

8. Kiberbűncselekmények felderítése és nyomozása

Simon Béla – Gyaraki Réka

8.1. A kiberbűncselekmények illetékességi és hatásköri felosztása

A kiberbűncselekmények nyomozása szempontjából – az illetékesség megállapításának kérdésében – az ügyek ok nélküli és értelmetlen áttételei, ezzel a nyomozás hátráltatása miatt szükséges tisztázni, hogy hogyan lehet megállapítani a kibertérben elkövetett bűncselekmények esetében az elkövetés helyét. Az illetékesség alatt a földrajzi, területi meghatározást értjük. A rendőrség nyomozó hatóságainak hatásköréről és illetékességről szóló 25/2013. (VI. 24.) BM rendelet 3. §-a alapján a nyomozás lefolytatására az a nyomozó hatóság illetékes, amelynek illetékességi területén a bűncselekményt – sorozatos bűncselekmények esetén a bűncselekmények többségét – elkövették. Amennyiben az elkövetés helye nem állapítható meg, vagy pedig a cselekmény jellegéből adódóan több hatóság lenne jogosult lefolytatni az eljárást, akkor a megelőzés elve érvényesül, vagyis ott fogják az ügyet kivizsgálni, ahol korábban intézkedtek. Az illetékesség tekintetében beszélhetünk *általános* és *kiemelt* illetékességről. Általános illetékességű nyomozó hatóságok a rendőrkapitányságok (így a kerületi és városi), kiemelt illetékességűek a megyei rendőrfőkapitányságok, a Budapesti Rendőr-főkapitányság, valamint a Készenléti Rendőrség Nemzeti Nyomozó Iroda és a Reptéri Rendészeti Igazgatóság. A kiberbűncselekmények esetében is első gondolatra sokakban az a válasz fogalmazódik meg, hogy ott követik el a kiberbűncselekményeket, ahol maga az eszköz található. Ugyanakkor a válasz ennyire nem egyszerű ennél a deliktumnál, hiszen ma, amikor már az asztali számítógépek helyett laptopokat, tableteket és okostelefonokat használunk, amelyek mozgatása, helyválttatása egyszerű, akkor már ennyire nem evidens a válasz. Amennyiben valaki útközben (két település között vagy éppen két ország között utazva) követi el egy vállalkozás ellen a jogellenes tevékenységét, akkor annak megállapítása, hogy ki jogosult megindítani a nyomozást, már ennyire nem egyszerű. Létezik az illetékesség megállapítására is olyan nézőpont, miszerint az elkövetés helye ott van, ahol maga a kibertérben elkövetett jogellenes cselekmény ténylegesen megvalósul (így fordulhatott elő az a probléma, amikor az elektronikus cégbejegyzés megjelent, hogy a cégbíróság székhelye szerinti kerületi kapitányságnál a közokirat-hamisítások miatt indított eljárások száma megsokszorozódott, mert valamennyi olyan ügyben, ahol cégbejegyzéssel vagy cégváltással kapcsolatban történt feljelentés vagy jogellenes cselekmény, azokat a kerületi kapitányságra továbbították). A fentiek értelmezése alapján azt gondolom, hogy a kibertér esetében – bár az nem egy egységesen meghatározott terület, tér – is megállapítható, hogy melyik nyomozó szerv jogosult eljárni. A nyomozó hatóság a hatáskörét

és az illetékességét hivatalból vizsgálja,¹ amennyiben valamelyik hiányát észleli, akkor átteszi a hatáskörrel és illetékességgel rendelkező nyomozó hatósághoz vagy ügyészhez.² A feljelentés esetén a hatóságnak 3 nap áll rendelkezésre, hogy az abban foglaltakat megvizsgálja, és az alapján elrendelje a nyomozást, vagy elutasítsa, illetve feljelentéskiegészítést rendeljen el. A nyomozó hatóság tudomására kell hozni minden olyan tényt vagy információt, amely alapján a nyomozást le lehet folytatni. Amennyiben a rendőrség a rendelkezésre álló adatok alapján elrendeli a nyomozást, úgy a feljelentésben foglaltakat egy, de akár több alkalommal is kihallgatás formájában tisztázhatja, pontosíthatja, amely során érdemes valamennyi információt maradéktalanul a rendelkezésre bocsátani. A rendelkezésre bocsátott információk mellett a rendőrségnek lehetősége van a 2017. évi XC. törvény, a büntetőeljárásról szóló törvény 261. §-a alapján adatkéréssel élni a szolgáltató(k) felé, aki az abban foglaltaknak megfelelően köteles azt teljesíteni akár ügyészi engedéllyel vagy anélkül. Az egyik legfontosabb kiindulópont lehet az IP-cím (*Internet Protocol address*) beazonosítása. IP-címet használ valamennyi világhálóra feljelentkezett számítástechnikai eszköz, ugyanakkor amennyiben az elkövetők nyilvános számítógépet használtak, vagy technikai úton meg tudták változtatni az IP-címüket, úgy annak sikeres beazonosítása nem minden esetben vezet az elkövetőhöz.

A büntetőeljárás megindulásakor jelentősége van, hogy az adott bűncselekményt hol követték el, és az eljárás lefolytatására melyik hatóságnak van hatásköre. Ez utóbbi meghatározása a nyomozó hatóság hatáskörével és illetékességével foglalkozó rendeletben³ van lefektetve, annyi kitételrel, hogy késedelmet nem tűrő esetben bármely nyomozó hatóság végezhet eljárási cselekményt, azonban erről a hatáskörrel és illetékességgel rendelkező nyomozó hatóságot köteles haladéktalanul tájékoztatni (BÁNÁTI et al. 2018, 473.). A nagyobb gondot sokszor az okozza a virtuális térben elkövetett cselekményeknél, hogy hol követték el a bűncselekményt, és így kinek kell a nyomozást lefolytatni (illetékesség). A 25/2013. (VI. 24.) BM rendelet szerint a nyomozás lefolytatására az a nyomozó hatóság illetékes, amelynek illetékességi területén a bűncselekményt elkövették.⁴ Problémaként merül fel, hogy kiberbűncselekmény esetében az jogosult-e eljárni, akinek a területén észlelték a bűncselekményt, vagy az a hatóság jogosult eljárni, akinek az illetékességi területén a jogellenes cselekményt elkövették, esetleg, ahol az elkövető bejelentett lakcímmel rendelkezik, életvitelszerűen tartózkodik? Amennyiben elfogadjuk, hogy az elkövetés helye szerinti hatóság jogosult eljárni, akkor is egyes bűncselekménytípusoknál, például az online hirdetések csalások esetében, kérdésként merül fel, hogy az elkövetés (tévedésbe ejtés) helye ott van, ahol az elkövető a szándékos megtévesztésre alkalmas dolgot vagy szolgáltatást feltöltött és meghirdette, vagy ott van, ahol azt a sértett vagy sértettek megrendelték. A virtuális tér jellemzőit, az informatikai eszközök elterjedését, tulajdonságait figyelembe véve, ha annak megállapítása lehetetlen, hogy hol történt a tárgy hirdetésének feltöltése a hirdetési vagy közösségi oldalra, akkor annak a hatóságnak kell lefolytatni az eljárást, ahol az elkövető lakik, ismeretlen tettes ellen folytatott nyomozás során ott, ahol a sértett él, több sértett esetén pedig a megelőzés szabályát kell alkalmazni vitás kérdésekben, azaz, ahol először tettek

¹ A Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről szóló 25/2013. (IV. 24.) BM rendelet.

² 25/2013. (IV. 24.) BM rendelet 4. § (2) bekezdés.

³ A Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről szóló 25/2013. (IV. 24.) BM rendelet.

⁴ 25/2013. (VI. 24.) BM rendelet 3. § (1) bekezdés.

feljelentést egy adott bűncselekmény elkövetése miatt.⁵ A kiberbűncselekmények jellemzői alapján el lehet mondani, hogy a virtuális térben elkövetett bűncselekmények esetében már problémát jelent az elkövetés helye, hiszen a világháló egy határok nélküli tér, amelyben az elkövetőnek és a sértettnek vagy áldozatnak még csak földrajzilag sem szükséges egy helyen tartózkodni, így annak megállapítása, hogy ki jogosult eljárni, a hatóságok között illetékességi vitát eredményez. Ibolya Tibor, a Fővárosi Főügyészség vezetője *A számítástechnikai jellegű bűncselekmények nyomozása* című jegyzetben (IBOLYA 2012) az alábbiak szerint közelíti meg a nyomozó hatóság illetékességének problémáját: a gyanúsított egy ismert aukciós portálon egy műszaki terméket hirdetett meg a bolti árnál jóval alacsonyabb értéken. A vételárat előre, egy meghatározott bankszámlaszámra kellett fizetni. A termékre több vidéki városból is érkezett megrendelés és pénzáttétel, amelyeket a gyanúsított egy budapesti bankfiókban felvette. Ez alapján Ibolya Tibor megállapításai a következők voltak:

- a cselekmény elkövetésének helye a gyanúsított lakóhelye, mert onnan töltötte fel a csalárd hirdetést,
- a cselekmény elkövetésének helye a bank budapesti fiókja, mert a gyanúsított ott vette fel a pénzt, a kár ott következett be,
- a cselekmény elkövetésének helye a sértett számlavezető bankfiókjához igazodik, mert a sértett onnan utalta el a vételárat, a kár ott következett be,
- a cselekmény elkövetésének helye a sértett lakóhelye, mert ott olvasta el a hirdetést,
- a cselekmény elkövetésének helye az internetes honlap üzemeltetőjének székhelye, mert az elkövetési magatartást a gyanúsított az interneten tanúsította,
- a cselekmény elkövetésének helye az internet, ezért az iratokat megküldik az ügyésznek állásfoglalásra.

Az említett dilemmák és lehetőségek a csalás (Btk. 373. §) tényállásával kapcsolatban kerültek bemutatásra, mégis valamennyi kibertérben elkövetett bűncselekmény esetében a hatóság számára problémát jelenthet, hogy ki illetékes az ügyben az eljárás lefolytatására. Az ügyészség álláspontja ugyanakkor, hogy az ügyek értelmetlen áttétele helyett azok gyors és eredményes lefolytatása legyen a cél, és ne a kapitányságokon folyamatban lévő ügyek számának csökkentése. Az online csalásokkal kapcsolatban (nem az információs rendszer felhasználásával elkövetett csalás tényállása értendő ezalatt) a BH2011. 332. bírósági állásfoglalás szerint: 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.” Ibolya ügyész úr továbbment az illetékesség fejtegetésekor, amikor azt írta, hogy fontos annak megállapítása, hogy a cselekményt a számítógép mint célpont ellen vagy a számítógép mint eszköz segítségével követték el. Az Egyesült Államokban ugyanakkor érdemes megfigyelni, hogy a joghatóság kérdése nem jelent ilyen problémát azon államokban, ahol van a kiberbűnözéssel, azaz számítógépes bűncselekményekkel kapcsolatban külön törvény, azokkal az országokkal szemben, ahol nincs külön kiberbűncselekményekkel kapcsolatos törvény. A külön kiberbűnözéssel kapcsolatos törvényekkel rendelkező államokban, amennyiben a deliktum elkövetési magatartása épp abba az államba irányul, vagy pedig a támadás vagy

⁵ Ez a szabály természetesen csak a több sértett esetében érvényesül.

jogellenes magatartás onnan származik, akkor a joghatóság nem kérdéses,⁶ hiszen annak az államnak a hatósága jogosult eljárni. Amennyiben a hazai szabályozást – beleértve, hogy a számítógépes bűnözésről szóló egyezmény sem rendelkezik ezzel kapcsolatban –, továbbá Ibolya Tibor ügyész úr álláspontját összehasonlítom az USA azon tagállamainak szabályozásával, ahol kifejezetten érvényesülnek a kiberbűnözéssel kapcsolatos törvények, akkor megállapítható, hogy melyik hatóság jogosult eljárni, egyszerűbben eldönthető. A hatáskör és illetékesség kérdésében az ügyek áttétele tekintetében elsősorban a szemléletmódbeli váltásra kellene koncentrálni, vagyis a megelőzés elve alapján az jogosult eljárni, amelyik hatóságnál hamarabb tették meg a feljelentést. Amennyiben az nem megállapítható, vagy az eljárás szempontjából a célszerűség szem előtt tartásával a gyanúsított tartózkodási helyének megfelelő hatóság illetékességi területén vagy több sértett esetén amennyiben azok egy helyhez köthetők, úgy azok tartózkodási helyén kellene lefolytatni az eljárást.

Az Európai Parlament és Tanács 2013/40. számú irányelvének 12. cikke a joghatóság kérdésében a tagállamokra bízta a döntést, így a direktívában említett bűncselekményeket

- a) egészben vagy részben a területükön követték el; vagy
- b) egy állampolgáruk követte el, legalább azokban az esetekben, ha a cselekmény az elkövetés helyén bűncselekménynek minősül.

A tagállamok biztosítják, hogy joghatósággal rendelkezzenek abban az esetben, ha

- a) az elkövető a bűncselekmény elkövetésekor fizikailag jelen van a területükön, függetlenül attól, hogy a bűncselekmény a területükön található információs rendszer ellen irányul-e; vagy
- b) a bűncselekmény a területükön található információs rendszer ellen irányul, függetlenül attól, hogy az elkövető a bűncselekmény elkövetésekor fizikailag jelen van-e a területükön.

