önálló nyomozást. Ezek közül a Kiskőrösi Rendőrkapitányság jutott a bűnözői csoport behatárolásában legtovább, de az egy évnél hosszabb előkészítés ellenére nem sikerült a megalapozott gyanú közléséhez elegendő bizonyítékot beszerezni valamely nevesíthető személlyel szemben.

A megcélzott kör egy Kunszentmiklóson élő, családi, szomszédi, ismerősi viszonyban álló személyek bűnkapcsolatokkal átszőtt amorf csoportja volt, amelynek tagjai folyamatosan bűnözésből tartották/tartják el magukat és családjaikat. A csoport működésének sajátossága, hogy a kibocsátási helytől távol, gyakran külföldön, utazó bűnözőkként tevékenykedtek, különböző vagyon elleni bűncselekmények folyamatos végrehajtásával, tippadókkal, orgazdákkal, segítőkkel. Az általuk használt járműveket, telefonokat, lábbeliket heti gyakoriséggal váltották vagy cserélték egymás között.

2017. január 30-ra virradóra, a Bajához közeli Érsekhalma külterületén, két egymáshoz közeli vadászházba lakatlefeszítéssel hatoltak be ismeretlen tettesek, és onnan több mint egy tucat gímtrófeát, valamint elektromos kéziszerszámokat, vadászöltözéket tulajdonítottak el, nagyjából huszonnégymillió forint értékben. A tárgyakat az ott talált kézikocsin távolabb vontatták, az agancsokat lefűrészelték, a koponyákat hátrahagyták. A két helyszín szemléjén hasonló lábnyomokat rögzítettek a hóban.

A vagyon elleni bűncselekmények nyomozásai felett szakirányítást gyakorló megyei bűnügyi osztály elérkezettnek látta az alkalmat az elkövetők elleni eredményes fellépéshez, ezért január 31-re koordinációs értekezletre rendelte be a legutóbbi eseménnyel érintett Bajai Rendőrkapitányság, a korábbi ügyek alapján legtöbb ismeretre szert tevő Kiskőrösi Rendőrkapitányság és a vélt elkövetők lakhelye szerinti Kunszentmiklósi Rendőrkapitányság bűnügyi vezetőit és előadóit.

Az értekezleten a bajai nyomozók ismertették az érsekhalmi trófealopás kriminalisztikai jellemzőit, a szemle főbb megállapításait, az elkövetők felderítése érdekében tett intézkedéseket, az azonosításukat lehetővé tevő bizo-

nyítékokat. A Kiskőrösi Rendőrkapitányság képviselői tájékoztatást adtak az általuk folytatott nyomozás főbb eredményeiről, a lehetséges elkövetőkre mutató adatok forrásáról, az adatok rendszerezéséről, az azokból levont következtetésekről, az azonosítást lehetővé tevő bizonyítékokról, illetve a bizonyítás nehézségeiről. A kunszentmiklósi nyomozók bemutatták a célcsoport jellemzőit, összetételét, a tagokkal kapcsolatos aktuális információkat, az általuk használt gépjárművek listáját.

A megyei bűnügyi osztály a csoporttagokhoz rendelt telefonszámok hívásforgalmi adatainak elsődleges ellenőrzéséről adott rövid tájékoztatást.

A résztvevők megállapították, hogy bár egyelőre az elkövetés óta eltelt idő rövidsége és – valószínűleg – a csoport begyakorolt kivédési technikái miatt nem álltak rendelkezésre friss bűncselekményre, így az érsekhalmi trófealopás ügyére vonatkozó terhelő adatok, azonban a megismert működési jellemzők alapján igen valószínű, hogy utóbbi cselekményt is e csoport tagjai követték el.

A gyanú tisztázásához célszerű volt a minél hamarabb történő személyes ellenőrzéseket végrehajtani, mivel az eltulajdonított tárgyak – mint ahogy a hozzájuk köthető más esetekben is – minden bizonnyal megindultak az értékesítési láncban, a használt segédeszközöket (gépjárművek, telefonok, lábbelik, feszítőeszközök) szokás szerint gyorsan váltják, megsemmisítik. A gyanút megalapozó adatok beszerzésére fordított idő a felderítés ismert nehézségeihez vezetett volna.

A résztvevők egy koncentrált akció végrehajtását határozták el másnapra, aminek célja az ismert elkövetői körből, annak szűkítését követően, az előéletük alapján bizonyosan bűnözői életvitelt folytató és vélhetően jelen bűncselekménnyel kapcsolatba kerülő személyek alapos ellenőrzése, velük szemben a bűncselekmény gyanújának megállapítása vagy kizárása házkutatások, előállítások, elszámoltatások, kihallgatások, DNS-minta-vételek révén.

A megyei bűnügyi osztály által kidolgozott terv alapján a kutatás tárgya huszonnyolc bűnügyi nyomozóval és technikussal, tizenegy helyszínen, kilenc célszeméllyel szemben, azonos időben végrehajtott, gépjárművekre is kiterjesztett házkutatásokon elsősorban a trófealopásokból származó, illetve azokhoz eszközként, segédeszközként használt tárgyak, a helyszíni lábbelinyomok nyomképzői, mobiltelefonok személyhez rendelését lehetővé tevő valamennyi azonosító szám, utazással kapcsolatos bizonylatok (úthasználati és tankolási blokkok, bírságértesítők stb.) lefoglalása, de legalább jegyzőkönyvi rögzítése volt.

