6. A kiberbűncselekmények statisztikai rögzítettsége

Simon Béla

Első kérdésként felmerül, hogy voltaképpen mit is érthetünk kriminálstatisztikai megközelítésből kiberbűncselekménynek. Ha a Büntető Törvénykönyvben található kategóriákat vesszük sorra, szinte minden bűncselekmény kapcsolható lehet a kibertérhez. Valójában alig van olyan tényállás, amelyet ne lehetne infokommunikációs eszközzel elkövethetőnek tekinteni. Esetünkben azon deviáns viselkedések sorolhatók a kiberbűncselekmények körébe, amelyek eredményüket és normasértő jellegüket tekintve nagyon gyakran érintik a kiberteret, vagy e tér nélkül kevésbé valósulhatnának meg (lásd: *A kiberdevianciák színtérmódozatai* 3. fejezet). A kiberbűncselekmények kriminálstatisztikai besorolása esetében is fontos a társadalomra való veszélyesség, amely például egy emberi testet ért támadás esetén viszonylag egyértelműen meghatározható súlyosságú, szemben a kibertérben elkövetett jogsértésekkel, ahol az effajta cselekvések nem ennyire egyértelműen skálázhatók. Az etikus hackerek tevékenysége és jogi megítélése erre kiváló példa. Lehetséges, hogy a rövid távú jogsértések hosszabb távon össztársadalmilag nagyobb közjót eredményeznek. Az eddig leírtakból látható, hogy a bűnözés pontos meghatározása e területen akadályokba ütközik, de ha elvonatkoztatunk attól a problémától, hogy a kibertérhez kapcsolódó bűncselekmények megállapíthatóságának kritériuma képlékeny, és csak azt vesszük figyelembe, hogy mi az, amit Magyarország statisztikai rendszere e bűncselekményi körhöz regisztrált, akkor azt gondolhatnánk, hogy könnyen tudunk trendvonalakat felmutatni az elmúlt időszakra. A *kiberbűnözés* kifejezés egy másik oldalával is érdemes foglalkoznunk. A kibertérre vonatkozóan találunk definíciós meghatározást, amit kötetünk elején részletesen is kifejtettünk.[1] Mennyiben része e kibertér fizikai összetevőinek a hálózati eszközök, szoftverek összessége? Mit értünk a kibertér virtuális összetevői alatt? Részét képezik-e az internethez nem kapcsolódó hálózatok? Számos kérdés merül fel, amelynek kimunkálása nem e fejezet célja (Munk 2018). Esetünkben a kiberteret érintő bűncselekményeket a gyakorlati megfontolásokat alkalmazó szervezetek – különösen az Europol – gyakorlata alapján tarjuk célszerűen besorolhatónak. Az Europol az általa lényegesnek tartott bűncselekményeket, a nemzetközi bűnügyi együttműködést segítő eljárásokat elemző projektekben (*analysis project,* AP; korábban *analysis work file,* AWF) kezeli. Itt a vagyonvisszaszerzéstől az egyes kábítószerfajtákon át számos projekt él – jelenleg 28 darab. Egy ilyen elemző projektnek külön „kezelőszemélyzete" van, akik a beérkező adatokat elemzik, értékelik, és az eredményeiket az érintett hatóságok támogatására megküldik. Az Europol Kiberbűnözési Kompetenciaközpontja (EC3) három ilyen AP-t kezel:

[1] Lásd: 1. fejezet.

https://doi.org/10.36250/00782_06

- *AP Cyborg:* támogatja az EU-ban a kritikus számítógépes és hálózati infrastruktúrákat érintő számítógépes bűnözés elleni vizsgálatokat.
- *AP Terminal:* a nemzetközi elektronikus és online fizetési csalások felderítésén dolgoznak.
- *AP Twins:* elemzési projekt, támogatja a gyermekek szexuális kizsákmányolásával és visszaélésekkel járó bűnözés minden formájának megelőzését és leküzdését.

Az Europol más szervei által kiberbűnözéshez kapcsolódóan kezelt AP-k:

- *AP Copy:* támogatja a szellemi tulajdonjogokkal kapcsolatos bűncselekmények megelőzését és az azok elleni küzdelmet.
- *AP Check-the-Web:*[2] a nyílt internetforrások figyelemmel kísérése és értékelése az iszlamista terrorizmus ellen.
- *AP Apate:* különféle csalási cselekményekkel szembeni fellépés (jellemzően online csalások) (SIMON 2018).

Tehát azt jelenthetjük ki, hogy ezekhez a kiberbűncselekményi kategóriákhoz kapcsolódóan egyértelműen besorolhatók a magyar bűnügyi statisztika által jelölt tényállások, amelyekből következtetéseket vonhatunk le. Sajnos azonban ez nem így van. A Bűnügyi Statisztikai Rendszer[3] adataiból nem különíthetők el a kérdéses kategóriák.

7. táblázat

A kibertérhez köthető bűncselekmények alakulása a 2013–2018. év első féléve közötti időintervallumban

Büntetőjogi kategória	2013	2014	2015	2016	2017	2018. I–VI. hó
Gyermekpornográfia	5225♦	142	334	272	1439▪	146
Készpénz-helyettesítő fizetési eszköz hamisításának elősegítése	3	1	3	3	1	4
Készpénz-helyettesítő fizetési eszközzel való visszaélés	5804	1186	870	23 064•	434	218
Készpénz-helyettesítő fizetési eszköz hamisítása	65	202	130	425	739	1432
Információs rendszer felhasználásával elkövetett csalás, (5) bekezdés (nincs elkülönítés a statisztikában)	250	1398	2176	3409	4467	1876

Megjegyzések:
♦ Ebből Nógrád megye: 4892.
▪ Ebből Heves megye: 1153.
• Ebből Pest megye: 22 687.