8.2. A kiberbűncselekmények nyomozása

8.2.1. A bűncselekmények eljárási szabályai

A kibertérben elkövetett vagy bármilyen, informatikai eszközökkel vagy eszköz/rendszer ellen elkövetett jogellenes cselekmény esetében is a büntetőeljárásról szóló törvény rendelkezéseit kell alkalmazni. Hazánkban – az Egyesült Államok egyes tagállamaival ellentétben – még nincs számítógépes bűncselekményekkel kapcsolatos külön anyagi és eljárásjogi szabályozás, azokra az általánosan érvényben lévő szabályokat kell alkalmazni, azzal, hogy az eljáró hatóságoknak a kényszerintézkedések és egyéb eljárási cselekmények törvényi ismerete mellett a kreativitásukat is igénybe kell venni, úgy, hogy a törvényesség, az egyenlőség és az arányosság követelményeit is be tudják tartani.

⁶ Arkansas Code of 1987, A.C.A. §5-27-606 Jurisdiction. Elérhető: <http://lexisnexis.com/hottopics/arcodes/Default.asp> (A letöltés dátuma: 2018. 05. 10.) Például Észak-Karolinának is van külön számítógépes bűnözéssel kapcsolatos törvénye: 2010 North Carolina Code, Chapter 14 Criminal Law. Article 60: Computer Related Crime.14-453.2.Jurisdiction.

8.2.2. A felderítés

A bizonyítás mint büntető eljárásjogi fogalom nem más, mint a büntetőjogilag (anyagi jogilag és eljárásjogilag) releváns, múltbéli tények megismerése a törvényes bizonyítási eszközök és módszerek útján, illetve ezeknek a tényeknek az igazolása és rögzítése bizonyítási eszközökkel (FANTOLY–GÁCSI 2013, 202.). A bizonyítás célja a büntetőjogi felelősség eldöntéséhez szükséges releváns tények, ismeretek megszerzése, feladata pedig a bűncselekmény vonatkozásában a tényállás tisztázása (FANTOLY–BUDAHÁZI 2015, 144.). A bizonyítékok tekintetében megkülönböztetünk szabad és kötött bizonyítási rendszert. Magyarországon a büntetőeljárás törvény alapján a szabad bizonyítás elve érvényesül, azaz minden, a büntetőeljárás alapján meghatározott bizonyíték felhasználható, ugyanakkor a törvény elrendelheti egyes bizonyítási eszközök igénybe vételét.⁷

8.2.3. A bizonyítékok összegyűjtése

Az internetes környezetben elkövetett bűncselekmények esetében a bizonyítékok összegyűjtése okozhatja az egyik legnagyobb problémát. A hagyományosnak mondható deliktumokkal szemben a számítástechnikai környezetben elkövetett jogsértő cselekmények vonatkozásában nemcsak fizikai, megfogható bizonyítékok lefoglalása (például: desktop, laptop, tablet, CD/DVD, pendrive) válhat szükségessé, hanem az azokon lévő adatok, információk, valamint a kibertérben lévő elektronikus (elektronikus információs rendszerben tárolt) adat megszerzése, megismerése és evidenciaként történő felhasználása is szükséges lehet. A bizonyítékok megszerzése tekintetében a hatóság rendelkezésére álló lehetőségeket a 2017. évi XC. törvény a büntetőeljárásról, valamint az 1994. évi XXXIV. törvény, a rendőrségről szóló jogszabály sorolja fel, amelyek alapján két típusú adatszerzés lehetséges: 1. a nyomozás elrendelése és a kényszerintézkedés elrendelése során szükséges az esetlegesen felmerülő akadályok miatt a különböző forrásokból – így nyílt vagy nem nyílt forrásokból – származó információk beszerzése és mérlegelése. Az elektronikus bizonyíték – mint a digitális eszközökből vagy a kibertérből nyerhető bizonyíték – magán viseli annak változékonyságát, manipulálhatóságát. Emiatt egyes tagállamokban az e-bizonyítékok összegyűjtésével és értékelésével szemben különleges követelményeket támasztanak annak érdekében, hogy a bíróságok számára elfogadható legyen. Nem mindegy ugyanakkor, hogy a bizonyítékként felhasználható adat hol található. Így az fizikai adathordozón – amelynek nyomain fellelhetők telefonon, számítógépen, nyomtatón vagy netalán gépjárműben, okoseszközön (hűtőgép, hűtő-fűtő berendezés stb.) – vagy a felhőben (*cloud*) tárolódik-e? Sok esetben, eltérően a fizikai térben található bizonyítékoktól, nem elég megtalálni a kérdéses „dolgot”, hanem annak útját mint egy bizonyítékláncolatot szükséges felderíteni és rögzíteni, ily módon

⁷ 1998. évi XIX. törvény a (rég) büntetőeljárásról.

alkalmas lehet a teljes bizonyításra. A bizonyítási eljárás lefolytatásához az alábbi elektronikus vagy digitális bizonyítékok, bizonyítási eszközök begyűjtése szükséges:⁸

- a telekommunikációs eszközök, illetve azok adattartalma,
- számítástechnikai eszközök, illetve azok adattartalma,
- egyéb adathordozók (például pendrive, merevlemez, memóriakártya), illetve azok adattartalma,
- elektronikus formában tárolt könyvelési iratok,
- elektronikus levelezés,
- hangfelvétel,
- elektronikusan tárolt távközlési előfizetői és forgalmi adatok, illetve egyéb mobilkommunikációs adatok,
- elektronikusan tárolt pénzügyi, előfizetői és forgalmi adatok,
- ATM-felvételek,
- mobilkommunikációs adatok,
- biztonsági kamerák és térfigyelő kamerák felvételei.

A bizonyítékok összegyűjtésére vonatkozóan az alábbi megállapítás tehető. A bizonyítékok leggyakoribb beszerzésének lehetősége – például: ATM-felvételek, biztonsági és térfigyelő kamerák felvételei tekintetében – elsődlegesen a nyílt típusú adatszerzés módszerének alkalmazása a célravezető. Ezek: adatkérés kényszerintézkedéssel, mint lefoglalás, információs rendszerben tárolt adatok; megőrzésre kötelezés az ügy megítélésétől vagy attól függően, hogy ismeretlen vagy nem ismeretlen tettes ellen folyt az eljárás; OSINT (*Open Source Intelligent*, azaz nyílt forrású/típusú információgyűjtés) alkalmazásával.

A nem nyílt adatszerzés tekintetében a nyomozó hatóság a nyílt eljárásban nem beszerezhető módon és lehetőségekkel szerezheti meg az ügy eldöntéséhez szükséges adatokat:

- bírói és ügyészi engedélyhez nem kötött leplezett eszközök alkalmazása,
- ügyészi engedélyhez kötött leplezett eszközök,
- bírói engedélyhez kötött leplezett eszközök alkalmazása,
- titkos információgyűjtés.

8.2.4. Az elektronikus bizonyítékok

A nyomozás során a múltban történt események megállapításához szükséges a bizonyítékok összegyűjtése, a tanúvallomások értékelése. A digitális bizonyítékok koncepciójának ugyanazok, mint bármely más bizonyíték, vagyis az információ felhasználásával az azt vizsgáló hatóságok igyekeznek az embereket és az eseményeket időben és térben elhelyezni annak érdekében, hogy a bűncselekmények okait, módszereit a lehető legpontosabban, leprecízebben feltárják. A büntetőeljárás törvény külön nem rendelkezik a digitális bizonyítékokról (*digital evidence*), hanem az elektronikus adatot, valamint az információs eszközt nevesíti, nem határozza meg azok fogalmát, hanem felsorolásszerűen, a hagyományos bizonyítékok körébe vonva tárgyalja azokat. A büntetőeljárásról szóló 2017. évi

⁸ A felsorolás nem teljes, azok köre folyamatosan változik, bűncselekménytípusonként eltérő lehet a bizonyítékként felhasználható elektronikus bizonyítékok köre.

XC. törvény és a Büntető Törvénykönyv is az *elektronikus* kifejezést használja, de emellett a hazai és a külföldi szakirodalomban használt *digitális* kifejezés is szerepel, ezért mindkettő érvényes jelenleg. A *digitális adat* olyan adat, amely egy kódolási eljárással jön létre, és amely alkalmas az elektronikus dokumentum előállításának és egyúttal a dokumentum tartalmának azonosítására. Digitalizálás alatt azt a folyamatot értjük, amelynek során a korábban más (analóg) hordozón rögzített tartalmakat valamilyen digitalizáló eszköz segítségével a számítógép által értelmezhető formában kódoljuk, illetve rögzítjük a gép által olvasható adattároló eszközre. A digitális bizonyítékok egyik nagy területe a hagyományos keresőoldalak kutatása és azok elemzése. A bűncselekményekkel, például a gyermekpornográfiával és a szexkereskedelemmel kapcsolatos nyomozások a digitális bizonyítékokkal foglalkoznak; azonban új utak nyíltak meg az internet egyre növekvő kihasználásával globális értelemben vett kommunikációs eszközként. Ilyen digitális bizonyíték lehet a közösségi oldalak (Facebook, Twitter, Instagram) vagy a különböző kommunikációra használt applikációk, oldalak (Messenger, Viber, Skype, e-mail) tartalma. A digitális bizonyítékok sokszor több információt hordoznak a hatóság számára, mint az elektronikus bizonyítékok, hiszen az azok tartalmához történő hozzáférés nagyobb segítséget nyújthat a hatóság számára, mint a kizárólag elektronikus úton keletkezett evidenciák. Ugyanakkor nem lenne szakszerű, ha a két típusú bizonyítékot megkülönböztetnénk egymástól, hiszen azok több ponton összefüggnek, sokszor együtt említik őket.

8.2.5. A bizonyítékok és az elektronikus adatok

A kiberbűncselekményekkel kapcsolatban a bizonyítékok, azok beszerzése, rögzítése rendhagyónak is tekinthető. A nyomozás során nem feltétlenül a fizikai térben behatárolható evidenciák észlelése nehéz, hanem az azokból összegyűjthető digitális bizonyítékok, amikre eltérő végrehajtási szabályok vonatkozhatnak. A további részletezés előtt szükséges tisztázni, hogy mit is ért a jog az *adat* és az *elektronikus adat* fogalma alatt.

8.2.6. Az adat és az elektronikus adat fogalma

A 2011. évi CXII. törvény az információs önrendelkezési jogról és az információs szabadságról (a továbbiakban: Infotv.) nem határozza meg az adat fogalmát, csak a személyes adat és a különleges adat meghatározását tartalmazza. A 2013. évi L. törvény, az állami és önkormányzati szervek elektronikus információbiztonságát szabályozó jogszabály (a továbbiakban: Ibtv.) értelmező rendelkezéseiben található meg az adat jogi fogalma. Az Ibtv. 1. § (1) bekezdés 1. pontja alapján adatnak tekinthető az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas. A régi Be. nem határozta meg az elektronikus adat fogalmát, sőt, sok esetben nem is használja ezt a kifejezést, így a hatóság a más jogszabályban található fogalomra támaszkodott. A 2018. július elsejétől életbe lépett új büntetőeljárás törvény már külön nevesíti azt: „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.”⁹

8.2.7. Az adatkérés

A 2017. évi XC. törvény, az új Be. megszüntette a megkeresés jogintézményét, és helyette bevezette a 261. §-sal az *adatkérést*, amelynek „keretében a büntetőeljárással összefüggésbe hozható,

- a) a szervezet birtokában lévő adat továbbítása,
 - b) a szervezet birtokában lévő elektronikus adat vagy irat továbbítása vagy
 - c) a szervezet által teljesíthető tájékoztatás adása
- kérhető.”¹⁰

8.2.8. Az adatkérés jelentősége a bizonyítás során

A nyomozó hatóság, az ügyészség és a bíróság adatkéréssel élhet jogi személy, jogi személyiséggel nem rendelkező gazdasági szervezet, állami vagy helyi önkormányzati szervezet felé is. Az eljárási törvény tételesen felsorolja az érintett szervezeteket. Az adatkérésnek fontos szerepe van a bűncselekmény felderítésében és további szakaszokban is, ugyanakkor számtalan esetben volt arra példa, hogy a gyanúsított épp egy adatkérés során szerzett tudomást az őt érintő eljárásról. A bizonyítás során a különféle adatok, információk (így például metaadatok) ismerete, hozzáférése a nyomozás alkalmával sok esetben szükséges, azok beszerzése a Be. 261. §-a alapján lehetséges a szolgáltatótól az előkészítő eljárás során, például az elektronikus hírközlési szolgáltatótól, banktitkokat, fizetési titoknak, értékpapírtitoknak vagy biztosítási titoknak minősülő adatot kezelő szervezettől, az egészségügyi és a hozzájuk kapcsolódó személyes adatot kezelő szervezettől. Meghatározott feltétel bekövetkezése esetére a rendőrség vagy a terrorizmus kezelésével foglalkozó szervezet ügyészségi engedéllyel, három hónapra (amely egyszer még meghosszabbítható) állami, helyi önkormányzati stb. szervezettől a Be. 266. §-a alapján adatszolgáltatást kérhet (feltételes adatkérés). De az adatkéréssel beszerezhető és felhasználható adatok a nyomozás szempontjából sokszor nélkülözhetetlenek; a hírközlési szolgáltatóktól beszerezhető a hívószám előfizetőjének a neve és adatai, a telefon IMEI-száma, a SIM-kártya IMSI-száma, valamint ennek alapján a híváslista, a hívások időtartama, valamint az úgynevezett kelő-fekvő pozíciók, a telefonpartner neve. Az adatkérés során a hatóság a harmadik félről az alkalmazásszolgáltatótól szerzi be az információt. A szolgáltató az elektronikus kereskedelmi szolgáltatásokról, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény alapján titkosított kommunikációt biztosító szolgáltatást nyújt, köteles az ilyen alkalmazás igénybevételével továbbított küldeményekkel, közlésekkel kap-

⁹ Be. 205. § (1) bekezdés.

