DOI: 10.38146/BSZ.2018.7-8.6

NAGY RICHÁRD

A kibertérben elkövetett vagyon elleni bűncselekmények nyomozásának egyes kérdései

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

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

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

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

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

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

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

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

A kiberbűncselekmények fogalmi megközelítése

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

A budapesti egyezmény a bűncselekményeket a következők szerint csoportosítja:

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

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

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

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

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

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

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

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

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

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

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

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

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

A bűncselekmények minősítése

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

9 BH 2015.244.

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

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

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

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

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

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

11 BH 2017.252.

12 Sinku Pál: i. m. 164. o.

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

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

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

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

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

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

Az elsődleges nyomozási cselekmények

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

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

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

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

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

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

Joghatóság, hatáskör, illetékesség

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

15 Goricsán Tamás Károly: A kényszerintézkedések végrehajtásának sajátosságai a számítástechnikai eszközök felhasználásával megvalósított bűncselekmények nyomozása körében. In: Gál István – Nagy András Zoltán (szerk.): i. m. 72. o.

16 Dornfeld László: A kibertérben elkövetett bűncselekményekkel összefüggésben alkalmazható kényszerintézkedések. Belügyi Szemle, 2018/2., 119–120. o.

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

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

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

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

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

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

17 BH 2011.332.

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

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

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

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

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

IRODALOM

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

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

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

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

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

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

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

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

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