Az érintetteknek a bűncselekmény idejére vonatkozó elszámoltatása tanúkihallgatásokkal történt. A teljes munkanapot kitevő akció során bűncselekmény gyanúja senkivel szemben nem alapozódott meg, de a házkutatásokon számos, telefonokkal kapcsolatos azonosítószám, néhány, a helyszíni nyomokhoz hasonló mintázatú lábbeli, vadászöltözék és egyéb tárgy rögzítésére került sor. Azoktól, akik nem szerepeltek a DNS-profil-nyilvántartásban, összehasonlításra mintát vettünk.

A lefoglalt tárgyak közül kiemelkedő jelentőségűnek bizonyult az egyik kisteherautóban talált autópályadíj-vásárlási bizonylat, amelyet az érsekhalmi betörés hajnalán egy az M8-as autópályához közeli település üzemanyagtöltő állomásán váltottak, az illető jármű forgalmi rendszámára. Ennek alapján nyomban intézkedtünk a benzinkút kamerafelvételeinek beszerzésére, ezeken látható volt, hogy a vásárlást a jármű tulajdonosa, a csoport vezetőjeként ismert *K. Imre* és a gépkocsit vezető másik férfi intézte. Utóbbit az akcióban részt vevő kunszentmiklósi nyomozók azonnal azonosították, *Sz. János* személyében. Nevezett apjának lakásán, az előző órákban tartott házkutatáson, az ágyneműtartóba rejtve, a nyomozók az érsekhalmi betörés helyszínén rögzített elkövetői lábnyom mintázatához hasonló, sáros cipőt találtak.

A későbbiekben a kisteherautó forgalmi rendszámát ellenőriztük a Nemzeti Útdíjfizetési Szolgáltató (NÚSZ) Zrt. adatbázisában, és megállapítottuk, hogy a jármű a betörés éjjelén Kunszentmiklós felől, Érsekhalma irányába, majd onnan Dunaújvároson át Székesfehérvár felé közlekedett. Érsekhalma közelében, a térfigyelő kamerák gyengébb minőségű felvételein szintén feltűnt egy típusában azonos, színárnyalatban hasonló jármű az érkezési és a menekülési időszakokban.

A betörés helyszínén leképeződött lábnyomok alapján négyfősre becsült elkövetői csoportból így két személy kilétét sikerült vélelmezni. A hívásforgalmi adatok elemzésére időközben bevontuk a nyomozásba a megyei elemző-értékelő osztályt, amely értékelőjelentésben mutatta ki, hogy a K. Imréhez rendelt telefonszám a betörés éjjelén pontosan követte az Sz. János által vezetett gépkocsi menetvonalát.

Eme összefüggések ismeretében két héttel később ismét kihallgattuk tanúként K. Imrét. Tagadta, hogy a teherautóját a kérdéses éjjelen bárki is használta volna. Ezzel párhuzamosan, a szintén tagadóan nyilatkozó Sz. János a vallomása ellenőrzésére alkalmazott poligráfos vizsgálaton a kritikus kérdésekben megtévesztő válaszokat adott.

A nyomozás kimenetele szempontjából ez a pillanat volt a fordulópont. A vázolt összefüggéseket a bajai nyomozók ismertették a nyomozást felügyelő

ügyésszel, aki egyetértett a nyomozó hatóság álláspontjával: a két férfival szemben megalapozott az érsekhalmi trófealopás gyanúja.

A bűncselekmény elkövetését a későbbiekben is tagadó K. Imrét és Sz. Jánost gyanúsítottként hallgattuk ki, majd őrizetbe vettük, és előzetes letartóztatásba kerültek.

Az érsekhalmi betörés további két elkövetőjét mintegy négy hónappal később sikerült azonosítani.

Az egyébként analfabéta *Sz. István* a helyszínen használt kézikocsiról vett törletből kimutatott DNS-profil és a februári akcióban tőle rögzített DNS-mintával azonosság révén, *Cs. László* pedig azzal került gyanúba, hogy a nála tartott házkutatás során felírt hívószámú és az ellenőrzések eredményeként a személyéhez rendelt telefonkészülék a betörés helyén és idején üzemelt.

Utóbbi két személy ellen is megalapozottá vált a betöréses lopás gyanúja, ezért együttesen vontuk őket eljárás alá, majd előzetes letartóztatásba kerültek.

Már a nyomozás kezdeti szakaszában sejthető volt, hogy a gyanúsítottak sorozatjelleggel, sokat utazva, heti gyakorisággal követték el a vadászházak elleni támadásokat, és a zsákmányolt trófeákat, szerszámgépeket azonnal egy Székesfehérvár közelében élő személyhez, feltehetően orgazdához szállítják. Két évre visszamenően, közel kéttucatnyi, hasonló ismérvekkel bíró betöréses lopás ügyében tekintettük át a bizonyítás lehetőségeit. A behatárolt elkövetői körhöz tartozó – döntően a februári akció során megismert – telefonkészülék-azonosítók alapján részletes összehasonlító értékelést végeztünk a megyei elemző-értékelő osztály bevonásával. Ezzel párhuzamosan folyt az egyes helyszíneken rögzített DNS-maradványok genetikai szakértői vizsgálata.

