DOI: 10.38146/BSZ.2023.10.3

CC BY NC ND

Tiltott adatszerzés és az információs rendszer elleni bűncselekmények sajátosságai Magyarországon 2013–2021 között[1]

Characteristics of Illicit Access to Data and Crimes against Information Systems in Hungary between 2013 and 2021

Deres Petronella
Dr. PhD, tudományos főmunkatárs
Országos Kriminológiai Intézet,
Büntető Jogtudományok Osztálya
deres@okri.hu

Absztrakt

Cél: A tanulmány célja az Országos Kriminológiai Intézetben elvégzett kutatás során megvizsgált – a Btk. XLIII. fejezetébe sorolt tényállások alapján indult – büntetőeljárások hazai jellemzőit vázolni.
Módszertan: A tanulmány az adatfelvétel, az adatelemzés és a bűnügyi iratelemzés módszertanának alkalmazásával készült.
Megállapítások: A hazai szabályozási környezet megfelelően lefedi a kibertámadások széles körét. A magyarországi jellemzők a kiberbiztonság és kiberbűnözés aktuális nemzetközi, európai fejleményeinek tágabb perspektívájában vizsgálhatók. Az adatokból megfigyelhető, hogy bár nem egyenletesen, de folyamatosan nő az ilyen bűncselekmények miatt tett feljelentések száma, hiszen egyre többen használnak a mindennapi életvitelük során különböző információs rendszereket úgy, hogy a biztonságos használatukkal kapcsolatos intézkedéseket részben vagy egészben mellőzik. Az országos vizsgálat konklúziója, hogy több, alapvetően jól körülhatárolható típusú cselekmény azonosítható. A jogalkalmazók számára kihívást jelenthet az új elkövetési módok nyomon követése, illetve az egyes elkövetési magatartások minősítése.
Érték: Következtetések és javaslatok megfogalmazása a Btk. XLIII. fejezetében foglalt bűncselekmények sajátosságaival kapcsolatban; az új kódex

1 Köszönetet szeretnék mondani valamennyi főügyészség és járási ügyészség vezetőjének és kollégáiknak, hogy a kutatás során az empirikus vizsgálat lebonyolítását lehetővé tették. Külön köszönettel tartozom azon főügyészségeknek, akik a konzultációk során megosztották megyei szintű tapasztalataikat; ezen belül is kiemelten a Szabolcs-Szatmár-Bereg, a Borsod-Abaúj-Zemplén és a Csongrád-Csanád Vármegyei Főügyészségeknek.

hatálybalépése óta Magyarországon nem zajlott a témakörre vonatkozó ilyen ívű és tartalmú, bűnügyi iratelemzést is magában foglaló kutatás.
Kulcsszavak: kiberbűnözés, tiltott adatszerzés, információs rendszer elleni bűncselekmények, bűnügyi iratelemzés

Abstract

Aim: The aim of the study is to present the results of the research carried out by the National Institute of Criminology on the implementation of the Criminal Code. Chapter XLIII of the Criminal Procedure Code was conducted by the National Institute of Criminology.
Methodology: The study was conducted using the methodology of data collection, data analysis, criminal file analysis.
Findings: The domestic regulatory environment adequately covers a wide range of cyber-attacks. Hungarian characteristics can be seen in the broader perspective of current international and European developments in cyber security and cybercrime. The data show a steady but not uniform increase in the number of reports of such crimes, as more and more people use various information systems in their daily lives, while neglecting, in whole or in part, measures to ensure their safe use. The conclusion of the national survey is that there are several types of offences which are basically well defined. It may be a challenge for law enforcement to keep track of new types of offences and to classify individual offences.
Value: Conclusions and recommendations on the specifics of the offences covered by Chapter XLIII of the BPC; the (new) Criminal Code since its entry into force, there has been no research of this scope and content on the topic, including criminal document analysis, in Hungary.

Keywords: cybercrime, illicit access to data, crimes against information systems, criminal file analysis

Bevezetés

Hatályos magyar büntetőkódexünk (a továbbiakban: Btk.) – a budapesti egyezmény[2] előírásainak megfelelően – XLIII. fejezetében önállóan rendeli büntetni a tiltott adatszerzés és az információs rendszer elleni bűncselekményeket (422–424. §) *„arra figyelemmel, hogy e tényállások egységesen meghatározható jogi tárgya az információs rendszerek megfelelő működtetéséhez és az abban foglalt*

2 Az Európa Tanács Budapesten, 2001. november 23-án kelt számítástechnikai bűnözésről szóló egyezménye.

adatok megőrzéséhez fűződő társadalmi érdek védelme" (Belovics, 2021). Ezen kívül más fejezeteiben is rendelkezik olyan tényállásokról, amelyeknek egyes elkövetési magatartásai a kiberbűnözés körébe is sorolhatók.[3]

Az informatikai rendszereket érintő egyes bűncselekmények számát tekintve az utóbbi években Magyarországon is emelkedés tapasztalható (Lajtár, 2019).

A kutatásról

Az Országos Kriminológiai Intézetben 2021–2022-ben végeztem kutatást a kibertérrel összefüggő bűncselekmények témakörében.