¹⁰ Be. 261. § (3)–(4) bekezdés.

csalatosan keletkező vagy kezelt¹¹ adatokat, beleértve a metaadatokat, azok keletkezésétől számított egy évig megőrizni.¹² Így az alkalmazásszolgáltatók tekintetében a kért adatok vonatkozásában a hatóság megkereséssel kell, hogy éljen. A külső engedélyhez kötött titkos információgyűjtésre jogosult szerv megkeresése esetén a titkosított kommunikációt biztosító szolgáltatást nyújtó alkalmazásszolgáltató a szolgáltatás típusát, a szolgáltatás előfizetőjének vagy felhasználójának a szolgáltatás igénybevételéhez szükséges azonosító adatait, a szolgáltatás igénybevételének dátumát, kezdő és záró időpontját, a regisztrációhoz használt IP-címét és portszámát, az igénybevételnél használt IP-címét és portszámát, a felhasználói azonosítót köteles átadni.¹³

8.2.9. Az elektronikus bizonyítékokhoz történő hozzáférés

A legtöbb problémát a nyomozó hatóság számára az jelenti, amikor a számítástechnikai rendszerben tárolt adathoz hozzá kell férni, vagy amikor az ügy szempontjából olyan lényeges adatra van szükség, amely valamelyik közösségi oldalon a felhasználó fiókjában vagy felhőben kerül elhelyezésre. Ezt a két esetet, illetve szabályozást tekintve az alábbiak szerint történik az eljárás. Van olyan, hogy akár a levelezési rendszer, akár pedig valamelyik közösségi háló fiókjába a belépéshez nem kell sem a felhasználónevet, sem a jelszót megadni, mivel az adott informatikai eszközön a kényszerintézkedést elszenvető be van jelentkezve, vagy a beállítások úgy vannak megadva, hogy a felhasználónevet és a jelszót az adott számítógépen vagy IP-címen megjegyzik, és az automatikus belépési funkció be van rajta állítva. A nyomozó hatóság számára az eljárás lefolytatása szempontjából a büntetőeljárásról szóló törvény alapján a következő eljárási cselekmény lefolytatása válhat szükségessé: bár a belépés akadályok nélkül végrehajtható, főleg abban az esetben, amikor a kényszerintézkedést elszenvető fél együttműködik, mégis a Be. 302. §-a szerint lehetséges a lakás, az egyéb helyiség vagy jármű átkutatása, valamint az információs rendszer, illetve adathordozó átkutatása a büntetőeljárás eredményességének érdekében. Ebből az eljárásjogi szabályból következik, hogy az informatikai rendszerben tárolt elektronikus adat – függetlenül attól, hogy a kutatást elszenvető fél abba beleegyezik-e vagy sem, illetve az adott rendszert (*ergo* számítógépet, adattároló eszközt) védik-e jelszóval vagy nem, az lefoglalható, átvizsgálható, az azon tárolt adat rögzíthető, megismerhető, az bizonyítékként felhasználható. A Be. alapján a kutatást (annak részletes szabályait lásd *A kutatás* című alfejezetben) az érintett – tehát nem feltétlenül a gyanúsított – jelenlétében kell lefolytatni. A kutatás megkezdése előtt az érintettet fel kell szólítani, hogy a keresett dolgot adja elő, vagy pedig az információs rendszeren tárolt adatokat tegye a hatóság számára hozzáférhetővé. Amennyiben a kért bizonyítékot a hatóság részére átadja, vagy az adatot önszántából hozzáférhetővé teszi – azaz a belépéshez szükséges jelszót megmondja, átadja –, úgy a kutatás nem folytatható (az erre vonatkozó részletes eljárás menete a későbbiekben kerül kifejtésre). Ugyanakkor amennyiben a hatósággal nem működik

¹¹ 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről.

¹² 2001. évi CVIII. törvény 13/B. § (1) bekezdés.

¹³ 2001. évi CVIII. törvény 13/B. § (1) bekezdés.

együtt az eljárással érintett, úgy a nyomozó hatóságnak más módon kell az információs rendszerben tárolt adatot megszerezni, megismerni, olyan formában, hogy az bizonyításra alkalmas legyen. Ugyanez a szabály vonatkozik arra az esetre is, ha a gyanúsított eleve be van jelentkezve a levelezési rendszerébe vagy pedig a közösségi fiókjába, és a hatóságnak „csak” a belépés gombra kell kattintania, vagy az automatikus belépés van a böngészőjébe beállítva. Ezekben az esetekben is érvényben van a számítástechnikai bűnözésről szóló egyezmény (az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezménye) 32. cikke, a *Tárolt számítástechnikai adathoz való hozzáférés határokra tekintet nélkül, hozzájárulás vagy nyilvános elérhetőség esetén* kimondja, hogy „a Szerződő Fél a másik Szerződő Fél engedélye nélkül:

- a) a nyilvánosság számára elérhető módon (nyílt forrású) tárolt számítástechnikai adathoz hozzáférhet, függetlenül az adat földrajzi elhelyezkedésétől; vagy
- b) a másik Szerződő Fél területén tárolt számítástechnikai adathoz hozzáférhet vagy a területén levő számítástechnikai rendszer útján azt megszerezheti, amennyiben a Fél beszerzi az adat számítástechnikai rendszer útján történő átadására jogszabályban feljogosított személy önkéntes és jogszerű hozzájárulását.”

A helyzet bonyolultságát adja, hogy nem minden állam írta ezt alá, így az eljárást csak az aláíró országok/felek területén kell végrehajtani. Kérdésként merül fel, hogy az egyezmény implementálása megtörtént-e a saját büntetőeljárásai törvényükben.

A kiberbűncselekmények nyomozása során a legnagyobb jelentősége egyrészt magának a felhasználó által megadott adatoknak van, másrészt a felhasználó által hagyott úgynevezett *internetes lábnyomnak*, avagy digitális nyomnak van, amely a webes böngészési előzményeket, a készített és a tárolt, feltöltött dokumentumainkat jelenti. A felhasználók nyomokat hagynak az interneten, a különböző informatikai eszközökön, akár levelezésekkel, (családi) fényképek, videók megosztásával, internetes rendeléssel, vásárlással, a különböző online piaci műveletekkel vagy pedig az elektronikus közigazgatási rendszerek (ügyfélkapu) igénybevételével. A régi Be. szerint a nyomozó hatóság feladata az, hogy a bizonyítási eljárás során a Be. rendelkezéseit betartva bizonyítsa a jogellenes cselekmény elkövetését, felderítse és értékelje az eljárás során összegyűjtött bizonyítási eszközöket,¹⁴ a törvényesség betartása mellett a szükséges nyomozati cselekményeket elvégezze. Az új büntetőeljárásai törvény a nyomozó hatóság feladatát már másképp határozta meg: a bűncselekmények felderítése érdekében előkészítő eljárást és nyomozást végez.¹⁵ Az informatikai eszközök és rendszerek terjedése, azok széles körű használata során új kihívásokkal szembesülnek a rendészeti és nemzetbiztonsági szervek, amelyek sok esetben megkönnyíthetik a cselekmény, illetve az elkövető megállapítását, ugyanakkor – a jogi szabályozásra figyelemmel – sokszor indokolatlanul van megkötve a kezük a bizonyítékok beszerzése és értékelése tekintetében. Érdekes módon, a jogalkotók szándékainak ismeretében a hatóságokat sokkal szigorúbb szabályok kötik az internetes környezetben elkövetett eljárási cselekmények szabályozása

¹⁴ A régi büntetőeljárásról szóló 1998. évi XIX. törvény 77. § (1)–(2) bekezdés.

¹⁵ Be. 31. § (1) bekezdés.

tekintetében, és a figyelem nagyobb eséllyel irányul rájuk, mint a felhasználók által hanyagul kezelt jelszavak, adatvédelmi beállítások esetére. A digitális bizonyítékok keletkezésével kapcsolatban a legfontosabb annak megértése, hogy valamennyi nyom egyedi, annak keletkezésével, értékelésével kapcsolatban nem szabad egy sémát felállítani, hiszen a bűncselekmények jellegétől, az elkövetők számától, informatikai tudásától és jellemzőitől függően változhatnak.

8.2.10. Bizonyítékok a fizikai térben

A kibertérrel összefüggésbe hozható deliktumokkal kapcsolatban a kutatás során a fizikai térben is keletkezhetnek bizonyítékok, az azokkal kapcsolatos cselekmények a kényszerintézkedés foganatosítása során dilemmát jelenthetnek.

1. Számítógép: az egyik legfontosabb nyomhordozó eszköz lehet a számítógép, amely fajtáját tekintve vagy PC (*personal computer*), vagy laptop. A számítógép a kutatás során általában a legkézenfekvőbb tárgy, ami szinte valamennyi bűncselekmény esetében hordozhat olyan nyomokat, amelyek bizonyítékként használhatók.
2. Mobiltelefon: a mobiltelefont ma már a legtöbb felhasználó miniszámítógépként, személyi asszisztensként használja. Sokszor több adatot és információt tartalmaz, és több mindent lehet megtudni a tulajdonosáról, mint a rendelkezésre álló rendszerből, a személyről elvégzett információgyűjtésből. A mobiltelefonok egyrészt telekommunikációs eszközök, másrészt dokumentumok, fényképek, egyéb adatok tárolására alkalmasak. Ugyanannyi vagy talán több információt hordozhatnak, ezért a bizonyítás során kiemelkedő szerepük van.
3. Perifériák: a perifériák azok a számítógéphez csatlakoztatható eszközök, amik egy további eszköz illesztését oldják meg. A perifériát általában – de nem feltétlenül – a külvilággal történő kapcsolattartásra használja a számítógép. Tipikus periféria a nyomtató, a billentyűzet, az egér és a monitor.¹⁶ A perifériák már nemcsak egyszerűen kiegészítik a számítógépet, hanem sok esetben olyan információt is hordoznak, amelyek digitális bizonyítékok nyomait hordozzák, így kényszerintézkedések során lefoglalásuk és vizsgálatuk nélkülözhetetlen.
4. Tartós adathordozók: Az Európai Parlament és a Tanács 2011/83/EU irányelve (2011. október 25.) a fogyasztók jogairól (23) bekezdése – a fenti határozatnak megfelelően – kimondja, hogy „[a] tartós adathordozóknak lehetővé kell tenniük a fogyasztó számára az adattárolást mindaddig, amíg [...] érdekei védelmének érdekében szükségesnek tartja”, továbbá, hogy „[a]z ilyen adathordozók közé sorolandók különösen a papír, az USB-kulcsok, a CD-ROM-ok, a DVD-k, a memóriakártyák vagy a számítógépek merevlemezei, illetve az elektronikus levelek.”

¹⁶ Periféria címszó. Elérhető: <https://pcforum.hu/szotar/perif%C3%A9ria> (A letöltés dátuma: 2018. 07. 30.)

8.2.11. Bizonyíték a virtuális térben

A nyomozás sikeres lezárásának érdekében a hatóságnak mérlegelnie kell, hogy mit lehet bizonyítéknak tekinteni, valamint azokat hogyan, milyen eszközökkel és milyen taktika keretében lehet beszerezni. A bizonyítékok megszerzése még a hagyományosnak nevezhető bűncselekmények (így a lopás, csalás vagy akár emberölés) esetében is gondos mérlegelést igényel. Mérlegelni kell, hogy mit kell bizonyítéknak tekinteni, valamint annak átgondolása is nélkülözhetetlen, hogy az evidenciákat milyen módszerrel szerzik meg és tárolják annak érdekében, hogy azok minden kétséget kizáróan az eljárás végéig alkalmasak legyenek a bíróság előtti bizonyításra. A *hagyományosnak* nevezhető bűncselekmények esetében – emberölés, közokirathamisítás, csalás, lopás stb. – a bizonyítás az elkövetés eszközének maradéktalan megszerzése, a helyszínen rögzíthető nyomok biztosítása, rögzítése (fénykép-, videó- vagy akár hangfelvétel formájában) esetlegesen oly módon, hogy azok alkalmasak legyenek arra, hogy szakértő vagy szaktanácsadó a hatóság által feltett kérdéseket minden kétséget kizáróan meg tudjanak válaszolni.