Az ügykutatás során az érsekhalmi betörést megelőző két hétben, Pest és Somogy megyében elkövetett, négy másik trófealopást sikerült az elkövetők személyéhez rendelni, és az ügyeket egyesíteni. A Sz. Istvánra és Cs. Lászlóra vonatkozó további DNS-azonosítások és Sz. István későbbi, önmagára és társaira nézve is terhelő vallomása mellett a nyomozás jelentős eredményeként könyvelhettük el az egyébként legális agancsfelvásárlással foglalkozó és ekként feltehetően a tippeket adó *H. János* orgazda eljárás alá vonását.

Intézkedésünk nyomán a vadászházaknál elkövetett sorozatos trófealopások országos szinten megszűntek, ezért szinte bizonyos, hogy a jelenség döntően a felderített bűnözői csoport számlájára volt írható. Mindamellett fájó, de józan tapasztalat, hogy a megtett erőfeszítések ellenére sem sikerült időben távolabbi, hasonló tárgyú ügyeket összevonni. Ennek fő oka részben a konok, de érthető elkövetői hozzáállás és az idesorolható leplezési technikák

(eszközök, társak cserélődése), részben a nyomszegény helyszínek, részben pedig a távközlési adatok korlátozott idejű (egy év) hozzáférése volt.

Úgy tűnik, hogy a bemutatott ügyben a felderítés sikerének kulcsa a digitális adatok összegyűjtése és rendszerezése volt. Valóban fontos adatokat szolgáltattak a kereskedelmi helyről beszerzett kamerafelvételek, az útdíjszolgáltató rendszámleolvasó informatikai rendszerei, a távközlési szolgáltatók térségi cellainformációi és egyes készülékekre vonatozó hívásforgalmi adatai. Az adatok bizonyítékká csiszolásához azonban előzőleg szükségeltetett a bűnözői csoporttal kapcsolatba került rendőri szervek aktuális információinak gyors kicserélése, az elkövetőkként számításba vehető személyekkel szemben a mielőbbi és megalapozott kényszerintézkedések végrehajtása, hiszen a házkutatásokon kerültek a nyomozó hatóság birtokába és tudomására olyan tárgyak és egyedi azonosítók, amelyekből a keletkezésükre, működésükre vonatkozó digitális adatokat lehetett felkutatni. A beszerzett digitális adatokat rendeztük és egyeztettük egymással, valamint a célszemélyek tanúként tett vallomásaival. Mivel a vallomások a felelősségre vonás alóli kibúvás szándékával nyilvánvaló valótlanságokat tartalmaztak, kirajzolódtak az elkövetők bűnös tevékenységének körvonalai. Ezeket minősítette előbb a nyomozó hatóság megalapozott gyanúnak, később, immár a tényállás képét alkotó megerősödésük után, az ügyész vádnak.

Afrikai kereskedők kirablása Zsanán

Sajátos sértetti kört megcélozva tervezett rablásokat elkövetni az a rokoni kapcsolatokon szerveződött csoport, amely az előző jogesetben bemutatottnál sokkal nagyobb előrelátással szervezte meg a befejezett stádiumba jutott bűncselekményét.

Az ötfős társaság értelmi vezetője a Pest megyei Táborfalván élő, vásári mutatványos család 31 éves tagja, *O. Zsolt,* aki a nyári üzemszezonon kívül használt teherautók adásvételével igyekezett jövedelemre szert tenni. A hazai forgalomból kiszorult, rossz műszaki állapotú kisteherautóknak a fejlődő országokba irányuló exportjával Budapesten számos színes bőrű kereskedő foglalkozik. E körben épített ki O. Zsolt üzleti kapcsolatokat, azonban 2016 elejétől váratlanul rablások célszemélyeiként tekintett partnereire. Tervéhez a körhinták és dodzsemek kezelésében kisegítő családtagként dolgozó húszéves öccsén, *O. Erik*en és huszonöt éves unokaöccsén, *Ny. János*on kívül beszervezte a Bács-Kiskun megyei Hajóson élő rokonai közül negyvenöt éves

nagybátyját, *Ny. Csabá*t, aki bevonta a Németországban dolgozó, többszörösen büntetett előéletű vőjelöltjét, a huszonegy éves, *K. István Dávid*ot.

Elképzelésük szerint az üzletfeleket teherautó-eladás ürügyével vidéki helyre csalják, ahol útonállásszerű támadással a vásárláshoz vitt pénzüket elrabolják. A megtévesztéshez alkottak egy fantomfigurát, aki O. Zsoltra hivatkozva átveszi az eladó szerepét, és telefonon a lesben álló rablókhoz irányítja a vevőt. A fantom szerepét a sértettek által nem ismert Ny. Csaba vállalta magára.