A kiberbiztonság és a kiberbűnözés hazai jellemzői (Deres, 2023) az aktuális nemzetközi, európai fejlemények tágabb perspektívájában mutatkoznak meg, így kutatásomban az Európai Bizottság biztonsági unióra vonatkozó új stratégiája alapján meghatározott legújabb irányvonalak mentén áttekintettem a pandémiás időszak főbb mérföldköveit a kiberbűnözés elleni küzdelem terén. *„A digitális kor technológiai, technikai és szolgáltatásforradalma miatt a digitalizáció megállíthatatlanul áthatja a digitális társadalom egészét"* (Jobbágy, 2022).

Megjegyzendő, hogy a digitális transzformációval kapcsolatos egyes kérdések megközelítése az Atlanti-óceán két partján eltérő eredők mentén alakult (Szecsi, 2021). Az Európai Unió 2022–2025 közötti időszakra elfogadott bűnüldözési prioritásaira is fókuszáltam, amelyek egyértelműen alátámasztják azt a megállapítást, hogy a kiberbűnözés a bűnözés szinte valamennyi ágensét áthatja.

A kutatásban ezen túl a Btk. XLIII. fejezetébe sorolt bűncselekmények sajátosságait elemeztem. Tanulmányomban az empirikus vizsgálat eredményeiről adok rövid áttekintést.

A kutatás empirikus szakaszának célja az volt, hogy képet adjon a Btk.

- 422. §-ában foglalt tiltott adatszerzés [és a bűncselekmény 2018. január 1-jén hatályba lépett új alapesete (422/A. §)];
- 423. §-ában foglalt információs rendszer vagy adat megsértése; és a
- 424. §-ában foglalt információs rendszer védelmét biztosító technikai intézkedés kijátszása

bűncselekmények 2013–2021 közötti időszakáról, jellemzőiről, az ezen tényállások alapján indult eljárásokról, különös figyelemmel a minősítési kérdésekre és a nyomozás eredményességét befolyásoló körülményekre, a nyomozás során felmerülő problematikákra fókuszálva.

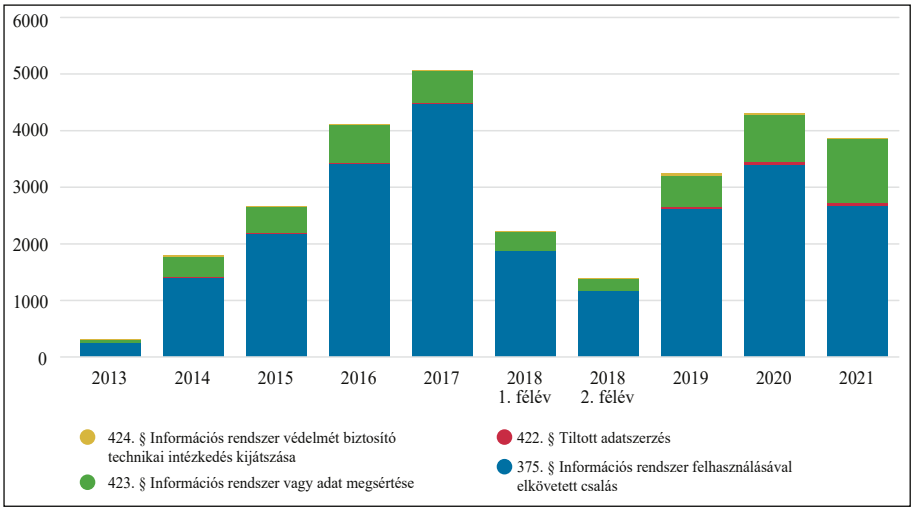
3 Lásd például a 375. szakaszt; továbbá az informatikai/számítástechnikai/infokommunikációs eszközök igénybevételével (is) elkövethető bűncselekményeket (zaklatás, gyermekpornográfia, kábítószer-kereskedelem stb.).

Közel 500 bűnügyi irat[4] – az új Btk. hatálybalépése és a 2021. december 31. közötti időszakban indult és jogerős bírói ítélettel vagy végzéssel lezárult ügyek – alapján értékeltem és elemeztem a hazai kiberbűnözés egy „szeletét"; a Btk. XLIII. fejezetébe sorolt tényállások joggyakorlatban jelentkező jellegzetességeit. Az adatgyűjtés szempontjai között szerepeltek egyrészt a cselekmények megismerését lehetővé tévő jellemzők (úgymint az elkövetések tárgya, módja, az elkövetők, a passzív alanyok, illetve sértettek jellemzői stb.), másrészt az eljárások felderítésének, bizonyításának és megítélésének sajátosságai.[5]

Bár az adat-, illetve az érdemi elemzés tárgya a Btk. XLIII. fejezetébe sorolt tényállásokra szűkült (a 422/A. § ügyében indult eljárás – a vizsgálat meghatározott paramétereinek keretében – nem volt), az adatelemzés során ugyanakkor a Btk. 375. §-ában foglalt információs rendszer felhasználásával elkövetett csalásra vonatkozó adatokat, azok szignifikánsan kiemelkedő volumenére figyelemmel, a diagramos kimutatásban feltüntettem (1. számú ábra).[6]

1. számú ábra

A Btk. XLIII. fejezetébe, valamint a 375. § alá sorolt bűncselekmények gyakorisága



Forrás: Egységes Nyomozóhatósági és Ügyészségi Bűnügyi Statisztika (ENyÜBS).