8.2.12. A kutatás és a lefoglalás

A kényszerintézkedések közül a kutatás és a lefoglalás szabályai kerülnek részletesen bemutatásra mint a bizonyítékok megszerzésének egyik, hatóság által történő kikényszerítése.

8.2.12.1. Kutatás

Nem új eljárási cselekményként, hanem a *házkutatás* kifejezés helyett alkalmazza a jogalkotó a *kutatást* mint kényszerintézkedést. Annak végrehajtásakor a hatóság beleavatkozik az Alaptörvényben meghatározott kutatást elszenvedő személy(ek) alapvető jogaiba azáltal, hogy a bűncselekmény gyanúja esetén annak bizonyítására, a bizonyítékok felkutatására, az elkövető kilétének megállapítására, valamint az információs rendszer, illetve adathordozó átvizsgálása érdekében hajtja végre. A kutatás a büntetőeljárás eredményes lefolytatása érdekében a lakás, az egyéb helyiség, a bekerített hely vagy a jármű átkutatása. A kutatás információs rendszer, illetve adathordozó átvizsgálására is kiterjedhet. A kutatásra vonatkozó eljárási szabálynál nincs lényegi változás annak elrendelése tekintetében. Így akkor kerül az elrendelésére, ha

- bűncselekmény elkövetőjének elfogására,
- bűncselekmény nyomainak felderítésére,
- bizonyítási eszköz megtalálására,
- elkobozható, illetve vagyonekobjzás alá eső dolog megtalálására vagy
- információs rendszer, illetve adathordozó átvizsgálására vezet.¹⁷

A kutatást a bíróság, az ügyészség vagy a nyomozó hatóság saját hatáskörében eljárva rendelheti el az új eljárási törvény életbelépése után. A védett helyiségekben, így a közjegyzői vagy ügyvédi irodában végrehajtandó kutatás esetében, amikor a közjegyzői vagy

¹⁷ 2017. évi XC. törvény 302. § (1) bekezdés.

ügyvédi tevékenységgel összefüggő védett adat megismerésére irányul az intézkedés, a kutatást a bíróság rendeli el, ahol az ügyész részvétele kötelező. Ugyanakkor azokra a helyiségekben, ahol szenzitív, illetve személyes adatokat kezelnek, például az egészségügyi intézményekben történő kutatás esetén sem a bíróság általi elrendelés, sem az ügyész részvétele nem szükséges a jogalkotó szándéka szerint. Ha a kutatás elrendeléséhez szükséges bírósági határozat meghozatala olyan késedelemmel járna, amely a kutatással elérni kívánt célt jelentősen veszélyeztetné, a kutatás a bíróság határozata nélkül is végrehajtható. Ilyen esetben a bíróság határozatát utólag haladéktalanul be kell szerezni. Ha a kutatást a bíróság nem rendeli el, annak eredménye bizonyítékként nem használható fel.¹⁸ A kutatást elrendelő határozatnak tartalmaznia kell a kutatás célját és az elrendelését megalapozó tényeket. Ha ez lehetséges, a kutatást elrendelő határozatban meg kell jelölni azt a személyt, bizonyítási eszközt, elkobozható vagy vagyoneklobzás alá eső dolgot, információs rendszert vagy adathordozót, aki vagy amely megtalálására a kutatás irányul. A kutatást az érintett ingatlan vagy jármű tulajdonosának, birtokosának vagy használójának a jelenlétében kell végrehajtani. A kutatásra vonatkozó lényeges változások nem történtek, így annak megkezdése előtt ismertetni kell a kutatást elrendelő határozat tartalmát, és a határozatot a helyszínen kézbesíteni kell.¹⁹ Ha a kutatás meghatározott személy, bizonyítási eszköz, dolog, információs rendszer vagy adathordozó megtalálására irányul, akkor fel kell szólítani az érintett ingatlan, illetve jármű tulajdonosát, birtokosát vagy használóját, illetve az általa megbízott személyt, hogy a keresett tárgyi bizonyítási eszköz vagy személy hollétét fedje fel, illetve a keresett elektronikus adatot tegye hozzáférhetővé. A felszólítás teljesítése esetén a kutatás csak akkor folytatható, ha megalapozottan feltehető, hogy a kutatás során más bizonyítási eszköz, dolog, információs rendszer vagy adathordozó is fellelhető. A Be. 305. § (4) bekezdése szerint tehát a hatóság felszólítására az elektronikus információs rendszer vagy adat önkéntes hozzáférhetővé tétele esetén a kutatás kizárólag abban az esetben folytatható, ha megalapozottan feltehető, hogy a további kutatás eredményeként újabb bizonyítékok is fellelhetők. A kutatás végrehajtását egy tervezésnek kell megelőznie, amely során a nyomozók adatkéréssel és információgyűjtéssel megszerzik azokat az adatokat, hogy milyen eszközöket kell keresni. Ennek tudatában lehetne előre megtervezni, hogy hogyan hajtsák végre a kényszerintézkedést. De nem minden információ szerezhető meg az eljárási törvényben meghatározott lehetőségekkel. Így tervezés során nem deríthetők fel azok az eszközök (például pendrive, SSD-kártya), amelyek a kereskedelmi forgalomban bármikor és bárhol beszerezhetők, és amelyek mérete alkalmassá teszi ezeket a könnyű elrejtésre. Fontosnak tartom annak hangsúlyozását, hogy ma már bármilyen bűncselekményről legyen szó – akár kiberbűncselekmény, testi sértés, vagyon elleni bűncselekmény, akár katonai bűncselekmény –, a gyanúsított vagy sértett birtokában lévő informatikai eszközöknek szerepük van a bizonyítás tárgya vagy eszköze tekintetében, így azok rejtékelyét, az azzal kapcsolatos teendőket szükséges megtervezni, az adathordozókra történő esetleges rögzítésre felkészülni. A számítástechnikai és telekommunikációs eszközök vonatkozásában a 100/2018. (VI. 8.) Korm. rendelet²⁰ alapján, valamint a lefoglalt eszköz tekintetében az arra vonatkozó BM-PM rendeletnek (a lefoglalás alponban részle-

¹⁸ 2017. évi XC. törvény 303. § (3) bekezdés.

¹⁹ 2017. évi XC. törvény 305. § (3) bekezdés.

²⁰ A nyomozás és az előkészítő eljárás részletes szabályairól szóló 100/2018. (VI. 8.) Korm. rendelet.

tezetteknek) megfelelően járnak el a hatóságok. Amennyiben felmerül annak lehetősége, hogy számítástechnikai eszköz átvizsgálása válhat szükségessé, úgy informatikai szakértők/szaktanácsadók kirendelésének szükségességét meg kell fontolni, akik esetleg már a kutatás alkalmával is megjelennek, elvégzik az adatok és eszközök szakszerű átvizsgálását, szükség esetén az adatok mentését. A Készenléti Rendőrség Nemzeti Nyomozóiroda Kiberbűnözés Elleni Főosztálytól (röviden: KR NNI KBEFO) vagy a Budapesti Rendőr-főkapitányság Korrupciós és Gazdasági Bűnözés Elleni Főosztály Pénzhamisítás és Csúcstechnológiai Bűnözés Elleni Osztály Csúcstechnológiai Bűnözés Elleni Alosztálytól (a továbbiakban: BRFK KGBEFO) szakirányítás kérhető. Mivel nem minden kapitányság rendelkezik a kényszerintézkedések végrehajtásához szükséges megfelelő eszközökkel, továbbá bizonyos szakkérdésekben a rendőrség állománya nincs a megfelelő tudás birtokában, emiatt sokszor vesznek igénybe külső segítséget. A külső segítség, a szakértő vagy szaktanácsadó az, aki a helyszínen elvégzi azokat a teendőket és rendelkezik azokkal az eszközökkel, amelyek a sikeresen végrehajtott eljárási cselekményhez elengedhetetlenek. Az informatikai eszköz tulajdonosát vagy kezelőjét az eljárás megkezdésekor fel kell szólítani, hogy a keresett adatot tegye hozzáférhetővé. Amennyiben az eszköze vagy csak egyes dokumentumok jelszóval vagy biometrikus azonosítóval védettek, akkor annak a hatóság rendelkezésére bocsátása a rendszerbe történő belépéséhez szükséges. Az információs rendszerben létrejönnek olyan információk, amelyek a különböző alkalmazások, szoftverek segítségével keletkeznek – dokumentumok, táblázatok, az internetről letöltött képek stb. (digitális lábnyom) –, amelyek háttérinformációval szolgálhatnak a hatóság számára, és amelyek egyébként nem beszerezhetők, csak az informatikai eszköz és a rajtalévő adat átvizsgálásakor. Ha csak egy bizonyos információra van szükség, amelynek szolgáltatására az állami, önkormányzati szerv egyébként is köteles, és az információ kinyeréséhez nem szükséges speciális ismeret, akkor a nyomozó hatóságok a megkeresés eszközhöz nyúlnak, azaz küldenek egy átiratot. Erre példa lehet annak lekérdezése, hogy adott időszakban mely munkatársak végeztek munkát az állami, önkormányzati szerv adott épületében. Ha a beszerezendő információ az eljárás szempontjából kiemelten fontos, vagy annak kinyeréséhez speciális információ szükséges, esetlegesen tartani lehet attól, hogy az adatokat törlik vagy felülírják, akkor egy erőforrás-igényesebb és gyorsabb eljárási cselekmény következhet: a lefoglalás.

8.2.12.2. Lefoglalás

Erre példa lehet, amikor a nyomozó hatóság akár az állami, önkormányzati szerv épületében önálló cselekményként, akár egy nyilatkozattételre jogosult személy tanúkénti kihallgatása alkalmával lefoglalja a munkatársak rendszerhasználatáról szóló logfájlokat tartalmazó adatokat és az azokat rögzítő adathordozót. A kutatás az eljárás alá vont személy jogaiba történő egyik legerősebb beavatkozás a fentebb említettek közül. Tipikusan akkor alkalmazható, ha más intézkedés nem biztos, hogy eredményre vezetne, vagy a nyomozás érdekében ez tűnik a legcélszerűbbnek. Jellemzően akkor kerül foganatosításra, ha az eljárás alá vont személy nem együttműködő, vagy a beszerezendő adat, információ nem egyszerűen körülírható, annak gyűjtéséhez speciális ismeret szükséges. Példaként említhető, amikor az állami, önkormányzati foglalkoztatott a hivatali informatikai eszközöket használja fel illegális tevékenységre, például zsaroló, fenyegető e-mailek küldésére, gyermekeket ábrá-

zó pornográf felvételek tárolására (SIMON–GYARAKI 2017). Az eljárásjog szerint tárgyi bizonyítási eszköz alatt értendő minden olyan tárgy – ideértve az iratot és az okiratot is –, amely a bizonyítandó tény bizonyítására alkalmas, többek között:

- amely a bűncselekmény elkövetésének vagy a bűncselekmény elkövetésével összefüggésben az elkövető nyomait hordozza,
- amely a bűncselekmény elkövetése útján jött létre,
- amelyet a bűncselekmény elkövetéséhez eszközül használtak, vagy
- amelyre a bűncselekményt elkövették.

Irat minden olyan tárgyi bizonyítási eszköz, amely műszaki, vegyi vagy más eljárással adatokat rögzít, így különösen a papíralapú vagy elektronikus adatként létező szöveg, rajz, ábra. Okirat az az irat, amely valamilyen tény, adat valóságának, esemény megtörténtének vagy nyilatkozat megtételének bizonyítására készül, és arra alkalmas. Az okiratra vonatkozó rendelkezések irányadók az okiratról készült kivonatra is. A 100/2018. (VI. 8.) Korm. rendelet a nyomozás és az előkészítő eljárás részletes szabályairól a kutatásról és a lefoglalásról felvett jegyzőkönyvvel összefüggésben a 86. § (1) bekezdésében az alábbi rendelkezéseket tartalmazza: „Az információs rendszer átvizsgálása során biztosítani kell az információs rendszer útján – védelmi eszköz vagy informatikai megoldás megkerülése vagy kijátszása nélkül – hozzáférhető adatok megismerését és rögzítését.”

Amennyiben tehát a nyomozás során számítógép lefoglalására kerül sor, fontos kiemelni, hogy egy kutatás alkalmával nem vizsgálhatjuk át a számítógépen tárolt adatokat. Sőt, ha az adott eszköz kikapcsolt állapotban van, akkor azt tilos a helyszínen bekapcsolni. Ennek az az oka, hogy minden bekapcsoláskor a korábban mentett adatok az adathordozón módosulnak. Olyan adatok is, amelyek a nyomozás során relevanciával bírhatnak (például, hogy mikor volt az utolsó rendszerindítás). Ez alól képeznek az esetlegesen a nemzetbiztonságot vagy a közbiztonságot súlyosan sértő bűncselekmények körébe tartozó esetek, vagy ahol a várható bizonyítékok késedelmes beszerzése rendkívüli érdeksérelemmel vagy kár okozásával járna. A bíróság előtt hitelt érdemlően bizonyítani kell tudni a rögzített digitális adatok, bizonyítékok eredetiségét. Az eljárás minden pontján – az intézkedés megkezdésétől egészen a bírósági tárgyalásig – igazolni kell tudni az eszközök változatlanságát, vagy ha azokon változtatás történt, akkor arra csak dokumentálás mellett, szakmai előírások betartásával van lehetőség.