2016. március 4-én, az esti órákban elsőre kissé különös, majdhogynem komikus tartalmú bejelentést tett telefonon a rendőrségre egy a Bács-Kiskun megyei Zsana község egyik erdei útján faaprítékot szállító helyi lakos, miszerint két, megkötözött kezű afrikai férfi kért tőle segítséget, mondván, előzőleg öt támadó kirabolta őket.

A nigériai–magyar kettős állampolgárságú kereskedő és barátja a nyomozóknak elmondta, hogy teherautók eladásának ígéretével Budapestről csalták őket az erdőbe, és elrabolták tőlük a vásárlásra magukkal vitt pénzt. A gyéren lakott területen lévő megbeszélt helyen egy autóssal találkoztak, akit követniük kellett az erdőbe. Amikor a felvezető jármű megállt, abból és a fák közül csuklyás, fegyveres férfiak ugrottak elő, az egyikük fejéhez pisztolyt nyomtak, a másikuk torkához bozótvágó kést szorítottak. Elvették pénzüket, telefonjukat, tabletjüket, majd összekötözték a kezüket, és elmenekültek.

A vevő O. Zsoltot jelölte meg, mint aki révén kapcsolatba lépett azzal az ismeretlennel, aki a szervezés és az út során telefonhívásokkal, egy joviális öregúr profilképével álcázottan internetes alkalmazásban, az útvonalról és az ígért teherautók képéről küldött üzenetekkel tartotta fenn benne a bizalmat.

A megyei rendőr-főkapitányság által felügyelt, később hatáskörbe vont nyomozás során hamar kiderült, hogy a felvezető gépkocsi forgalmi rendszáma egy győri telephelyen parkoló teherautóhoz tartozott.

Mivel a vevő O. Zsoltra hivatkozott, haladéktalanul ki kellett volna őt kérdeznünk. Nevezett azonban másnap estig nem volt elérhető. Családtagjai kitérő válaszokat adtak a hollétéről. Végül, az ellene kiadott elfogatóparancs hatására önként megjelent a rendőrségen, és azt állította, hogy ő csupán közvetített nigériai ismerőse és az általa csak telefonon ismert eladó között. A vevőtől előleget vett át, amit azonban nem továbbított. Már ekkor ellentmondásba keveredett, hiszen a félrevezető sms-ek az előlegnek az eladóhoz érkezésére utaltak. A továbbiakban részletesen beszámolt az előző napjának eseményeiről, gondosan beleszőve a lakásától mintegy száz kilométer távolságban lévő kiskunsági helyszínre vezető útjának célját, miszerint egy

Zsanához közeli faluban, előzetes megbeszélés alapján, vételi céllal, teherautó-alkatrészt szándékozott megtekinteni. Az úti cél előtt a gépkocsijából kifogyott az üzemanyag. Emiatt felhívott egy Hajóson élő rokont, és megkérte, hogy nagybátyját, a később azonosított másik elkövetőt, Ny. Csabát küldje érte segítségül. Ny. Csaba így már indokkal jelent meg a lakásától több mint ötven kilométer távolságban lévő helyszín közelében a felhívott rokon gépkocsijával.

A kihallgatott Ny. Csaba arra a kérdésre, hogy miért nem a saját Opel Vectrájával sietett O. Zsolt segítségére, úgy nyilatkozott, hogy azért, mert azt fia használta, a Budapestre, repülővel érkező vőjelöltje, K. István Dávid Hajósra szállításához. A Vectrának azért volt jelentősége, mert, mint később bebizonyosodott, a sértetteket fogadó, Ny. Csabáéval típusazonos felvezető autó sértettek által látott rendszáma valójában a Vectráéból lett átalakítva.

Az első napok tanúkihallgatásai során feltérképeztük az elkövetőként számításba vehető személyeket, a vallomásokban megnevezett rokonokat és kívülállókat. A vallomásokból igen kusza kép alakult, tele ellentmondással, amelyekre nem lehetett magyarázat az egy-két napos időmúlás okozta emlékezethalványulás.

Az O. Zsolt és Ny. Csaba lakásán a nyomozás kezdetén végrehajtott házkutatások ebben az esetben is döntő bizonyítékokat szolgáltattak a palástolni igyekezett eseményre. Mindamellett, hogy rögzítették a kiterjedt család tagjainak telefonszámait, amelyeket egyébként szinte követhetetlen módon adtak egymásnak használatra, Ny. Csaba lakásán, a szemétben lefoglaltak egy a kiskunhalasi Tesco áruházban, a rablás utáni órában kiállított vásárlási bizonylatot. Ugyancsak lefoglalták az erősen szennyezett Opel Vectra feltűnően tiszta rendszámtábláit, amelyről később a vegyész szakértő ragasztóanyag maradványát mutatta ki.

A Tesco-nyugta alapján haladéktalanul beszerzett áruházi kamerafelvételeken együtt volt látható O. Erik, Ny. János és K. István Dávid, amint vidáman vásároltak élelmiszert, szeszes italt.

A nyomozás kezdete után két héttel, a házkutatásokon, a tanúvallomásokban és telefonkészülék-szemléken rögzített telefonszámok elemzése eredményeként a kihallgatott személyek megjelölt útvonalain felkutatott, lefoglalt és elemzett kamerafelvételek (kiskunhalasi benzinkutak, hajósi, zsanai önkormányzati térfigyelő rendszerek) alapján megalapozódott a nigériai sértettek kirablásának gyanúja O. Zsolttal és négy rokonával szemben.