4 A Legfőbb Ügyészség Informatikai Főosztálya által megküldött VIR-adatok alapján a főügyészségek által megküldött (időközben jogerőre emelkedett) ügyekkel együtt mindösszesen 462 bűnügyi irat elemzését végeztem el.

5 Az értékeléshez kidolgozott adatlap 45 pontban, több mint 100 alpont segítségével ügyenként (ezen belül elkövetőként) rögzíti az elkövetőre, a sértettre, a bűncselekményre, az eljárásra és a jogkövetkezményekre vonatkozó adatokat.

6 A statisztikai adatok legyűjtését Koplányi Gergely segítségével végeztem.

A vizsgált bűncselekmények gyakoriságát tekintve a vizsgált időszakban:
- 229 tiltott adatszerzés bűncselekményét;
- 5153 információs rendszer vagy adat megsértése bűncselekményét;
- 151 információs rendszer védelmét biztosító technikai intézkedés bűncselekményét regisztrálták Magyarországon.

A bűncselekmények megyei megoszlásában az látható, hogy
- a Btk. 422. §-át tekintve a legtöbb megyében tíz alatti az előfordulások száma;
- a Btk 423. § vonatkozásában a közel kilencéves terminusban Budapest (1261), Pest megye (582) és Győr-Moson-Sopron megye (410) szignifikánsan kiemelkedik a megyék közül; a többi megyében – Nógrád megye (63) kivételével – száz fölötti számadatokat látunk;
- a Btk 424. §-át szemügyre véve, Budapest és Csongrád-Csanád megye van az élvonalban, e két megye számadatai adják az ügyek közel felét.

Az empirikus kutatás tárgyát képező jogerős ügyek legnagyobb hányadát a Btk. 423. §-ába ütköző információs rendszer vagy adat megsértésének bűncselekménye teszi ki, míg a 422. és a 424. §-okba foglalt tényállások kisebb számban fordulnak elő.

Az adatokból megfigyelhető, hogy nem egyenletesen, de folyamatosan nő az ilyen bűncselekmények miatt tett feljelentések száma, hiszen a mindennapi életvitelük során egyre többen használnak különböző információs rendszereket (levelezőprogramok, közösségi oldalak stb.) úgy, hogy a biztonságos használatukkal kapcsolatos intézkedéseket részben vagy egészben mellőzik.

Következtetések

Az országos vizsgálat konklúziója szerint több, alapvetően jól körülhatárolható típusú cselekménykategória azonosítható.

Tiltott adatszerzés

A Btk. 422. §-ában foglalt tiltott adatszerzés vonatkozásában a cselekmények jelentősebb részét hozzátartozók vagy volt hozzátartozók, barátok sérelmére elkövetett bűncselekmények miatt tett feljelentések teszik ki. A leggyakoribb tényállás a más lakásában, egyéb helyiségében történtek technikai eszközzel történő megfigyelése, de előfordult kémprogram telepítése is. Itt említenénk, hogy az adatvédelmi kérdések tengerentúli anomáliáiról izgalmas összehasonlító elemzést olvashatunk a *The Texas Lawbook* hasábjain (Szecsi & George, 2023).

Az ügyek egy részében egymás közelségében élő személyek tettek feljelentést amiatt, hogy a szomszédos ház biztonsági kameráin keresztül megfigyelik őket. Ezekben az ügyekben a nyomozó hatóság a feljelentéseket rendszerint elutasítja, vagy az eljárást megszünteti, tekintettel arra, hogy sem a bűncselekmény elkövetéséhez megkívánt célzat, sem pedig az elkövetési mód nem állapítható meg.

A Kúria a Bfv.III.299/2017. számú jelentős ügyben a járásbíróság marasztaló végzését felülvizsgálati eljárás keretében megváltoztatta, és a terheltet az ellene emelt vád alól felmentette.

A Zalaegerszegi Járási Ügyészség ügyében az irányadó tényállás lényege szerint a terhelt 2015. március 26-án a munkahelyére egy kft. épületébe bevitt egy kamerát, amelyet a női WC-ben rejtett el az ajtó fölött lévő lámpabúra mellé. Ezzel az volt a célja, hogy a mellékhelyiség használata közben intim helyzetben megfigyelje a kolléganőit. A vádlott a jogosulatlanul megszerzett és megismert személyes adatokat, esetleges magántitkokat saját célra akarta felhasználni, a kamera által készített felvételeket stresszoldás gyanánt akarta nézegetni. A kamera 10 óra és 12 óra 45 perc között üzemelt, majd egy női munkatárs észlelte és levette. A kamera adattovábbításra nem volt alkalmas, az észlelésig három munkatársról készített felvételt, azokat azonban a terhelt már nem tudta megnézni.