1. A lefoglalásra aprólékosan fel kell készülni. Ha okunk van feltételezni, hogy az elkövető konspirál és adatait rejt, vagy biztonsági intézkedéseket vethet be az adatok hozzáférhetetlensége érdekében, akkor mindig vonjunk be szaktanácsadót (KR NNI KBEFO, NBSZ, BRFK KBEFO vagy belső rendszergazda), esetleg szakértőt a szakértői névjegyzékből.
2. A kutatás, lefoglalás megkezdésekor az intézkedés alá vont személyeket el kell távolítani az adott eszköz közeléből, és meg kell akadályozni a fizikai hozzáférést (szükség esetén kényszerintézkedések alkalmazásával). Az intézkedés alá vont személyeket célszerű akár ekkor kihallgatni arra vonatkozóan, hogy ki használja a számítógépet. Az elkövetők ezen a területen általában nem tapasztalt kriminális személyiségek – így az első kényszerintézkedés okozta „sokkot” még hatékonyabban ki lehet használni.

3. Az inkriminált IT-eszköztől fénykép- és videófelvételt indokolt készíteni, majd a külső fizikai adatkapcsolatot megszakítani (a hálózatról leválasztani). Wifi-kapcsolatot a bejövő internet kapcsolatának megszakításával – például külső antenna lecsavarásával, laptopon repülőgépmód-kapcsolóval –, jegyzőkönyvi rögzítés mellett kell megszüntetni.
4. Alapvető szabály, hogy az eljárási cselekménnyel érintett személyt sosem hagyjuk magára, mindig felügyelet alatt kell állnia, és meg kell fosztani minden lehetséges kommunikációs eszköz alkalmazásának lehetőségétől. Indokolt a ruházat átvizsgálása is, amely során felszólítjuk a zsebében található tárgyak átadására.
5. Az adatkapcsolat megszüntetését követően rögzítjük a jegyzőkönyvben, fénykép-, esetleg videófelvételen, hogy milyen alkalmazások futnak, milyen környezetben helyezkedik el a számítógép, amiből esetlegesen a használatját is lehet azonosítani (például csak ő cigarettázik, és csikkek vannak a gépnél).
6. Amennyiben szükségessé válhat, úgy minden, az eljáráshoz kapcsolódó adathordozót lefoglalunk, majd a számítógépet lehetőség szerint rendes, szabályos leállítással kikapcsoljuk.
7. Amennyiben destruktív folyamatok zajlanak az eszközön – azaz törlés vagy enkriptálás zajlik –, akkor minden más intézkedést megelőzően indokolt lehet a folyamatok megszakítása, amit leghatékonyabban az áramellátás (az elektromos áram vagy az akku lecsatlóása) megszüntetésével valósítható meg.
8. Amennyiben az elkövető személye vagy az aktuálisan futó alkalmazások (BitLocker, Truecrypt, DiskCryptor, FileVault) arra engednek következtetni, hogy az eszköz titkosítva van, de az eljárási cselekmény fogantatásánál a titkosítás fel van oldva, akkor semmiképpen nem kapcsolható ki az eszköz a jelszó ismerete nélkül. Ilyen esetben például a laptoptal szakértőhöz kell menni, vagy azt kihívni, amennyiben ez semmiképpen nem oldható meg, akkor az egyébként titkosított, de aktuálisan elérhető adatokról nem titkosított másolatot kell készíteni folyamatos jegyzőkönyvi, esetleg videófelvételes rögzítés mellett.
9. A gép kikapcsolás nélküli – jellemzően szakértőt igénylő – vizsgálata abban az esetben is szükséges lehet, ha valamilyen hálózati szolgáltatás (Facebook, Gmail stb.) vagy felhőalapú tárolás valósul meg. Ezek a kapcsolatok az eszközök kikapcsolásával, elszállításával jellemzően megszűnnek, így az eljárás adataira tekintettel mérlegelni kell, hogy mi szolgálja jobban annak érdekeit.
10. A csomagolásra legalkalmasabb a nagyméretű plasztikzsák bekötve, bűnjelcímkézve. (Nem megfelelő eljárás, hogy a készüléket és annak csatlakozási felületeit a lefoglalást elszennvedő által is aláírt öntapadós vagy leragasztott papírokkal biztosítjuk, hiszen ezek sérülése, leválása esetén nem bizonyítható az eszközök lefoglaláskori állapota.)
11. Ezt követően nyílik majd lehetősége a szakértőnek vagy a szaktanácsadónak, hogy a bitazonos másolat készítését követően a másolaton szakértői munkát, keresést hajtson végre. A bűnjelzsák kibontása az érintettek előzetes kiértesítését követően jegyzőkönyvi rögzítés mellett lehetséges, ha arra a szakértőnek történő megküldés előtt szükség van.

Bontható digitális eszközök esetén lehetőség van rá, hogy egyenként rögzítsük az eszközben található adathordozók gyártmányát, típusát, egyedi sorozatszámát – természetesen minden esetben fényképek készítése mellett az eszközről és a szerelési folyamatról. Ennek akkor lehet jelentősége, ha a szakértő kirendelését megelőző ajánlatkéréshez pontos információkat szeretnénk megadni. Itt tehát három lehetőség van:

- a helyszínen rögzítjük az eszközök tulajdonságait,
- későbbi bűnjelzsák bontásakor vesszük fel az adatokat,
- a szakértő az ajánlatát hiányos adatok alapján adja meg, ami később az ajánlat ki-bővítéséhez vezethet.

Nem bontható vagy lezárt burkolatú digitális eszközök esetén rögzíteni kell az eszköz gyártmányát, típusát, egyedi sorozatszámát. Fontos, hogy hiteles igazságügyi másolatot készíteni megfelelő hardver (írásvédő) és/vagy szoftver segítségével lehetséges. A másolási folyamat nem változtathatja meg az eredeti adatot. Az igazságügyi másolás eredménye lehet hiteles másolat (*forensic clone*) vagy hiteles lemezkép (*forensic image*). Előbbinél egy 4GB-os pendrive-on lévő 3MB-os kép másolata kb. 4GB-os lesz, míg az utóbbinál csak kb. 3MB-os. Ezek az eszközök (például írásvédő) csak kiemelt rendőri egységeknél állnak rendelkezésre. Az általános bűnügyi munkában szükséges szoftverek (FTK Imager)²¹ alkalmazásának szabályai gyakorlati foglalkozásokon kerülnek ismertetésre. Az azonos bittartalmat egy kódolással generált ellenőrzőösszeg (hash-kulcs) igazolja. Ha az eredeti adatot akár egy bittel is módosítják, akkor az újragenerált kód nem lesz azonos. Ezzel biztosítható az adatok integritása.

8.2.13. Általános eljárás a mobilkommunikációs eszközök lefoglalása esetén

Az eszközt működésben tartani kizárólag akkor szükséges, ha az ügy során ésszerűen feltételezhető, hogy az észlelt biztonsági elemek vagy titkosítás akadályoznák a *post mortem* – azaz kikapcsolt állapotú – szakértés hatékonyságát. Ebben az esetben a mobil kommunikációs eszközt bekapcsolva kell tartani, de a távközlési hálózattól el kell szigetelni (például Faraday-kalitka segítségével), valamint biztosítani kell az eszköz folyamatos tápellátását. Bekapcsolva lefoglalt eszköz hálózattól való elszigetelése azért indokolt, mert a felhasználó távolról megsemmisítheti az eszközön tárolt digitális bizonyítékokat, illetve a normális hálózati működés során is megváltozhatnak a készülékben tárolt digitális bizonyítékok.

8.2.14. A szemle

A bűncselekmény elkövetésével érintett rendszer alaposabb vizsgálata lehet szükséges a bűncselekmény elkövetője által hátrahagyott nyomok összegyűjtése és rögzítése érdekében. A vizsgálat a szemle szabályai szerint hajtható végre. A régi Be. alapján szemlét

²¹ FTK Imager. Elérhető: <https://accessdata.com/product-download/ftk-imager-version-3.2.0> (A letöltés dátuma: 2018. 09. 19.)

a bíróság, illetőleg az ügyész rendel el és tart, ha a bizonyítandó tény felderítéséhez vagy megállapításához személy, tárgy vagy helyszín megtekintése, illetőleg tárgy vagy helyszín megfigyelése szükséges.²² A szemle mint bizonyítási cselekmény lehetőséget biztosít a nyomozó hatóságnak, az ügyészségnek, illetve a bíróságnak arra, hogy a bizonyítandó tény megállapítása érdekében, vagy amennyiben a bizonyítás szempontjából indokolt, tárgyat, személyt vagy helyszínt megfigyeljen. A szemlénél, ha a hatóság úgy ítéli meg, vagy valamilyen körülmény indokolja, szakértőt is lehet alkalmazni, vagy amennyiben az információs rendszer vagy adathordozó átvizsgálása valami miatt különleges szakértelmet igényel, az elektronikus bizonyítékok összegyűjtésére szaktanácsadó vehető igénybe, aki a későbbiekben már nem rendelhető ki szakértőként. A szemle alkalmával a bizonyítás szempontjából jelentős körülményeket részletesen rögzíteni kell. A szemlén fel kell kutatni és össze kell gyűjteni a tárgyi bizonyítási eszközöket, és gondoskodni kell a megfelelő módon történő megőrzésükről. A szemle tárgyáról, ha lehetséges és szükséges, kép- vagy hangfelvételt, illetve képet és hangot egyidejűleg rögzítő felvételt, rajzot vagy vázlatot kell készíteni, és azt a jegyzőkönyvhöz kell csatolni. Az interneten található bizonyítékok mentése általában *online szemle* keretében történik. Az adatmentésben az eljáró nyomozók végzik az ügyben releváns adatok keresését és rögzítését, így az internetes kereséseket, a letöltött fájlokat. Az adatmentés folyamatáról jegyzőkönyv vagy jelentés készül, amelynek részletesnek kell lennie, a folyamatokat, megállapításokat rögzíteni kell. Az adatokról érdemes úgynevezett *image-fájl*t készíteni, amit *hash-kulccsal* kell azonosítani, amelyet egy adathordozón rögzítenek (ez utóbbi lehet CD-/DVD-/BR-disc vagy winchester). E mozzanat részleteit is jegyzőkönyvben kell rögzíteni. Amennyiben az információs rendszer vagy adathordozó részletes átvizsgálása a nyomozó hatóság részéről nem szükséges, bizonyos esetekben az elektronikus bizonyíték adatkérés útján is beszerezhető.

8.2.15. Leplezett eszközök a kiberbűncselekmények felderítésében

A fent nevesített kényszerintézkedések mellett a másik legcélravezetőbb megoldás a nyomozó hatóság kezében a leplezett eszközök alkalmazása, amelyek különösen alkalmasak lehetnek a szervezett bűnözés, a terrorcselekmény megállapítására, a korrupcióval összefüggő bűncselekmények és a kiberbűnözés felderítésére, megelőzésére. A büntetőeljárási törvényben, a Rendőrségről szóló 1994. évi XXXIV. törvényben, továbbá a Nemzeti Adó- és Vámhivatalról szóló 2010. évi CXXII. törvényben, a 100/2018. (VI. 8.) Korm. rendeletben meghatározzák a leplezett eszközök alkalmazásának lehetőségeit, az ügyési és bírói engedélyhez kötött, valamint ahhoz nem kötött lehetőségeket. A szabályozás említését azért tartom fontosnak, mivel ez az egyik olyan lehetőség a nyomozó hatóság kezében, amellyel a kibertérben elkövetett jogellenes cselekményeket és az azt elkövetőket jóval nagyobb eséllyel lehet tetten érni, mint a nyílt eljárásban meghatározott módszerekkel.

²² Be. 119. § (1) bekezdés.

8.2.16. A leplezett eszközök igénybevételének általános szabályai

A számítógépes bűncselekmények olyan atipikusnak nevezhető, a társadalmat, gazdaságot és nemzetállamokat veszélyeztető cselekmények, amelyek az elkövetés jellege, annak hatása miatt nemcsak a nyomozó szervekre, hanem a nemzetbiztonsági szervezetekre is feladatokat rónak. „A leplezett eszközök alkalmazása olyan a magánlakás sérthetlenségéhez, valamint a magántitok, a levéltitok és a személyes adatok védelméhez fűződő alapvető jogok korlátozásával járó, a büntetőeljárásban végzett különleges tevékenység, amelyet az erre feljogosított szervek az érintett tudta nélkül végeznek.”²³

A leplezett eszközök alkalmazása során az azt igénybe vevő szervezetnek be kell tartania:

- a szükségesség,
- az arányosság,
- a célszerűség elvét.

Azaz a leplezett eszközök akkor alkalmazhatók, ha

- megalapozottan feltehető, hogy az eljárás során bizonyítékként felhasználható adatok, információk a leplezett eszköz alkalmazása nélkül nem lennének megismerhetők;
- a leplezett eszköz alkalmazása nem jár az érintett(ek) alapvető jogainak aránytalan sérelmével.

A leplezett eszközök és módszerek alkalmazása a számítógépes bűncselekmények felderítésének talán egyik legfontosabb lehetősége, ugyanakkor nem minden esetben olyan egyszerű, mint a hagyományos bűncselekmények esetében.