A bizonyító erejű digitális adatok közül a Tesco áruház képfelvételei mellett (amelyen az ötből három elkövető együtt látható a rablás után!) kiemel-

kedett a sértettek helyszínre csalásához ismeretlen személy által használt telefonszám azonosítása. A kérdéses telefonszámot ugyanis nemcsak a rablás előkészítésére használták, hanem olyan „civil” számokkal való forgalmazásra is, amelyekből visszafejtett kapcsolati ábra középpontjában O. Zsolt állt. Ezek részben hozzátartozói hívószámok voltak, de számos, az O. Zsolt által más, az ügyben érdektelen, főként a tehergépkocsi-adásvételek kapcsán köthető személyekhez tartoztak.

Utóbbi körbe tartozott egy másik nigériai kereskedő, akit 2016. február 18-án, az ismertetett módszerrel és az ismert fantomszámmal kívántak Budapestről Hajós környékére csalni. Az őt és kísérő honfitársát szállító autót O. Erik vezette, aki menet közben O. Zsolttól kapott utasításokat. A két afrikai bizalmatlanná vált, és végül elálltak az egyre gyanúsabbá váló vidéki üzletkötéstől. O. Eriket határozott fellépéssel rábírták a fővárosba visszafordulásra. Jellemző, hogy ekkor a fantomszám készüléke Táborfalva térségében üzemelt.

Ugyancsak potenciális sértett lehetett az, a tanúként kihallgatott szudáni férfi, akit a fantomszám használója a zsanai rablás utáni napra teherautó-vásárlás végett Szarvasra kívánt csalni. Az „eladó” nyomatékosította, hogy a szudáni mindenképpen vigyen magával hatmillió forintot. A külföldi március 5. (az intenzív nyomozási cselekményeink ideje) után nem érte el a kérdéses telefonszámon partnerét.

Még az egyik legismertebb internetes apróhirdetési oldal üzemeltetőjének válasza is megerősítette, hogy a kérdéses számot tartalmazó hirdetésfeladások az O. Zsolthoz köthető számítógép hálózati azonosítószámáról érkeztek.

2016. március 17-én, egy időben, három településen, összehangolt intézkedés keretében elfogtuk O. Zsoltot és négy társát, a létszámban is a sértetti vallomásokkal egyező számú gyanúsítottakat. A „tescós csoport” vallomásai a következő lényeges elemeket tartalmazták.

O. Erik előbb tagadta, hogy a bűncselekmény napján járt volna Kiskunhalason, és saját magát nem, de társait felismerte a képfelvételeken. Későbbi vallomásai minden tekintetben zavarossá váltak, végül megtagadta a vallomástételt. A sértetteket egyébként ismerte, mert dolgozott náluk autóbontáson.

Ny. János első nyilatkozata szerint a tárgybeli napon valóban elutazott Táborfalváról Kiskunhalasra O. Erikkel, de nem O. Zsolt gépkocsiján, hanem autóbusszal. A Tescóban valóban találkozott K. István Dáviddal, aki oda találkozót beszélt meg O. Erikkel.

Vallomásaiban a legkövetkezetesebb a rutinos bűnöző, a Németországból a cselekmény napján hazaérkező K. István Dávid volt, aki tagadta, hogy a

kérdéses időpontban elhagyta volna apósa hajósi lakását. Az áruházi felvételeken felismerte magát és társait, de vitatta a felvétel idejét.

O. Zsolt főbb vonalakban fenntartotta a tanúként elmondottakat, azzal a lényegi eltéréssel, hogy az alkatrésznéző útjára magával vitte O. Eriket és Ny. Jánost, akik még az üzemanyag kifogyása előtt, Zsana térségében, ismeretlen okból kiszálltak a gépkocsijából.

Ny. Csaba gyanúsított vallomásaiban nem tért el a tanúként tett nyilatkozatától, áldozati szerepbe helyezte magát, aki csak azért került eljárás alá, hogy az elkövetői létszám összeálljon.

A későbbi vallomások közül kiemelkedik Ny. Jánosé, aki magára vállalta a nigériai sértettek kirablásának általa vezetett végrehajtását, négy, meg nem nevezett társával. E vallomásának előzménye O. Zsolt többszöri, írásos rábírása volt, mely küldemények egy részét a büntetés-végrehajtási intézetben elfogták, ugyanakkor O. Zsolt elismerte a levelek „nem komoly szándékkal” történő megírását. A rábírásban O. Zsolt a legjobb ügyvédeket, rövid fogva tartási időt és a mutatványos eszközparkból a „sárkányos légvárat” ígérte elesett sorsú unokaöccsének.

Itt említendő meg, hogy a nyomozás során számos, egymással kapcsolatban nem álló zárkatársat hallgattunk ki a gyanúsítottak környezetéből. A védelem által elfogultnak és súlytalan tartalmúnak minősített tanúvallomások azonban mindannyiszor tartalmazták azt, a bűncselekmény helyére, módszerére, kivitelezésére, résztvevőire vonatkozó valóságmagot, amelyről csak az azonos cselekményben részt vevő tettesek számolhattak be.