A terheltet a járásbíróság tárgyalás mellőzésével hozott jogerős végzésével a Btk. 422. § (1) bekezdés b) pontjába ütköző tiltott adatszerzés bűntette miatt egy év hat hónap időtartamra próbára bocsátotta. A jogerős ítélet ellen a Legfőbb Ügyészség a Be. 416. § (1) bekezdés a) pontjára hivatkozással a terhelt javára, a tiltott adatszerzés bűntette miatt emelt vád alóli felmentés érdekében nyújtott be felülvizsgálati indítványt.

A magántitok jogosulatlan megismerése bűntett tárgyában egységes volt az a joggyakorlat, hogy a bűncselekményt csak magánlakásban lehetett elkövetni (BH2014.134., Fővárosi ítélőtábla 3.BÍ.98/2012/6.).

Figyelemmel arra, hogy a Btk. módosításakor csak a jogosulatlanul megszerezhető titokkör kibővítésére került sor, az elkövetési magatartások, illetve elkövetési tárgyak szélesítésére nem, a joggyakorlat megváltoztatására nem volt jogszabályi alap.

A Kúria megállapította, hogy a felülvizsgálati indítvány alapos. A terhelt maradéktalanul megvalósította az adott bűncselekmény elkövetési magatartását, vagyis a tárgyi oldal szükséges eleme tényállásszerű, viszont az elkövetés helye tekintetében nem, ezért bűncselekmény megállapítására sem kerülhet sor.

Megjegyzendő, hogy a Btk. 2018. január 1-jén hatályba lépett módosítása szerint megállapított új alapeset [422. § (1a)] alapján azonban az ilyen helyszínen megvalósított elkövetési magatartás (azóta) már tényállásszerű.

Több ügyészség gyakorlatában felmerült a bűncselekmény rendbeliségének problematikája (lásd például Budapesti IX. kerületi Főügyészség Gazdasági

Bűnügyek Részlege egyik ügyében a másodfokú bíróság megállapította, hogy a bűncselekmény rendbelisége nem a sértettek számához igazodik, hanem annyi rendbeli, ahány magánlakást az elkövető átkutat, megfigyel, az ott történteket rögzíti, függetlenül attól, hogy hány személy titkának megismerésére törekszik).

A vizsgált tényállás és egyéb bűncselekmények vonatkozásában felmerült halmazati kérdéseket illusztrálja az alábbi jogeset.

A Debreceni Járási Ügyészség ügyében a vádlott informatikus foglalkozású, büntetlen előéletű. A vádlott és a sértett baráti kapcsolatban állt egymással.

2017. évben sértett megkérte vádlottat arra, hogy a Samsung márkájú notebookját javítsa meg. A vádlott a notebook javítása során a notebookon található tartalmakat, köztük a sértettről készült fényképfelvételeket lementette. A fényképfelvételek között több szexuális tartalmú erotikus beállítású kép is megtalálható volt, amelyeket vagy maga a sértett készített, vagy az ő hozzájárulásával készültek saját használatra. A letöltött képeket egy Micro SD kártyán tárolta.

A tartalommásoláshoz a sértett engedélyt nem adott, arról a későbbiekben a vádlott sem tájékoztatta.

2019. évben a vádlott megharagudott a sértettre, ezért a sértett nevén a Facebook közösségi portálon egy profilt hozott létre, amely oldalra a korábban jogosulatlanul megszerzett képekből 16 erotikus tartalmú képet feltöltött. A profilról ismerősnek jelölte a sértett édesanyját, édesapját és élettársát, akik előtt így megnyílt a lehetőség a feltöltött képek megtekintésére. A profilt a sértett édesanyja látta először, aki szólt a sértettnek és élettársának, így azt valamennyien megtekintve, a Facebook irányába jelzéssel éltek az álprofil törlése érdekében, ami meg is történt.

Az ügyben személyes adattal visszaélés miatt indult a büntetőeljárás.

A nyomozás során az ügyészség átiratában észrevételezte, hogy a terhelt cselekménye személyes adattal visszaélés vétségével halmazatban a Btk. 422. § (1) bekezdés e) pontja szerint minősülő és büntetendő tiltott adatszerzés bűntettét is megvalósított. Ezen cselekménye 2017. évben azzal valósult meg, hogy a sértett notebookján lévő fényképeket lementette. A bíróság tárgyalás mellőzésével a vádlottal szemben – a váddal egyezően – egyrendbeli, a Btk. 422. § (1) bekezdés e), és egyrendbeli, a Btk. 219. § (1) bekezdés a) pontjának megsértése miatt 280 óra közérdekű munka büntetést szabott ki.