8.2.17. Az információs rendszer titkos megfigyelése

A bírói engedélyhez kötött leplezett eszközök egyike – ahogyan az előzőekben is említettem – az információs rendszer titkos megfigyelése. Az eszköz alkalmazása során az arra feljogosított szerv bírói engedéllyel az információs rendszerben kezelt adatokat titokban megismerheti, az észlelteket technikai eszközzel rögzítheti. A rögzítés módját a Be. nem határozza meg, így az a megfigyelt személytől, a bűncselekmény jellegétől és a helyszín adott tulajdonságaitól kiterjedhet:

- a rendszerben tárolt adatok tartalmára, esetleg a metaadatokra,
- a rendszerhez történő hozzáféréshez szükséges jelszavakra, felhasználó azonosítókra,
- a rendszeren keresztül történő kommunikáció megfigyelésére, megismerésére,
- a rendszert használók megismerésére (hang- és képrögzítésre).

Az információs rendszer titkos megfigyelése történhet közvetlenül és közvetetten; a számítástechnikai eszközön egy kívülről feltelepített program segítségével, valamint

²³ Be. 214. § (1) bekezdés.

a számítógépet megfigyelő kép-, illetve hangrögzítésre alkalmas eszköz elhelyezésével [Be. 232. § (3) bekezdés, a hely titkos megfigyelése], illetve ennek a két rendszernek a kombinációjával együttesen.

8.2.18. Az előkészítő eljárás

Az új büntetőeljárásról szóló törvény a nyomozásokban nagyobb szerepet szán az ügyészségnek mint közvádlnak mind a vizsgálati, mind pedig a felderítési szakban. A törvény szerint az ügyészség nyomoz, felügyeli a felderítés törvényességét, valamint irányítja a vizsgálatot. Az ügyészség előkészítő eljárást végez, és a más szerv által végzett előkészítő eljárásban ellátja az e törvényben meghatározott feladatait.²⁴ A kibertérben elkövetett deliktumok során az előkészítő eljárásnak kiemelt jelentősége van, hiszen a hagyományos bűncselekményekkel ellentétben magasabb a látencia, valamint a bizonyítást is sokban nehezíti a nemzetközi és technikai jellege is. Előkészítő eljárást a nyomozó hatóság vagy az ügyészség folytathat le annak érdekében, hogy megállapítsák, hogy a bűncselekmény gyanúja fennáll-e.²⁵ Maga az előkészítő eljárás nem más, mint a leplezett eszközök alkalmazására feljogosított szerv által folytatható eljárás, valamint nyílt eszközökkel is folytatható adatszerzés, amit a törvényben meghatározott szervezetek és azok megsegítésére a rendőrség belső bűnmegelőzési és bűnfelderítési feladatokat ellátó szerve, illetve a rendőrség terrorizmust elhárító szerve is végezhet. Az előkészítő eljárás az egyik legalkalmasabb jogintézménye lehet annak, hogy a hatóság egyszerű gyanú esetén saját monitorozó tevékenységet végezve a törvényben meghatározott eljárás lehetőségével éljen, és a rendelkezésre álló idő – hat hónap, egyes esetekben kilenc hónap – alatt bűncselekmény elkövetésének fennállását bebizonyítsa, vagy épp elvesse. Bármely bűncselekmény miatt folytatható (így nincs megkötés sem a büntetési tétel, sem pedig a bűncselekmény típusa tekintetében), így a kibertérben elkövethető valamennyi deliktum miatt, saját hatáskörben eljárva a nyomozó hatóságok vagy az ügyészség megkezdheti az eljárást. Az előkészítő eljárás esetében elvégezhető adatszerző tevékenység a rendelkezésre álló és a törvényben meghatározott szervezetek nyilvántartásaiból és a törvényben még nem szabályozott OSINT-tal (*Open Source Intelligence* – nyílt forrású információgyűjtés) is elvégezhető. Az OSINT-tevékenység törvényben történő szabályozásával kapcsolatban nem vagyok meggyőződve annak szükségességéről, ugyanakkor az azáltal szerzett bizonyítékok hitelessége, felhasználhatósága kérdéseinek tisztázása viszont időszerű lenne már. A leplezett eszköz is igénybe vehető az előkészítő eljárás során, de csak azzal a gyanúsítottal szemben, aki a bűncselekmény elkövetőjeként szóba jöhet, és az ő tartózkodási helyének megállapítása, elérhetőségének megismerése céljából. A kiberbűncselekmények esetében az elkövetők megismerése, felderítése mindig nehézséget okoz az internetes felhasználók anonimitása miatt. A bűnözők számára egyre népszerűbb a kibertér, mivel az azon keresztül folyó kommunikáció ténye a hatóságok számára sokszor nehézségekbe ütközött. Amennyiben az unió kívánságát figyelembe vesszük, miszerint a kibertér ne a bűnözők menedéke legyen, úgy további szabályozásokra még szükség lenne, anélkül, hogy a szólás- és véleménynyilvánításhoz fűződő jogok sérülnének.

²⁴ Be. 25. § (1)–(3) bekezdés.

²⁵ Be. 340. § (1) bekezdés.

8.2.19. Az előkészítő eljárás során alkalmazható ügyészi engedélyes leplezett eszközök

A leplezett eszközök alkalmazásának előnye, hogy a bűncselekményt elkövetővel szemben az annak végrehajtására feljogosított szerv – azért, hogy az eljárás célját titokban tartsa – a bűncselekményre vonatkozóan információkat, adatokat gyűjthet anélkül, hogy arról az adott személy értesülne. A számítógépes környezetben elkövetett gazdasági, illetve tartalom-bűncselekmények, valamint a terrorcselekmények bizonyítása esetében a rendelkezésre álló leplezett eszközök alkalmazása nagyobb sikerrel kecsegtethet, mint a korábbi Be.-ben szabályozott lehetőségek.

8.2.20. A fizetési műveletek megfigyelése

A fizetési műveletekre vonatkozó új eljárásjogi szabályozás különösen alkalmas lesz az információs rendszer felhasználásával elkövetett gazdasági bűncselekmények felderítésére és vizsgálatára. Bármelyik bűncselekmény elkövetésének legfontosabb bizonyítása lehet a pénz útjának nyomon követése, az illegális forrásból származó jövedelmek felderítése, de a kibertérben elkövetett bűnözésnél – ahol sokszor csak egy bankszámlaszám ismert, és esetleg egy fiktív vagy hajléktalan személy, ahol a számlák közötti átvezetések a netbankolásnak köszönhetően bárholnan és bármikor intézhetők – a fizetési műveletek határozott időtartamra történő megfigyelésének köszönhetően a pénz mozgása, a számlák birtokosainak tevékenysége valós időben válik nyomon követhetővé, és nem napokkal vagy esetleg jóval később beszerezhető adatokból ismerhető meg. Fizetési művelet megfigyelésének számít például a pénzforgalmi számlával kapcsolatos valamennyi fizetési művelet vagy a fizetési műveletekre vonatkozó adatok rögzítése, továbbítása.

A fizetési műveletek megfigyelése legfeljebb három hónapra rendelhető el, amelyet az ügyészség egy alkalommal legfeljebb további három hónappal hosszabbíthat meg. A megfigyelés alatt a fizetési műveletek felfüggeszthetők legfeljebb két napig, de ennek tényéről a pénzügyintézet – a szolgáltató – sem az érintettnek, sem harmadik félnek nem adhat tájékoztatást.

A kriptovalutákkal kapcsolatos műveletek mint fizetési műveletek megfigyelésének szabályai jelenleg még nem kivitelezhetők. A probléma egyik oka, hogy a fizetési művelet nem függeszthető fel, hiszen nincs számlavezető bank a digitális pénz mögött, valamint a 100/2018. (VI. 8.) Korm. rendeletben meghatározott szabályok szerint a szolgáltatót tájékoztatni kell az eljárásról, ami a kriptovaluták esetében nem lehetséges.

8.2.21. Álvásárlás

Az ügyészség engedélyével a bűncselekménnyel feltehetően összefüggésbe hozható dolog vagy annak mintája megszerzésére vagy szolgáltatás igénybevételére, az eladó bizalmának erősítése céljából a bűncselekményre vonatkozó tárgyi bizonyítási eszközt eredményező dolog megszerzésére vagy szolgáltatás igénybevételére, az elkövető elfogásának

elősegítésére irányuló színlelt megállapodás köthető és teljesíthető.²⁶ Az álvásárlás tehát nemcsak kézzel fogható dolog, hanem bármilyen szolgáltatás igénybevételére alkalmazható (feltételezhetően a dark net esetében bitcoinért, vagyis kriptovalutáért megszerezhető illegális szolgáltatás vagy dolog is érthető alatta). Az álvásárláshoz fedett nyomozó vehető igénybe.

8.2.22. *Fedett nyomozó alkalmazása*²⁷

A fedett nyomozó feladata a kibertérben elkövetett bűncselekmények esetén speciálisabb lehet, mint a fizikai térben végzett munkájuk, hiszen amellett, hogy a technikai eszközök sokszor a segítségükre lehetnek egy-egy feladat elvégzése során, ugyanakkor hátráltató tényező is az, hogy ismerniük kell a kibertérben alkalmazott nyelvezetet, a szakzsargont, és nem utolsósorban nehezítésként előfordulhat, hogy a bűnözővel nem kerülnek kapcsolatba személyesen. A Be.-ben a fedett nyomozó alkalmazására legfeljebb hat hónapra van lehetőség az ügyészség engedélyével, amely alkalmanként hat hónappal meghosszabbítható. A büntetőeljárás céljának végrehajtása érdekében „[...]

- a) bűnszervezetbe történő beépülés,
- b) terrorista csoportba vagy terrorcselekmény feltételeinek biztosításához anyagi eszközök szolgáltatása vagy gyűjtő, továbbá terrorcselekmény elkövetését vagy terrorista csoport tevékenységét anyagi eszközök nyújtásával vagy egyéb módon támogató szervezetbe történő beépülés,
- c) álvásárlás,
- d) rejtett figyelés végrehajtása,
- e) [...] az információ továbbítása vagy
- f) a bűncselekménnyel összefüggő információk és bizonyítékok megszerzése érdekében alkalmazható.”²⁸

Fedett nyomozó alkalmazása különösen alkalmas lehet olyan bűncselekmények elkövetésének bizonyításában az előkészítő eljárás vagy a felderítés²⁹ során, amikor az ügy bonyolultsága, az abban részt vevő személyek összetartása miatt egyébként lehetetlen lenne a bizonyítékok megszerzése vagy azok biztosítása.

Ilyen bűncselekmény lehet különösen a kritikus infrastruktúrák elleni támadások malware-rel vagy a gyermekpornográfia bűncselekmény bizonyítása, amikor is az elkövetők zárt csoportokban kommunikálnak egymással titkosított csatornákon, így a szervezetbe történő beépülés, a tagok megismerése, a bűncselekmény helyének lokalizálása során lehet kiemelkedő jelentősége a munkájuknak.

²⁶ Be. 221. §.

²⁷ Be. 222. §.

²⁸ Be. 222. § (2) bekezdés.

²⁹ A nyomozás és az előkészítő eljárás részletes szabályairól szóló 100/2018. (VI. 8.) Kormányrendelet 133. §.

„Nem büntethető a fedett nyomozó az alkalmazása során elkövetett bűncselekmény, szabálysértés vagy közigazgatási bírsággal sújtandó szabályszegés miatt, ha annak elkövetése

- a) a fedett nyomozó alkalmazásának eredményességéhez, az alkalmazással elérni kívánt bűnüldözési célhoz szükséges, és az alkalmazással elérni kívánt bűnüldözési érdek jelentősebb, mint a fedett nyomozó felelősségre vonásához fűződő érdek,
- b) a fedett nyomozó biztonságának biztosítása, lelepleződésének megakadályozása érdekében szükséges, és a fedett nyomozó biztonságával, lelepleződésének megakadályozásával kapcsolatos érdek jelentősebb, mint a fedett nyomozó felelősségre vonásához fűződő érdek, illetve
- c) más bűncselekmény elkövetésének megelőzése vagy megszakítása érdekében szükséges, és a bűncselekmény megelőzéséhez vagy megszakításához fűződő érdek jelentősebb, mint a fedett nyomozó felelősségre vonásához fűződő érdek.”³⁰

8.2.23. A szakértő

A szakértő bevonásának, szerepének fontossága, a szakértő igénybevétele egy büntetőeljárás során mindig is kérdéses. A szakvéleménynek egyre nagyobb szerepe van a bizonyítási eszközök között, hiszen a technika, technológia fejlődésének köszönhetően a korábban még sikertelenül befejezett ügyekben szerzett bizonyítékok értékelhetővé váltak, és a bizonyítás és az elkövető felderítése is egyre sikeresebb lett. A büntetőeljárás törvény alapján, ha a bizonyítandó tény megállapításához vagy megítéléséhez különleges szakértelem szükséges, szakértőt kell alkalmazni.³¹ Szakértelmet igénylő kérdésnek, vagyis szakkérdésnek minősíthető minden olyan releváns kérdés, ami nem minősül jogkérdésnek, és a bizonyításhoz szükséges felhasználhatósága szakértelmet kíván. Az új büntető eljárásjogi törvény ismét nem határozta meg a különleges szakértelem fogalmát (ahogy más jogszabályok sem), ennek ellenére a szakértő kirendelése szükségességének mérlegelésekor az alábbi meghatározást kell szem előtt tartani: a jogi szakmától különböző, valamely más tudományos, technikai szakterületre, esetleg művészeti ágra vonatkozó ismereteket takarja. A szakértő a bíróság különleges szakértelmét pótolja, feladata a releváns szakkérdések megvilágítása és értékelése. Ebből következik, hogy a szakértő jogkérdésekben nem nyilváníthat véleményt. Ebből következhetne, hogy a szakértő csak olyan különleges szakkérdésekben adhat véleményt, amellyel kapcsolatban a bíróságnak nincs relevanciája (szubjektív tényező), ami nem zárja ki tehát azt, hogy egyes esetekben a nyomozó hatóság eljáró tagja, aki viszont képességeinél vagy tudásánál fogva bizonyos véleményt adhatna, megtehetné azokat a cselekményeket, amelyekre képes. A szakértő és szaktanácsadó jogszabályi környezete mellett az egyes bűncselekménytípusok vizsgálata során a kirendelésükre ténylegesen a törvényben meghatározott különleges szakértelem miatt kerül sor, vagy pedig a nyomozó hatóság tagjának a „kényelmét”, esetleg a tehetetlenségét vagy még rosszabb esetben „mert így szoktuk” hozzáállását tükrözi. A bizonyítás tárgya közé tartozik a szakvélemény, amelynek elkészítése csak az igazságügyi szakértői tevékenységről szóló törvényben meghatározott feltételek

³⁰ Be. 224. § (1) bekezdés.