A gyanúsítottak alibijének ellenőrzése és a cselekménnyel összefüggő téridő vetület tisztázása érdekében tanúként kihallgatni szándékozott, összesen kilenc hozzátartozó (többségükben nő), élve jogával, megtagadta a vallomástételt. A nyilvánvalóan összehangolt döntésükkel rábízták a nyomozó hatóságra, hogy a hiányos bizonyítékláncolatot megalapozott következtetésekkel egészítse ki.

Az elkövetők alapvetően primitív, de valamilyen mértékben átgondolt módszert alkalmaztak a mit sem sejtő külföldiek kirablására, hiszen a lakóhelyeiktől távoli megjelenésüket igyekeztek legalizálni, számoltak a térfigyelő kamerák bizonyító felvételeivel, ennek érdekében megtévesztő mozgásokat tettek, a csaliautó használatát titkolták, forgalmi rendszámát megmásították, mindamellett nem számoltak az áruházi kamerák felvételeivel, amelyek alapján teljessé vált az elkövetők száma, és világossá a mozgásuk, tevékenységük. Ugyancsak végzetes volt számukra a vezetőjük óvatlansága, amellyel nem tudta magát el-

határolni a sértettek megtévesztéséhez a helyébe léptetett fantomszemélytől, és a kérdéses telefonszámot köznapi kapcsolattartásra is használta.

Az afrikai sértettek elleni fegyveres rablás ügyében figyelemre méltó körülmény volt, hogy az addig üzleti jellegű – és mint ilyen, bizalmi – viszonyt O. Zsolt váratlanul bűnös szándékkal igyekezett kihasználni. A korábban szintén nigériai és a később szudáni üzletfelek irányába tett rablási előkészületek egy sorozat részeiként tekinthetők, amely sorozat kibontakozását a befejezett rablás ügyében gyorsan megtett hatósági fellépés szakította meg.

A nyomozások tapasztalatai

Az ismertetett két csoport összetartó erejét képező közös bűnelkövetői szerepvállalást részben a terheltek szabadságelvonásával, részben néhány csoporttag későbbi, kényszerű – igaz, részleges – beismerése révén sikerült megbontani. Illúzió lenne azt gondolni, hogy ezek a szokványos bűnözők a büntetőeljárások várható joghatásaitól tartva – különösen a kunszentmiklósi csoport – valamennyien elállnának a jövőbeli bűnös tevékenységüktől. Az azonban alappal feltételezhető, hogy néhány tagjuk, különösen a családosok, vagy az idősebbek, a várhatóan kiszabott és nagy valószínűséggel végrehajtandó szabadságvesztésük letöltése után nem vállalnak aktív, tettesi szerepet hasonló bűncselekményekben. A jövőbeni működését illetően a csoport átrendeződése is hordozhat ismeretlen veszélyforrásokat (a tagok stressztűrő képessége, informátorok kapcsolódása stb.).

A bemutatott esetek felderítési tapasztalatait összegezve leszögezhetjük, hogy hazánk digitális lefedettsége jelentős előnyt kínál a bűncselekményeket utazó jelleggel, sorozatban elkövetők vagy az elkövetéshez jelentős helyváltoztatást igénylő tettesek azonosításához. Amíg a vélt elkövetők nem kerülnek látómezőbe, addig a digitális adatok beszerzésére a relevancia vizsgálata nélkül szükséges intézkedni, hiszen az adatokra vonatkozó megőrzési idő a későbbi hozzáférést nem teszi lehetővé. Ha pedig körvonalazódott az elkövető(k) személye, célszerű haladéktalanul felfedni valós céljainkat, a gyanú érzékeltetését, és akár korlátozó intézkedések révén begyűjteni a digitális adatok forrásait, hordozóit, tárgyait. Ezzel az „odacsapással”[2] nemcsak preventív célt érhetünk el, de mód nyílik a személyekhez köthető digitális

2 Uo. 152. o.

adatok elemzésére, értékelésére, rendszerezésére, egyben védekezési taktikájukban hibázásra kényszeríthetjük a társas elkövetőket.

Az egyes személyekre vonatkozó digitális (és más nyomozási) adatoknak az egymáshoz illeszthető csomagokba rendezése után tervszerű és határozott intézkedéseket kell tenni a behatárolt elkövetői kör ellen. Ez a fajta késleltetett végrehajtás, mint láttuk, nemcsak hogy nem veszélyeztette a felderítés sikerét, hanem éppen hogy egyfajta lüktető dinamizmust adott a nyomozásoknak mindamellett, hogy bizonytalanságban tartotta a célba vett csoportok tagjait. Megfelelő mennyiségű és minőségű adatok együttállása esetén a támadó fellépéssel nem szabad késlekedni, mert elvész a meglepetésre alapozott kedvező alkalom.