Információs rendszer vagy adat megsértése

A Btk. 423. §-ában foglalt információs rendszer vagy adat megsértése miatt indult ügyekben jellemzően abból az okból tesznek feljelentést, hogy a sértett által használt levelezőrendszerbe, közösségi oldalhoz tartozó fiókba valaki – többnyire

a sértett által ismert, vele haragos viszonyban lévő személy (hozzátartozó, volt házastárs/élettárs, jelenlegi vagy volt munkavállaló, ismerős stb.) – belépett, ott módosításokat hajtott végre, üzenetet küldött, a hozzáférést a jelszó megváltoztatásával lehetetlenné tette, vagy az ott tárolt adatokat megismerte. Az elkövetést legtöbbször személyes ok motiválja: féltékenység, bosszú, harag, szexuális motiváció, de előfordult fiatalkori „csínytevés" is. Az ilyen személyes motivációból elkövetett – különösen a közösségi oldalakat érintő – cselekmények a sértettek számára különösen nagy pszichés terhet jelentenek. A sértő/ártó bejegyzések, tartalmak nemcsak a magánéletüket befolyásolhatják, hanem a társadalmi státuszukat – leginkább a munkahelyi viszonyaikat – is érinthetik, különösen a kisebb településeken történő elkövetéseknél.

Vádemelésre ilyen ügyekben legtöbbször akkor kerül sor, ha az elkövető büntetett előéletű vagy a bűncselekményt más bűncselekménnyel halmazatban követte el, egyéb esetekben az ügyészség elterelést (vádemelés elhalasztása, feltételes ügyészi felfüggesztés) alkalmaz.

Egyes esetekben más bűncselekményekhez kötődik az elkövetés: viszonylag nagy számban kapcsolódik vagyon elleni bűncselekményekhez, illetve a zaklatás tényállásához; előbbieket illetően legtöbbször az alapcselekmények leplezése ilyenkor a kiberbűncselekményt (is) elkövető célja (például lopott gépjármű elektronikájában adatváltoztatás az alvázszám átírásával).

A modern gépjárművekre elkövetett lopás bűncselekményéhez szintén kapcsolódik e tényállás, hiszen az ilyen autók rendszere informatikai rendszer, így ismert elkövető esetén szakértői vélemény alapján pontosan meg lehet állapítani, hogy mely módszerrel történt a gépjármű kinyitása vagy a motor beindítása.

A 423. §-sal kapcsolatban a vizsgált tényállásokkal „együttálló" becsület csorbítására alkalmas cselekmények megítélését illetően az úgynevezett „Facebookos" eseteknél – olykor az úgynevezett „bosszúpornó" (revenge porn) esetkörének megvalósulásával – a becsület csorbítására alkalmas cselekmények értékelése több ízben elmarad (mivel az elkövető képfelvételeket hoz nyilvánosságra, adott esetben a nagy nyilvánosság előtti elkövetés is megállapítható, avagy privát üzenetváltás szövegét teszi közzé a sértett nevében becsületcsorbítására alkalmas tényt állító bejegyzéssel). A képmáshoz való jog büntetőjogi védelme (lásd erről Gál & Szomora, 2016; EBH 2013.B.21.) aktuális szabályozásának áttekintése a jelen kutatásban vizsgált tényállások kontextusában külön értékelés tárgyát képezheti, ezzel összefüggésben szükségesnek mutatkozhat az ultima ratio és az arányosság elvével való összhang elemzésére is figyelmet fordítani, különös tekintettel a nagy nyilvánosság előtti elkövetés, a jelentős érdeksérelem (219. §, 226. §, 422. §) és a becsület csorbítására alkalmas tényre elkövetett magatartások értékelésére.

A 423. §-sal kapcsolatban az alábbi kérdéskörök érdemelnek még kiemelést.

A) Az egyik esetben a büntetőjogi felelősség megállapíthatósága körében alapvető jelentőséggel bírt az úgynevezett „etikus hacking” és a büntetőjogi normába ütköző, büntetőjogilag szankcionálandó magatartás elhatárolása (lásd erről még Mezei, 2020).

A vád rövid történeti tényállása szerint a vádlott a Magyar Telekom Nyrt. rendszergazda munkatársainak adatait felhasználva belépett az Nyrt. authentikációs feladatokat ellátó, úgynevezett LDAP szerverére, ahol jogosulatlanul saját felhasználói profilokat hozott létre és adatokat gyűjtött. A védelem az eljárás során hivatkozott arra, hogy a vádlott cselekményének társadalomra veszélyességében tévedett, hiszen felvette a kapcsolatot a sértetti társaság illetékeseivel, és tájékoztatást is adott a rendszer sérülékenységéről, azaz etikus hackinget végzett, amely magatartás nem járhat büntetőjogi felelősségre vonással.

A bizonyítási eljárás azonban egyértelművé tette, hogy a vádlott kifejezett sértetti tiltás ellenére is folytatta tevékenységét, így ezen a ponton túl a bíróság sem látta elfogadhatónak az etikus hackingre vonatkozó hivatkozást.

A vádhatóság közérdekű üzemre elkövetett információs rendszer megsértésének bűntettével vádolta a terheltet, amely minősített eset megállapítására a bíróság nem látott lehetőséget.