³¹ Be. 188. § (1) bekezdés.

alapján végezhető.³² Az igazságügyi szakértő feladata – a hatóság kirendelése vagy megbízása alapján –, hogy a tudomány és a műszaki fejlődés eredményeinek felhasználásával készített szakvéleménnyel döntse el a szakkérdést.³³ Szakkérdésnek minősülnek azok a vizsgálatok, amelyek elvégzéséhez különleges szakértelem szükséges (például halott személy esetében DNS-vizsgálat, mérgezéssel összefüggő toxikológiai vizsgálat stb.) A szakértő feladata, hogy az adott ügyben a hatóság által történt kirendelés alapján, a legjobb tudása szerint, pártatlanul, a szakértői kirendelő határozatban feltett kérdésekre a törvényben meghatározott határidő alatt befejezze a vizsgálatot. De a szakértőnek nem feladata, hogy jogkérdésben döntsön. Vagyis az, hogy a hatóság egy cselekményt bűncselekménnyé minősítsen, vagy a pontos tényállás meghatározását a szakértőtől várja, már nem tartozik a különleges szakértelem alá. Ugyanúgy igaz ez a kiberbűncselekmények esetében is, még ha az eljáró nyomozó a legkevesebb informatikai ismerettel is rendelkezik, akkor sem várhatja el az általa kirendelt informatikai szakértőtől, hogy minősítse az adott cselekményt.

8.2.24. Szakértő, szaktanácsadó és eseti szakértő

Szakértő alkalmazására akkor van tehát szükség, ha a bizonyítandó tény megállapításához vagy megítéléséhez különleges szakértelem szükséges.³⁴ A meghatározás nem is feltétlenül szükséges, hiszen a különleges szakértelem szubjektív fogalom, ráadásul azt sem fejtí ki a jogalkotó, hogy az adott szakértelem valamilyen különleges eszköz felhasználásával vagy pedig a szakember különleges tudásával függ össze. Az informatikával kapcsolatos ismeretek igen széles körben mozognak. Kezdve azzal, hogy a jogalkalmazók körében annak ismerete, hogy melyik mobil eszköz, számítógép milyen típusú operációs rendszerrel működik, vagy melyik futtatható rajta, egészen a komoly informatikai tudást igénylő programozási kérdésekig, eltérést mutat, amely összefügg az életkorral, a tanulással és a nyitottsággal az új tudás felé. A rendőrségen dolgozó nyomozók tudása tekintetében is erős eltérések mutatkoznak, amit még nehezít az is, hogy az informatikai eszközök szinte valamennyi bűncselekmény vagy szabálysértés esetében megtalálhatók mint bizonyítékot hordozó eszközök, így az sem teljesen egységes, hogy milyen esetekben elég egy egyszerű megállapítás. Ehhez még hozzátartozik, hogy semmilyen iránymutatás, állásfoglalás nem született arra vonatkozóan, hogy mely típusú vizsgálatok esetében szükséges a szakértő kirendelése, és mely esetekben elég, ha azt rendőri jelentés formájában (amely teljes bizonyító erejű okirat) az ügy gazdája végzi el. A szakértő szerepe a büntetőeljárás során a rendelkezésre bocsátott adatok, eszközök vizsgálata a feltett kérdésekre, ezáltal a bizonyítékok szolgáltatása. Az eseti szakértő olyan – az eljárásban megállapítandó vagy megítélendő jelentős tény vagy egyéb körülmény megállapításához vagy megítéléséhez – megfelelő szakértelemmel rendelkező természetes vagy jogi személy, aki nem igazságügyi szakértő; valamint olyan igazságügyi szakértő, aki az igazságügyi szakértői szakterületekről, valamint az azokhoz

³² 2016. évi XXIX. törvény az igazságügyi szakértőkről, 5–10. §.

³³ Az igazságügyi szakértőkről szóló 2016. évi XXIX. törvény 3. § (1) bekezdés.

³⁴ Be. 188. § (1) bekezdés.

kapcsolódó képesítési és egyéb szakmai feltételekről szóló rendeletben meg nem határozott szakterületen ad szakvéleményt.³⁵

A szakértői törvény szerint eseti szakértő is igénybe vehető, ha

- az adott szakterületen nincs bejegyzett igazságügyi szakértő,
- az adott szakterületen – időszakos hiány vagy egyéb szakmai ok miatti hiány okán – a bejegyzett igazságügyi szakértők egyike sem tud eleget tenni a kirendelésnek, vagy
- az adott szakterület nem szerepel a miniszter rendeletében felsorolt szakterületek között.

A jogalkotó a 9/2006. (II. 27.) IM rendelet mellékleteiben határozza meg azokat a szakterületeket és az azokhoz tartozó felsőfokú végzettségeket, amelyek igazságügyi szakértői tevékenység végzésére jogosítanak:

- a tűzvédelmi, valamint személy- és vagyonvédelmi területeken,
- orvosi, továbbá egyes pszichológiai és biológiai területeken,
- munkabiztonsági területen,
- mező- és erdőgazdálkodási, valamint az élelmiszeripari területeken,
- közlekedési és az ipari területeken,
- informatikai és hírközlési területeken,
- környezetvédelmi, a természetvédelmi és a vízügyi területeken,
- kulturális területen,
- gyógypedagógiai és egyes pszichológiai területeken,
- közgazdasági, vámügyi és egyes pénzügyi területeken,
- lakás- és építésügyi, településrendezési, valamint az idegenforgalmi területeken,
- kriminalisztikai területeken,
- audiovizuális média területén,
- titokvédelmi területen.

Abban az ügyben, amelyben számítástechnikai eszköz vagy az azon tárolt adat került lefoglalásra, és szükséges annak vizsgálata, mindenképpen fel kell tenni a kérdést: biztos, hogy ki kell rendelni szakértőt az adott ügyben? A kérdés megválaszolásakor mérlegelni kell, hogy a szakértő, még ha a legcsekélyebb vizsgálatot is végzi, mindig időt vesz el, és növeli a bünygyi költséget, amely a végén nem feltétlenül térül meg az államnak. Jogszabály meghatározhatja azokat a szakkérdéseket, amelyekben meghatározott szakértő jogosult véleményt adni.³⁶ Milyen vizsgálatok végezhetők el a szakértő igénybevétele nélkül?

- Egy adott informatikai vagy mobilkészít típusának, IMEI-, IMSI-számának megállapítását a nyomozó hatóság bármely tagja el tudja végezni, még abban az esetben is, ha a készüléken nem látható ez az információ.
- Amennyiben a mobiltelefonon lévő információk hozzáférhetők, úgy az abban tárolt fényképek, telefonkönyv, kimenő, bejövő, nem fogadott hívások mind a telefon menüjéből, mind pedig a szolgáltatótól beszerezhetők, az ügy előadója önállóan képes megnézni. Ugyanez vonatkozik az üzenetekre is.

³⁵ Az igazságügyi szakértőkről szóló 2016. évi XXIX. törvény 2. § (2) bekezdés.

³⁶ Be. 188. § (3) bekezdés.

- Amennyiben a számítástechnikai rendszer hozzáférésehez szükséges jelszó rendelkezésre áll, arról természetesen feljegyzést kell készíteni, az abban tárolt adatok tulajdonságaihoz, kiterjesztésükhöz, típusának megállapításához szintén nem kell szakértő kirendelése.

8.2.25. Az igazságügyi szakértő kirendelésének szükségessége

Jelenleg általánosan elmondható, hogy a kibertérrel összefüggő bűncselekmények esetében a nyomozó hatóság azért rendel ki szakértőt, mert vagy félnek attól, hogy a digitális bizonyítékot nem ismerik fel, eljárási hibát követnek el a kényszerintézkedés végrehajtásakor, az ügy fajtája ténylegesen indokolja, vagy az ügyben eljáró ügyészség csak a „pecsétetes” papírt fogadja el, és a hatóság tagja által készített jelentést, amely egyébként közokiratnak minősül, nem fogadja el, hanem szakértő kirendelését írja elő. A szakértőtől várják el azt a szaktudást, amivel nem rendelkeznek. De ne várjuk el, hogy a szakértő minden esetben az ügy kellő ismerete nélkül képes elvégezni az ügygazda munkáját, és a vonatkozó törvény értelmében ez nem is az ő feladata.

Annak meghatározását, hogy az adott ügyben milyen tárgyi bizonyítékra van szükség, és azt milyen kényszerintézkedéssel kell beszerezni, ne a kirendelt szakértőtől várjuk el. A kirendelő határozatban a pontosan meghatározott tényállás, az adatkérés és a nyílt információgyűjtés során beszerzett adatok szükséges mértékű tájékoztatása hozzájárul a főlegszakszakértői vizsgálatok elvégzéséhez és a kiegészítő szakvélemény készítéséhez, továbbá a bűnügyi költség főlegszakszak növeléséhez.

8.2.26. Igazságügyi informatikai szakértő kirendelése, az igazságügyi szakértő jogai és kötelezettségei

A kirendelésre vonatkozóan általában a szokásjog játszhat szerepet, pedig egyes esetekben az adott kérdés megválaszolása saját hatáskörben is megoldható lenne. Az igazságügyi szakértővel kapcsolatban elvárható magatartás, hogy úgy kell eljárnia, mint ahogyan azt kirendelője (az ügy előadója) tenné, ha rendelkezne olyan különleges szakértelemmel, amelyre vonatkozóan szakértő bevonását látta szükségesnek. A szakértőtől elvárható tehát az az ismeret és jártasság, amely biztosítja számára, hogy a kirendelésekor birtokába került informatikai eszközök vagy elektronikus adatok vizsgálata úgy történjen, hogy egyrészt a kirendelő határozatban megadott tényállásnak megfelelően a feltett kérdésekre teljes mértékben válaszoljon, kétség se férjen hozzá, hogy azok megőrizték eredetiségüket, változatlanságukat. Az elkészített szakértői véleménynek érthetőnek, világosnak kell lenni, hogy az alkalmas legyen a büntetőeljárásban a további felhasználásra. Nem utolsósorban pedig a szakértő kötelessége a számára átadott tárgyak, eszközök, adatok eredetiségének a megőrzése és a szakértői vélemény elkészítésével együtt a hatóság számára történő visszaadása.

A kirendelt szakértő köteles és jogosult mindazokat az adatokat megismerni, amelyek a feladatának teljesítéséhez szükségesek, e célból

- a) az eljárás ügyiratait – a törvényben meghatározott kivételekkel – megismerheti,
- b) az eljárási cselekményeknél jelen lehet,

- c) a terhelttől, a sértettől, a tanútól, a vagyoni érdekelttől, az egyéb érdekelttől és az eljárásban kirendelt szakértőtől felvilágosítást kérhet,
- d) a kirendelőtől újabb adatokat, ügyiratokat és felvilágosítást kérhet,
- e) a kirendelő felhatalmazása alapján a neki át nem adott tárgyi bizonyítási eszközt, elektronikus adatot megtekintheti, megvizsgálhatja, mintavételt végezhet.