Végezetül szükséges kiemelni, hogy a bemutatott esetek tettesei alacsony iskolázottságú, esetenként óvatlan bűnelkövetők voltak, akik védekezési módszereikben a konok tagadáson, az azonosítható tárgyak váltogatásán, a megtévesztő helyváltoztatásokon túl alig voltak képesek eredményesen kitérni az azonosításuk elől. Az ellenük történő hatósági fellépés sikere az adatok összehangolásával, a gyors erőkoncentrációval és viszonylag rövid idejű adatelemzéssel volt elérhető. Ne feledkezzünk meg azonban arról a kvalifikált elkövetőről, aki a „digitális lábnyomát” sokkal nagyobb előrelátással igyekszik eltüntetni. A páncélszekrénynyitások, a lakásbetörések, a gépkocsilopások és kiemelt jelentőséggel a sorozatgyilkosságok (különösen a magánnyos) tetteseinek felderítésére kellő létszámú, felkészültségű és – kívánatosan – önállósított egységet kell működtetni.

A digitális tér csupán lehetőséget nyújt a nyomozó hatóság számára. A siker záloga a digitális adatoknak a kriminalisztikai látásmódon alapuló, a kiforrott nyomozási módszertannal („kriminalisztikai ajánlásokkal”) kombinált, ebből fakadóan értő és hatékony feldolgozása.

DOI: 10.38146/BSZ.2018.7-8.13

KÖNYVISMERTETÉS

Tóth J. Zoltán:
A büntetőjogi rágalmazás és becsületsértés

Médiatudományi Intézet, Budapest, 2017, 272 oldal

Jelen könyv a Médiatudományi Könyvtár 27. kötete. A szerző egyrészt azt tűzte ki célul, hogy áttekintést ad arról, milyen elméleti problémák vetődnek vagy vetődhetnek fel a szólásszabadságnak a méltóság, illetve a becsület védelme érdekében történő, kriminális jellegű korlátozásai során, másrészt hogy vázolja, vajon e problémákra milyen válaszok születtek és születnek az ilyen jellegű korlátozásokat alkalmazó, jellemzően európai országokban, ezen belül is elsősorban Magyarországon. Harmadikként végül azt a célt fogalmazta meg, hogy ismerteti és elemzi az Emberi Jogok Európai Bíróságának vonatkozó gyakorlatát.

Az előbbi propozitumoknak megfelelően a monográfia is három részre tagolódik, amelyeket – a módszertani differenciáltságot ezáltal is egyértelműben érvényre juttatva – az adott rész saját bevezetése nyit, végén pedig önálló összegzés zár, egymásra épülő – így akár önálló munkákként is helytálló – egységekként.

A munka felhasznált források széles körére támaszkodik. A primer források hangsúlyos szerepe a kötet szerkesztésekor is fontos szempont volt, ugyanis az – határozatmutatóként – a munka végén elhelyezkedő szakirodalomtól külön, az előszó előtt szerepel. A szerző nagy számban hivatkozza az Emberi Jogok Európai Bíróságának döntéseit, az Alkotmánybíróság, illetve a magyar bíróságok döntéseit, és több választottbírósági határozatot is. A releváns külföldi döntések esetén főként amerikai ügyekre és egyesült királyságbeli jogesetekre támaszkodik. A szakirodalmi apparátust tekintve kiemelendő, hogy a magyar nyelvű jog- és filozófiatudományi monográfia és szaktanulmányok széles köre mellett feldolgozta az alapvető angol nyelvű elérhető munkákat, kisebb részben pedig egyéb munkákat is. A szerző a korábban publikált eredményeit is sikeresen integrálta jelen munkába.

Az első rész a rágalmazás és a becsületsértés jogfilozófiai és a jogbölcseleti gondolkodásban formálódó megítélését mutatja be a történeti módszer segítségével. Az ókori görög szerzők közül *Platón*t emeli ki, a vonatkozó római gondolkodók eredményeinek bemutatása pedig *Cicero* és *Seneca* művein keresztül történik. *A középkori és kora újkori teológiai és szekuláris elméletek* című fejezet után *(Aquinói Szent Tamás, Erasmus, Machiavelli, Blaise Pas-*

cal, Spinoza) a felvilágosodás korának szólásszabadsággal és defamatorikus cselekményekkel kapcsolatos elméleteit *(Montesquieu, Beccaria)* veszi górcső alá a szerző. A deontológiai és utilitarista irányzatok ismertetésének részeként nagyobb terjedelemben foglalkozik a szerző *Kant* nézeteivel, azokat egész morálfilozófiáját meghatározó alapkategóriáin, a tisztaész-használaton, az akarat autonómiáján és a szabadság fogalmán keresztül mutatva be. A *Jeremy Bentham*mel foglalkozó elemzése végén a szerző megállapítja, hogy Bentham a becsület elleni vétkek három kategóriáját határozta meg, úgymint gyalázó szavak, testi méltatlanság és sértő fenyegetések. Ez után foglalkozik *Constant* és *Hegel* vonatkozó elméleteivel.