Az ügyben sor került igazságügyi informatikus szakértő kirendelésére is, többek között annak tisztázása érdekében, hogy az LDAP szerver pontosan milyen szerepet tölt be az elektronikus hírközlő hálózatban. A szakértői vélemény megállapításaiból ugyanakkor a bíróság és az ügyészség eltérő következtetéseket vont le.

Az ügyészség álláspontja szerint a módosított vádirati tényállásból egyértelműen megállapítható a közérdekű üzemre való elkövetés, még akkor is, ha az LDAP szerver nem működik közre közvetlenül a jelek továbbításában.

A bíróság ezzel szemben a Btk. utaló rendelkezéséből kiindulva úgy foglalt állást, hogy a támadott szerver nem feleltethető meg az Eht. 188. § 19. pontjában meghatározott elektronikus hírközlő hálózat, azaz a Btk. értelmezésében a közérdekű üzem fogalmának.

A Szolnoki Járásbíróság ítélete ügyészi fellebbezést követően másodfokon emelkedett jogerőre.

Kiemelésre méltó továbbá a „BKK-etikus hacker” néven elhíresült ügy.

Az elkövető számítógépes ismereteit felhasználva a frissen meginduló online jegy- és bérletvásárlást lehetővé tévő rendszerben hibát tapasztalt, amit kihasználva a tényleges ártól olcsóbban, 50 forintért tudott bérletet vásárolni. Ezt a hibát az elkövető a BKK részére jelezte, majd a hibát a nyilvánosság elé is tárta. A tevékenység – a Legfőbb Ügyészség álláspontjára is figyelemmel – azért

volt etikusnak tekinthető, mert nem okozott több kárt, a hibát azonnal feltárta, mindvégig transzparensen végezte a tevékenységét, hiszen saját azonosító adatait és bankkártyáját használta. Erre tekintettel a társadalomra veszélyesség hiánya okán került megszüntetésre a büntetőeljárás.

B) Több esetben DDoS túlterheléses támadás és kibertámadással összefüggő szolgáltatás nyújtása (cybercrime-as-a-service) volt az ügy tárgya.

Konkrét esetben az első- és másodrendű vádlottak által indított kibertámadások eredményeként nem volt megállapítható, hogy a megtámadott IP-címeken lévő alkalmazások vagy rendszerek nem lassultak le, nem váltak elérhetetlenné és nem „omlottak" össze.

Az illetékes járásbíróság jogerős ítéletében mindkét vádlottat folytatólagosan elkövetett információs rendszer megsértése bűntettének kísérletében [Btk. 423. § (2) bekezdés a) pont I. fordulata] mondta ki bűnösnek.

C) Ide sorolhatóak azok az esetek is, amelyekben a hivatalos személy elkövető más (az elkövető munkatársa) érvényes felhasználói azonosítójával és jelszavával, például a RobotZsaru-rendszerbe vagy más hivatali információs rendszerbe jogosulatlanul bejelentkezett, ott adatokat törölt, illetve módosított [423. § (2) a) és b) pontok].

Információs rendszer védelmét biztosító technikai intézkedés kijátszása

A 424. §-ában foglalt információs rendszer védelmét biztosító technikai intézkedés kijátszása az információs rendszer vagy adat megsértéséhez, valamint az információs rendszer felhasználásával elkövetett csaláshoz kapcsolódó sui generis előkészületi deliktum, az ügyészségek gyakorlatában a legkisebb számban fordul elő (2021-ben 15 ügyet regisztráltak).

Valamennyi tényállás szempontjából jellemző, hogy a bíróság a bűncselekményt beismerő vádlottakkal szemben tárgyalás mellőzésével (büntetővégzésben) hoz érdemi döntést, valamint általánosnak mondható a bíróság elé állítás jogintézményének alkalmazása is. A kiszabott szankciók súlyossága a cselekmény tárgyi súlya mellett az elkövető személyi körülményeitől függ; a beismerő, büntetlen előéletű terheltekkel szemben a bíróság jellemzően próbára bocsátás intézkedést alkalmaz.

A nyomozás során felmerült tapasztalatok alapján megfogalmazott észrevételek

Végezetül néhány egyéb észrevétel a nyomozás eredményességét befolyásoló körülmények, a nyomozás során felmerülő problematikák körében.