Forrás: BSR 2018

[2] AP Check-the-Web. Forrás: www.register.consilium.europa.eu/doc/srv?l=EN&f=ST%208457%202007%20REV%202 (A letöltés dátuma: 2018. 10. 30.)

[3] Bűnügyi Statisztikai Rendszer. Forrás: www.bsr.bm.hu/SitePages/Nyitolap.aspx (a letöltés dátuma: 2018. 10. 30.), https://bsr.bm.hu/Document (A letöltés dátuma: 2018. 10. 30.)

A gyermekpornográfia bűncselekmény esetszáma nagy mozgásokat mutat. E bűncselekmény esetében a legnagyobb kiugrásokat 2013-ban és 2017-ben egy-egy ügycsoport eredményezte. Ezekben az esetekben nem a sértettek számához igazodott a rendbeliség, hanem az eljárás során biztosított felvételek számához, amely egy helytelen gyakorlat. A bankkártyához kapcsolódó visszaélések közül a *készpénz-helyettesítő fizetési eszközzel visszaélés folyamatosan csökkent az elmúlt öt évben, kivétel a 2016-os évet.* A BSR-rendszerben nincs lehetőség az információs rendszer felhasználásával elkövetett csalás (5) bekezdésében rögzített minősítést (elektronikus készpénz-helyettesítő fizetési eszköz felhasználásával) külön kezelni a többi tényállástól. Így összességében kijelenthetjük, hogy e tényállás erőteljes emelkedést mutat az elmúlt évekre – akár a bankkártyával, akár más módon történő elkövetésnél is (7. táblázat).

8. táblázat

A klasszikus kiberbűncselekmények alakulása a 2013–2018 első féléve közötti időintervallumban

Büntetőjogi kategória	2013	2014	2015	2016	2017	2018. I–VI. hó
Személyes adattal való visszaélés	2635	1059	975	487	722	530
Közérdekű üzem működésének megzavarása	73	66	34	40	38	31
Tiltott adatszerzés	20	31	23	20	16	6
Információs rendszer vagy adat megsértése	823	565	520	702	586	345
Információs rendszer védelmét biztosító technikai intézkedés kijátszása	580	31	15	44	8	5
Csalás	37 345	33 362	31 976	43 383	22 197	12 884

Forrás: BSR 2018

A kibertérben elkövethető bűncselekmények körében az elmúlt 5 évben jelentős csökkenés látható. A statisztikai adatok közé sorolható még a *nemzeti adatvagyon körébe tartozó állami nyilvántartás elleni bűncselekmény,* ami a hatálybalépése óta nem valósult meg, valamint a *jogosulatlan titkos információgyűjtés vagy adatszerzés,* ami 2 esetben valósult meg 2013 óta. Ezekben az esetekben nem beszélhetünk bűnelkövetői mintázatokról és trendekről sem. A kriminálstatisztikai adatok alapján 2013 óta 17 darab terrorcselekményt regisztráltak, de ezek közül nem állapítható meg, hogy mely esetekben volt érintett a kibertér. A csalás jellegű magatartások esetében a statisztika a 2017. év májusát megelőző időszakra vonatkozóan nem tartalmaz pontos információkat – azok együtt szerepelnek az összes csalással. Ezek az adatok azért különösen érdekesek, mivel az interneten elkövetett csalás jellegű cselekmények túlnyomó többsége helyes minősítés esetén e tényállásban jelenik meg (8. táblázat). Annak további vizsgálata indokolt, hogy a hatalmas statisztikai kiugrásokat okozó ügyekben mi okozta az éves országos összes esetszámot sokszorosan meghaladó bűncselekményszám előfordulását. Ezek nyilvánvalóan nem a társadalmi viszonyokat követő és bemutató statisztikai eredmények, sokkal inkább a statisztikai rendszer hibás működése valószínűsíthető mögötte. A bűnügyi statisztikai adatokból tehát nem látható egyértelműen

a kiberbűncselekmények hagyományos bűncselekményektől elválasztható struktúrája és dinamikája. E statisztikai probléma nemcsak Magyarországon jelentkezik, hanem azt Európa számos országában észlelte a GENVAL-jelentés (Simon 2018). Ennek orvoslására 2017 májusában a Bűnügyi Statisztikai Rendszerben bevezetésre került egy plusz kérdés: Az adott bűncselekményt online környezetben követték el? Ennek éves eredményeit még nem ismerjük, de az eddigi gyakorlat azt mutatja, hogy az összesítés sok fals-pozitív elemet is tartalmazni fog. A híradásokon túlmenően azonban más forrásból is az lehet a feltételezésünk, hogy a kiberbűncselekmények fenyegetése jelentős. Egyes szakértői vélemények szerint a kiberbűnözés globális és éves szinten 1200 milliárd USD kárt okozott 2017-ben (Frész 2017). E kijelentéseket jellemzően olyan személyek teszik, akiknek érdekében áll a problémák démonizálása. Azonban nyilvánvalóan egy információbiztonsággal foglalkozó vállalkozástól sem várható el, hogy megnyugtató nyilatkozatot tegyenek a várható trendekre vonatkozóan. Az elmúlt időszakban inkább az jellemző, hogy e nyilatkozatok gyakrabban jelennek meg a médiafigyelem homlokterében.