A szakértő a vizsgálat során személyt és tárgyi bizonyítási eszközt, elektronikus adatot tekinthet és vizsgálhat meg, a személyhez kérdéseket intézhet.³⁷ Ha a szakértő olyan tárgyi bizonyítási eszközt vagy elektronikus adatot vizsgál meg, amely a vizsgálat folytán megváltozik vagy megsemmisül, annak egy részét lehetőleg az eredeti állapotban úgy kell megőriznie, hogy az azonosság, illetve a származás megállapítható legyen. A kirendelő meghatározhatja azokat a vizsgálatokat, amelyeket a szakértőnek a kirendelő jelenlétében kell elvégezni, ezáltal biztosítva van annak lehetősége, hogy a nyomozó hatóság a vizsgálatokban aktívan részt vegyen, ezáltal folyamatosan figyelemmel kísérje a szakvélemény elkészítésének menetét. Az új szakértői törvény a szakértői vélemények tartalma vonatkozásában az alábbi kötelezettségeket fogalmazza meg.³⁸

„A szakvéleménynek tartalmaznia kell

- a) a leletet,
- b) a vizsgálat módszerének rövid ismertetését,
- c) a szakmai ténymegállapításokat,
- d) a szakértő véleményét,
- e) ha az ügyben korábban vizsgálat lefolytatására került sor, és a kirendelés erre kiterjed, a korábbi vizsgálatra vonatkozó adatok és megállapítások értékelését,
- f) a módszertani levélre történő utalást, illetve a módszertani levélben foglaltaktól történő eltérés esetén ennek indokait.”

A szakértő – valamennyi típusú igazságügyi szakértőt értve alatta³⁹ – részvételének szükségessége a kiberbűncselekmények nyomozása vagy bármelyik eljárási cselekménye során vita tárgyat képezheti. Nincs egységes álláspont sem a hatóságok, sem a büntetőeljárás egyéb résztvevői – így az ügyészség, bíróság – között annak tekintetében, hogy van-e szükség szakértő kirendelésére, és ha igen, mikor, vagy pedig fölösleges pénzkidobás a legtöbb esetben, hiszen azokat a vizsgálatokat, amelyeket elvégez, azt akár a helyi informatikus vagy rendszergazda is el tudja végezni.

³⁷ Be. 192. §.

³⁸ Az igazságügyi szakértőkről szóló 2016. évi XXIX. törvény 47. § (1) bekezdés.

³⁹ Az igazságügyi szakértők típusát, ahol szükséges, pontosan meg fogom határozni. Amikor a szakértő kifejezést használom, akkor mint gyűjtőfogalmat értem alatta.

8.2.27. A szakértő vagy szaktanácsadó igénybevételével kapcsolatban felmerülő elvárások, feltételek

A régi büntetőeljárásról szóló törvény alapján csak abban az esetben szükséges a szakértő kirendelése, ha a bizonyítandó tény megállapításához vagy megítéléséhez különleges szakértelem szükséges,⁴⁰ ennek szabályozása a 2017. évi XC. törvényben sem változott.

Az eljárásjogunk sajnos nem határozza meg a *különleges szakértelem* fogalmát, így előfordulhat, hogy még abban az esetben is ki kellett rendelni a szakértőt, amennyiben a nyomozó hatóság tagja rendelkezik a szakkérdés megválaszolásához szükséges képességgel, tudással (esetleg a megfelelő végzettsége is megvan hozzá, de mégsem szakértő), pusztán azért, hogy ezáltal bizonyítási eszközt szolgáltatson a nyomozás során. Ugyanakkor a nyomozás során a szakértő által készített szakvélemény részbizonyítéknak minősül, hiszen az ő feladata a rendelkezésre bocsátott bizonyítékok, valamint az őt kirendelő határozatban feltett kérdésekből levonható következtetések megállapítása, azok alapján a vélemény elkészítése.

A szakértő alkalmazása kötelező, ha

- a) a bizonyítandó tény, illetőleg az eldöntendő kérdés személy kóros elmeállapota, illetőleg kábítószerfüggősége,
- b) a bizonyítandó tény, illetőleg az eldöntendő kérdés kényszergyógykezelés szükségessége,
- c) a személyazonosítást biológiai vizsgálattal végzik,
- d) elhalt személy kihantolására kerül sor.

A kiberbűncselekmények esetében a szakértő kirendelése más, mint az eddig ismertett eljárési szabályok során, mert a kényszerintézkedésnél történő igénybevétele az ügytípusok és a nyomozók felkészültségének függvénye. Az igazságügyi szakértőkről szóló törvény alapján tehát „Az igazságügyi szakértő feladata, hogy a hatóság által kirendeléssel vagy megbízás alapján, a tudomány és a műszaki fejlődés eredményének felhasználásával készített szakvéleménnyel, a függetlenség és pártatlanság követelményének megtartásával döntse el a szakkérdést, és segítse a tényállás megállapítását.”⁴¹ A szakterületek elkülönítése az igazságügyi szakértőkről szóló, korábban hatályos 2005. évi XLVII. tv. 3. § (1) bekezdésében, majd a jelenleg hatályos 2016. évi XXIX. tv. 5. § (5) bekezdésében foglalt felhatalmazás alapján a 9/2006. (II. 27.) IM rendeletben történt meg.

A rendelet az informatika vonatkozásában az alábbi (szak)területeket határozza meg:

- informatikai berendezések, számítógépek, perifériák és helyi hálózatok (hardver),
- informatikai biztonság,
- informatikai rendszerek tervezése, szervezése,
- stúdiótechnika, multimédia területtel összefüggő informatikai tevékenység,
- számítástechnikai adatbázis, adatstruktúrák,
- szoftverek [9/2006. (II. 27.) IM rendelet 6. számú melléklet A) pont, MÁTÉ 2017].

Az informatikai szakértő kirendelésével kapcsolatban fontos, hogy ne azért történjen meg annak igénybevétele, mert a hatóság a jogszabályok és/vagy alapvető informatikai tudás birtokában nem képes az ügyben dönteni, hiszen magának a szakvéleménynek az elkészítése időigényes, és esetleg fölösleges bűnügyi költséget generálhat.

⁴⁰ A régi büntetőeljárásról szóló 1998. évi XIX. törvény 99. § (1) bekezdés.

⁴¹ Az igazságügyi szakértőkről szóló 2016. évi XXIX. törvény 3. § (1) bekezdés.

A szakértő kirendelése mellett szóló érvek:

- mivel a digitális nyomok változó környezetben keletkeznek, így azok változatlan-ságának biztosításához az átlagosnál magasabb szakértelemre is szüksége lehet,
- a kutatás és lefoglalás során a szakértő igénybevétele a nyomok rögzítésénél hasznos lehet,
- a tiszta, világos megfogalmazás,
- a bíróság előtt sokszor nagyobb érvényt lehet szerezni a vádnak.

A szakértő kirendelése ellen szóló érvek:

- a nem alapos vagy nem érthető szakértői vélemény nehezítheti a nyomozást, vagy nem megfelelő bizonyítékot eredményezhet,
- esetlegesen a szakértő elfogulatlansága megkérdőjelezhető,
- a szakértés elvégzésére nyitva álló határidő – a 60 + 30 nap – egyes esetekben hosszú, indokolatlanul késlekedhet annak befejezésével,
- sokszor indokolatlanul magas a szakértő díjazása,
- a hatóság nem mindig szakkérdésben veszi igénybe, sokkal inkább az általános ismeretek hiánya miatt.

A szakértő alkalmazása kirendeléssel – határozattal – történik, amelyben többek között meg kell jelölni

- a) a szakértői vizsgálat tárgyát és azokat a kérdéseket, amelyekre a szakértőnek választ kell adnia,
- b) a szakértő részére átadandó iratokat és tárgyakat, ha az átadás nem lehetséges, az iratok és a tárgyak megtekintésének helyét és idejét,
- c) a szakvélemény előterjesztésének határidejét (2016. évi XXIX. tv. 45. §).

Ha a szakvélemény elkészítéséhez sürgős részvizsgálatra van szükség, e vizsgálat kirendelő határozat nélkül, az ügyész vagy a nyomozó hatóság szóbeli rendelkezése alapján is elvégezhető.⁴² A szakértő a szakvéleményét két hónapon belül kell, hogy előterjessze. Ez a határidő a szakértő kérelmére egyszer, legfeljebb egy hónappal hosszabbítható. Az eljárási törvény szerint általában egy szakértőt kell alkalmazni egy eljárásban az adott szakkérdésben. Ha a vizsgálat jellege szükségessé teszi, több szakértő is kirendelhető. Ez úgy is történhet, hogy a kirendelés csak a szakértői csoport vezetőjét jelöli ki, és feljogosítja őt arra, hogy a többi szakértőt bevonja. A köztudomású tények meghatározása egyébként szubjektív jellegű a kiberbűncselekmények nyomozása során, hiszen az informatika sok esetben speciális szakértelmet igényelhet, illetve a nyelvezete (általában angol) miatt, az informatikai eszközök gyors változása és sajnos sokszor az életkori sajátosságokból kifolyólag előfordulhat, hogy az ügyészség vagy a bíróság rendel majd ki szakértőt, amennyiben ezek miatt a nyomozás irataiban, a jelentésben, a jegyzőkönyvben foglaltak nem érthetők vagy értelmezhetők.

8.2.28. A szakértő kirendelésének lehetősége

A bíróság, az ügyész, illetőleg a nyomozó hatóság a szakértői névjegyzékben szereplő igazságügyi szakértőt, illetőleg szakvélemény adására feljogosított gazdasági társaságot

⁴² Be. 189. § (1)–(2) bekezdés.

(a továbbiakban: gazdasági társaság), szakértői intézményt vagy külön jogszabályban meghatározott állami szervet, intézményt, szervezetet (a továbbiakban: szervezet), ha ez nem lehetséges, kellő szakértelemmel rendelkező személyt vagy intézményt (a továbbiakban: eseti szakértő) rendelhet ki szakértőként. A témában végzett vizsgálataim során feltett kérdésekre adott válaszok alapján a rendőrségnél a következő általános gyakorlatokról szereztem tudomást: a bűnügyi állomány tekintetében a házkutatás és lefoglalás eljárása a bűncselekmények típusától függ. Amennyiben feltehetőleg elektronikus adat kerül lefoglalásra, úgy egy CD-t, DVD-t, esetleg külső merevlemezt visznek magukkal, amelyre a vizsgálni kívánt adatokat kimentik. A saját maguk által vitt eszközöket lefoglalják a büntetőeljárási törvényben előírtaknak megfelelően, majd ezt követően szakértőt rendelnek ki, akinek feladata az adathordozó átvizsgálása, a kirendelő határozatban feltett kérdések megválaszolása. Ugyanakkor, amennyiben nagyobb adat lefoglalása és vizsgálata válik szükségessé, úgy az egész számítógép, illetve informatikai eszköz lefoglalása mellett szoktak dönteni. Arra a kérdésre, hogy milyen módon hozzák el a számítógépeket, informatikai eszközöket, megkapó válasz született: az áramforrásból és a hálózathoz eltávolítják, majd ezt követően valamennyi ki- és bemeneti egységet leragasztják, és a rendeletnek megfelelően bűnjelezik, majd szállítják be a kapitányságra vagy közvetlenül az igazságügyi informatikai szakértőhöz. A lefoglalás tekintetében nincs protokoll, hanem az ügy előadója sokszor saját elgondolása szerint dönt arról, hogy kell-e, mikor, és milyen módon történjen meg annak végrehajtása. Az egyenruhás – azaz közrendvédelmi állomány – tekintetében sem sokkal jobb a helyzet. Általában nem fordítanak gondot az oktatásukra, képzésükre. A legmeglepőbb dolog, hogy régi megszokott módszerrel „vizsgálják” meg egy talált vagy igazoltatás során gyanússá vált mobiltelefont: a *#06# kombinációk leütésével a telekommunikációs eszköz IMEI-számát ismerik meg. Arra a kérdésre, hogy mi a helyzet azokkal az eszközökkel, amelyek jelszóval vagy ujjlennyomattal védettek, nem tudtak válaszolni. A mérlegelés, illetve annak lehetősége, hogy a fent említett kombinációval esetleg bizonyítékokat semmisíthetnek meg, fel sem merült.

8.2.29. A szakértő és a szaktanácsadó

Az elmúlt időszakban nem volt jellemző, hogy a kirendelt szakértő túlterjeszkedett volna a kompetenciáján. Ugyanakkor az ügyészségek általában megengedhetőnek tartják, ha a nyomozó hatóság tagja a kirendelő határozatban arra kéri a szakértőt, hogy a bűncselekménnyel kapcsolatban keressen adatokat, ugyanis ez már a saját kompetenciáján, feladatán történő túlterjeszkedés. Az ügyészségen elfogadhatónak ítélik meg, ha bizonyos esetekben az ügyben eljáró hatóság végzi el az adatállomány elemzését, értékelését, de ők sem tudták meghatározni, hogy pontosan milyen kérdésnél húzható meg a határ. A helyszínen igénybe vett szakértő vagy szaktanácsadó feladata, a számítógép átvizsgálása a hatóság irányítása alatt nélkülözhetetlen lehet. Ugyanakkor, ahogy a táblázatban is megtekinthető, az informatikai szakértők is specializálódnak, így amennyiben nem a szakterületének megfelelő területről ad ki szakvéleményt, úgy az a bizonyítékok értékelésénél nem vehető figyelembe. Ugyanúgy aggályos, ha a szakértő nemcsak az adatok átvizsgálását végzi el, hanem egyes esetekben kijelenti, hogy annak tartalma alapján milyen bűncselekmény elkövetése állapítható meg.