1) A kutatás tárgyát képező bűncselekményi körben a legfőbb nehézséget a használt eszközök, programok elkövetőhöz kötése jelenti. A napi jogalkalmazás során a legtöbb gyakorlati probléma a hálózati kapcsolatokhoz tartozó előfizetők és az egyes előfizetések tényleges használójának megállapítása körében merül fel.
2) Az elkövető azonosítására a sértett által szolgáltatott adatokból vagy az internetes kommunikáció során használt azonosítókból (IP-címek, MAC-cím) lehet eredményesen következtetést levonni.
3) Több megyében (például Borsod-Abaúj-Zemplén, Hajdú-Bihar, Somogy) is jellemző az információs rendszer vagy adat megsértésének az az esetköre, amikor az elkövetési magatartás a sértettek e-mail címéhez tartozó felhasználói fiókjába, közösségi oldalon (Facebook, Twitter, WhatsApp stb.) regisztrált profiljába, vagy egyéb internetes platformon regisztrált felhasználói fiókjába történő belépés, abban történő adatváltoztatás vagy adattörlés, illetőleg jelszó megváltoztatásával az adott felhasználói fiók hozzáférhetetlenné tétele (személyes indíttatásból, féltékenység, bosszú stb. miatt). Ilyen esetben indokolt a kommunikációs szolgáltatók megkeresése a használt IP-címek tekintetében. Bevett eljárásjogi gyakorlat, hogy önkéntes adatszolgáltatás keretében külföldi tartalomszolgáltatók is megkeresésre kerülnek, akik az úgynevezett forgalmi adatokat az esetek nagy részében közlik (regisztráció során/korábbi belépéseknél/jelszóváltoztatásnál használt IP-címek). Előfordul, hogy a regisztráció során megadott egyéb adatokat is közölnek a szolgáltatók (telefonszám, bankszámlaszám is rendelkezésre állhat).
4) Ide kapcsolódóan sajátos problémakört jelent a legelterjedtebb közösségi oldalak, tartalomszolgáltatók (Facebook, Google) amerikai egyesült államokbeli honossága.
5) A felderítés tekintetében további nehézséget jelentenek az internetszolgáltatók által egyre többet használt, úgynevezett NAT-olt, vagy más néven címfordítással alkalmazott hálózati kapcsolatok felépítése. E technológia alkalmazása a még jelenleg is túlnyomórészt használt IPv4-címek korlátozott száma miatt szükséges.
6) Az IP-cím azonosítása után magának a tényleges felhasználónak az azonosítása is problémákba ütközhet, hiszen egy internet-előfizetés mögött ma már jellemzően több tényleges felhasználó is használja ugyanazt a végpontot, mely túlnyomórészt vezeték nélküli útválasztóval kerül megosztásra, de lehetséges az is, hogy nagyobb felhasználói kört kiszolgáló munkahelyi végponthoz vagy nyilvános internetelérési ponthoz vezethető vissza az adott IP-cím. Ezen lokális hálózatok mögött a forgalmi adatok naplózására

vagy nem kerül sor, vagy olyan rövid ideig, ami nem teszi lehetővé a ténylegesen használt eszköz azonosítását.

7) Problémát jelent, hogy sokszor az elkövetők, a sértettek, az adatok és a bűnözői infrastruktúra részei különböző országokban találhatók, ami joghatósági kérdést vet fel: melyik ország jogosult eljárni az ügyben, és mely ország jogrendszere szerint?

8) A menetíró készülék manipulálásával kapcsolatos ügyekben – ahol a tehergépjárművek menetíró készülékeinek manipulálásával (mágnes- vagy más személy aláíró kártyájának igénybevételével) követték el a bűncselekményt – az ügyek egy részének elhúzódásához az vezet, hogy az elkövetők külföldi állampolgárok, akiknek a cselekményét Magyarországon mint tranzitországon történő keresztülutazásuk során észlelik. A nyelvi nehézségek okán és a külföldre történő kézbesítés kapcsán többször szükséges fordító és tolmács igénybevétele.

9) Egyes megyék tapasztalatai szerint a Magyarországon foganatosítható eljárási cselekmények után a külföldi szervek megkeresése ritkán jár eredménnyel: több esetben az elkövetési magatartás kifejtése és a célzott rendszer helye eltér egymástól, országokat, akár földrészeket átívelve, így a bizonyítékokat külföldről kell beszerezni, ami hosszadalmas, nehézkes, a jogsegélyek eredményessége igen változó.

   A külföldi hatóságokkal való jó együttműködésre példa többek között a Szombathelyi Járási Ügyészség ügye, amelyben a nyomozás elrendelésére a holland hatóságok által az Europol SIENA rendszerén keresztül megküldött információk alapján került sor. Az ügyben úgynevezett elosztott szolgáltatásmegtagadással járó túlterheléses támadás (DDoS) elkövetése miatt került sor – feltételes ügyészi felfüggesztés keretében – a büntetőjogi felelősség megállapítására.

10) Kibertérrel összefüggő (de nem a kutatásban vizsgált bűncselekményi körben) bűncselekmény nyomozása során szerzett pozitív tapasztalat volt, hogy a külföldi sértett Magyarországon megbízott a képviseletével egy ügyvédi irodát, amely a kapcsolatfelvételt és a szükséges bizonyítékok beszerzését megkönnyítette és meggyorsította.

11) Kiemelést érdemel végül az Egri Járási és Nyomozó Ügyészség ügye, amelyben magas szintű informatikai ismeretekkel rendelkező terhelt tagadta a bűncselekmény elkövetését, többirányú védekezést terjesztve elő. Ezért a bűnösségének bizonyítása mind a nyomozati, mind a bírósági eljárásban nehézségekbe ütközött, de az eljárás a vádlott elítélésével ért véget [Btk. 423. § (2) bekezdés b) pontjába ütköző és aszerint minősülő információs rendszer vagy adat megsértésének bűntette].