Az előzmények főbb csomópontjainak ismertetése után kerül sor *John Stuart Mill* nagy hatást gyakorló munkásságának bemutatására, elemzésére, értékelésére és utóéletének vázolására. Mill meghatározó elveit *A szabadságról* című munkájában fektette le. Mill alapelve az volt, hogy *„az önvédelem az egyetlen olyan cél, amelynek érdekében az emberiségnek […] joga van beavatkozni bármely tagja cselekvési szabadságába. Az egyetlen cél, amelynek érdekében jogosan lehet […] erőszakot alkalmazni: mások sérelmének a megakadályozása.”*[1] Mill három olyan esetkört határozott meg, amikor a vélemény elfojtása megengedhető: 1. ha a vélemény igaz, és az a vélemény, amely alapján az előbbit el kívánják fojtani, hamis; 2. ha mind az elfojtott, mind a többségi vélemény csak részben igaz; 3. ha az elfojtott vélemény hamis, és az a vélemény igaz, amelynek hívei az előbbi képviselőit korlátozzák nézeteik terjesztésében. A szerző ezt a milli elméletet egy negyedik elemmel is bővíti, amely szerint az is lehetséges, hogy egyik sem igaz vagy hamis, mert mindkettő csupán vélemény, igazságérték nélkül.[2]

A milli eszme angolszász jog- és politikaelméleti továbbélésének és továbbfejlesztésének eredményeit a szerző – többek között – *Oliver Wendell Holmes, Harold J. Laski, Louis B. Schwartz, Jeremy Waldron* munkásságán keresztül mutatja be. A jogfilozófiai és jogelméleti gondolkodás fejlődése legnagyobb eredményének azt tartja, hogy ma már csak a részletkérdések tekintetében folyik vita, az alapkérdést (a szólás kiemelt védelmének fontosságát) már senki nem kérdőjelezi meg.

A monográfia második része a rágalmazás és a becsületsértés európai és magyar jellegzetességeit tárja fel. Az elvégzendő feladatot tovább pontosítva

1 Tóth J. Zoltán: A büntetőjogi rágalmazás és becsületsértés. Médiatudományi Intézet, Budapest, 2017, 48. o.
2 Uo. 51. o.

rögzíti a szerző, hogy az anyagi büntetőjogi normák vizsgálatára kerül sor, ezen belül is csak az egyedi emberi személy méltóságát és/vagy becsületét sértő vagy arra alkalmas tényállításokkal és egyéb cselekményekkel, illetve azok megítélésével foglalkozik. Ez a rész két szerkezeti egységre bontható. Az első, két fejezetet felölelő egység az európai országok megoldásait összegzi (Németország, Ausztria, Svájc, Olaszország, Franciaország, a Benelux államok, Spanyolország, Portugália). Ez után tér ki önálló fejezet formájában egyéb uniós országok vonatkozó jogszabályi megoldásainak összegzésére.

E rész második nagy egysége foglalkozik a magyar joggal. A történeti áttekintést a középkorral kezdi, ismerteti *Szent István* dekrétumának vonatkozó részét[3], ugyanakkor a szokásjog jelentőségét – annak partikuláris jellegét kiemelve – elismeri, helyesen intve ezáltal az olvasót a jelen megoldásai módszertanilag kifogásolható visszavetítésének kétes eredményű voltára. Nagyobb terjedelemben elemzi a Csemegi-kódex vonatkozó rendelkezéseit, változásait, egészen az annak különös részét felváltó 1961. évi V. törvényig. Ezt követően röviden áttekinti a magyar történeti fejlődést az Alkotmánybíróság 36/1994. (VI. 24.) AB határozatáig.

A hatályos magyar jog elemzése során támaszkodik a joggyakorlatra, az OBH és a KSH vonatkozó statisztikai eredményeit pedig önálló tanulmánynak beillő lábjegyzetben adja közre. Külön fejezetet szentelt a rendszerváltozás utáni alkotmányos büntetőjog időszakának és a méltóság védelmének mint a véleménynyilvánítási szabadság korlátjának alaptörvényi megjelenésének.

A kötet harmadik része elemzi az Emberi Jogok Európai Bíróságának a büntetőjogi rágalmazással és becsületsértéssel összefüggő joggyakorlatát. A szerző a döntéshozatali rendszer vázolása után meghatároz négy, az EJEB szerint a véleménynyilvánítási szabadság terjedelme szempontjából releváns megkülönböztető tulajdonsággal jellemezhető személyi kört. Külön foglalkozik a politikusok ellen elkövethető cselekményekkel, az örökletes államfők sérelmére megvalósított cselekményekkel, a politikusnak nem minősülő közszolgákkal kapcsolatos esetekkel, valamint a bírókkal vagy az igazságszolgáltatás más szereplőivel kapcsolatos ügyekkel. A rész (és egyben a könyv) végén a szerző összegzi a strasbourgi esetjogban kikristályosodott, defamatorikus bűncselekményekkel kapcsolatos elveket.

---

3 Szent István Második Dekrétumának 53. fejezetét a király rágalmazóiról: „Ha ki valamely ispánnak vagy más keresztyén embernek álnokul ezt mondja: Hallám vesztedre szólni a királyt, és reá bizonyodik a dolog, haljon meg.”

KÖNYVISMERTETÉS

Tóth J. Zoltán munkája nemcsak a defamatorikus bűncselekmények történeti, jogelmélet-történeti megalapozását adja, hanem a komparatív, a dogmatikai és a jogesetelemző módszer jó arányérzékű vegyítése révén olyan komplex munkát alkotott meg, amely minden bizonnyal a téma megkerülhetetlen szakirodalmává fog válni.

Készítette: Nagy Péter