Összegzés

A hazai szabályozási környezet megfelelően lefedi a kibertámadások széles körét, a jogalkalmazók számára kihívást jelenthet az új elkövetési módoknak a nyomon követése, az egyes elkövetési magatartások minősítése.

A 21. század globális kihívásaira figyelemmel *„[N]em becsülhető alá egy megfelelő időben megalkotott, kellően megfontolt olyan tagállami megoldás, amely egyszerre van tekintettel a hazai jogrendszer koherenciájára és teszi lehetővé a nemzetközi és uniós vívmányok alkalmazását, ezáltal is integrálódva egy komplex eszközrendszerbe”* (Polt, 2022).

Különösen fontos, hogy a jogalkalmazók is megismerhessék az informatikai bűnözéssel kapcsolatos legújabb trendeket, aktuális, naprakész ismereteket szerezzenek (az ügyészségen belül lásd többek között: Számítógépes Bűnözéssel Foglalkozó Országos Ügyészségi Hálózat, a Fővárosi Főügyészségen Európában másodikként felállított kiberkontaktpontok intézménye, majd annak tapasztalatai nyomán az egész ügyészi szervezetre történő elrendelése).

Az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) 2020 áprilisában közzétett dokumentumának (URL1) célja a számítógépbiztonsági incidenskezelő csoportok és a bűnüldöző, igazságszolgáltatási szervek közötti együttműködés, valamint az igazságszolgáltatással való együttműködésük támogatása a kiberbűnözés elleni küzdelemben; szervezeti, jogi, technikai és kulturális együttműködési perspektívákról való tájékoztatással, valamint az aktuális hiányosságok azonosításával és az együttműködés további fokozására vonatkozó ajánlások megfogalmazásával.

Álláspontom szerint ennek mentén hazánkban megfontolásra javasolható egy olyan (multidiszciplináris) platform létrehozása, amely lehetővé teszi, hogy a számítógépbiztonsági incidenskezelő csoportok a büntetőeljárásokban részt vevő mindhárom állami szerv (nyomozó hatóság, ügyészség, bíróság) közös részvételével valósítsanak meg képzést, szakmai tréninget a vonatkozó – kiberbűncselekmények, kiberbiztonság, új, aktuális fenyegetettségek, kihívások, várható tendenciák – területen.

Felhasznált irodalom

Belovics E. (Szerk.) (2021). *Büntetőjog II. Különös Rész*. HVG-Orac.

Deres P. (2023). A kibertérrel összefüggő bűncselekmények sajátosságai Magyarországon. *Ügyészek Lapja, 30*(1), 75–79. https://ugyeszeklapja.hu/?p=4096

Gál A. & Szomora Zs. (2016). A képmáshoz való jog fragmentáris büntetőjogi védelme. In Gellén K. & Görög M. (Szerk.), *Lege et fide. Ünnepi tanulmányok Szabó Imre 65. születésnapjára* (pp. 133–145). Iusperitus.

Jobbágy Sz. (2022). Metaverzum, a virtuális univerzum, világunk digitális kivetülése. Utópia vagy kézzelfogható valóság a digitális jövőben? *Hadtudományi Szemle, 15*(2), 131–160. https://doi.org/10.32563/hsz.2022.2.8

Lajtár I. (2019). A kiberbűnözésről. *Ügyészek Lapja*, *26*(1), 47–52. http://ugyeszeklapja.hu/?p=774

Mezei K. (2020). A jogosulatlan belépés, avagy a hacking szabályozása a büntetőjogban. *Rendőrségi Tanulmányok, 3*(2), 23–43. https://bm-tt.hu/rtt/wp-content/uploads/2022/08/2020_2_mezei_kittti.pdf

Polt P. (2022). A 21. század kihívásainak hatása a büntetőeljárásra. Kriptovaluták, azaz az új vagyoni értékek büntetőjogi kérdései. *Kriminológiai Tanulmányok, 59*(2ksz), 6–17.

Szecsi, G. (2021). How to Ensure National Security in the New Media Age. *Transatlantic Antitrust and IPR Developments, 1,* 50–55. https://law.stanford.edu/wp-content/uploads/2015/04/2021-1.pdf

Szecsi, G. & George, G. (2023). *Which State Leads the Way? A Comparison of Data Privacy. Laws in Texas and California.* https://texaslawbook.net/which-state-leads-the-way-a-comparison-of-data-privacy-laws-in-texas-and-california/

A cikkben található online hivatkozás

URL1: *An overview on enhancing technical cooperation between CSIRTs and LE.* https://www.enisa.europa.eu/publications/support-the-fight-against-cybercrime-tools-for-enhancing-cooperation-between-csirts-and-le/@@download/fullReport

Alkalmazott jogszabályok

2012. évi C. törvény a Büntető Törvénykönyvről

2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről

2003. évi C. törvény az elektronikus hírközlésről

A cikk APA szabály szerinti hivatkozása

Deres P. (2023). Tiltott adatszerzés és az információs rendszer elleni bűncselekmények sajátosságai Magyarországon 2013–2021 között. *Belügyi Szemle*, *71*(10), 1729–1742. https://doi.org/10.38146/BSZ.2023.10.3