JOGI FÓRUM PUBLIKÁCIÓ

www.jogiforum.hu

Az információs rendszerek elleni bűncselekmények uniós szintű szabályozása, különös tekintettel az Európai Unió 2013/40/EU sz. Irányelvére

Szerző:

dr. Mezei Kitti

2015. június 14.

Az információs rendszerek nincsenek tekintettel az országhatárokra, a hálózatok révén az összekapcsolt információs rendszerek adatállományához távolról is hozzá lehet férni. Az információs technológia rohamosan fejlődik és ennek következtében új bűnelkövetési formák jelennek meg, így az információs rendszerek felhasználásával elkövetett bűncselekmények száma is fokozatosan növekszik évről évre, és emiatt különösen fontos, hogy a jogalkotók is gyors ütemben tudjanak válaszolni ezekre a változásokra. A hatékony fellépés ezzel a bűncselekmény típussal szemben megköveteli a nemzetközi bűnügyi együttműködést, illetve a büntetőjogszabályoknak a nemzetközi összehangolását, a szükséges minimumszabályoknak a megalkotását. Uniós szinten a minimumszabályokat az új *2013/40/EU Irányelv* határozza meg az információs rendszer elleni támadások tekintetében. Mielőtt az új irányelvvel részletesen foglalkoznék, a korábbi uniós szabályozást ismertetném.

Az első fontos nemzetközi jogi dokumentum az OECD 1986-ban kibocsátott jelentése volt, amelyben iránymutatást kívántak adni a számítógépes környezetben elkövetett bűncselekmények megismeréséhez és a kodifikáció elősegítése volt a cél.

Az első uniós dokumentum *az Európai Tanács 9 (89). számú Ajánlása* (Computer-Related Crime), amely tartalmaz egy minimum listát. Ez a lista iránymutatásul szolgál a tagállamok jogalkotói számára, amennyiben ilyen típusú bűncselekmény esetében új jogszabályokat hoznak, vagy a régiek kerülnek átalakításra, akkor abban az esetben kötelezve vannak arra, hogy az ajánlással összhangban járjanak el.

A minimumlista a következőket tartalmazza:

- a számítógépes csalás,
- a számítógépes hamisítás,
- a számítógépes adatokban és programokban történő károkozás,
- a számítógépes szabotázs,

- a jogellenes behatolás: a számítógépes rendszerbe vagy hálózatba történő jogosulatlan bejutás a biztonsági intézkedések megsértése révén,
- a jogellenes titokszerzés,
- védett számítógépes programok jogellenes másolása.

Továbbá tartalmaz egy fakultatív listát is, amelynek az elemei pedig a következőek:

- A számítógépes adatok és/ vagy programok megváltoztatása
- A számítógépes kémkedés
- A számítógép jogellenes használata
- Védett programok jogellenes használata.

Az *ET. 95. (13.) számú Ajánlása* pedig az információs technológiákkal kapcsolatos büntető eljárási problémákra törekedett megoldást találni.

A 2001 novemberében Budapesten aláírt *„Számítástechnikai Bűnözésről Szóló egyezmény”* (Convention on Cyber-crime) az ajánlásokhoz képest továbblépést jelentett és újabb jogi normákat fogalmazott meg.

- A számítógépes technikai fogalmakat definiálja és ezáltal egységes értelmezést nyújt (számítógépes rendszer, számítógépes adat, internetes szolgáltató, átmenő adat).
- Mind az anyagi és eljárásjogi szabályozást tartalmazza.
- Az anyagi jogban a bűncselekménytípusok köre kibővült és újabb jogsértési típusok jelennek meg (pl. gyermekpornográfiával kapcsolatos bűncselekmények).

A bűncselekménytípusokat logikusan csoportokba rendezi (A számítástechnikai rendszer és a számítástechnikai adatok hozzáférhetősége, sértetlensége és titkossága elleni bűncselekmények; A számítástechnikai bűncselekmények; A számítástechnikai adatok tartalmával kapcsolatos bűncselekmények).

Az Egyezményt a 2004. évi LXXIX. törvénnyel hirdették ki Magyarországon, és ezzel összhangban a Btk.-ba a 300/C. § a Számítástechnikai rendszer és adatok elleni bűncselekmény tényállását felvette, valamint egyéb más törvényi tényállásokat kiegészített a meghatározottak szerint.

Ugyanebben az évben *az Európai Tanács 2001/413/IB kerethatározata* került elfogadásra a nem készpénzes fizetőeszközökkel összefüggő csalás és hamisítás elleni küzdelemről.[1]

2002-ben jelent meg *az „Elektronikus hírközlési adatvédelmi Irányelv"*, amely tartalmazza az alapvető szabályokat, amelyek célja, hogy biztosítsa a felhasználóknak az elektronikus hírközlési és technológiai szolgáltatások iránti bizalmát. Ezek a szabályok különösen a „spamek" betiltására, a felhasználó előzetes beleegyezését kérő (opt-in) rendszerre és a cookie-k telepítésére vonatkoznak. Ez az irányelv 2011-ben egészült ki az ún. „cookie" irányelvvel", amely alapján a viselkedésalapú reklám célba juttatásához használt cookie-k kizárólag az érintettek hozzájárulását követően helyezhetők el a felhasználók számítógépein.[2]

Az Európai Tanács 2004/97/EK határozattal létrehozták *az Európai Hálózat- és Információbiztonsági Ügynökséget (ENISA),* amely az Unió, a tagállamok, a magánszektor és az európai polgárok szolgálatában álló hálózat- és információbiztonsági szakértői központ. Jelenleg az 526/2013/EU rendelet szabályozza a szervezet működését.

2005-ben pedig az információs rendszerek elleni támadásokról szóló *2005/222/IB tanácsi kerethatározat* elfogadására került sor,[3] amelynek a célja számítógépes bűnözés elleni küzdelem és az információbiztonság előmozdítása. A transznacionális bűnözés ezen új formáját tekintve a kerethatározat fő célja az igazságügyi és egyéb illetékes hatóságok közötti együttműködés javítása az információs rendszerek elleni támadások területére vonatkozó büntetőjogi szabályok közelítése

1 http://www.rendeszetelmelet.hu/Graphics/pdf/Nagy_Zoltan_Andras_A_2013_40_es_Unios_direktiva.pdf http://www.pecshor.hu/periodika/XIII/gyaraki.pdf, 237-239. oldal

2 http://adatvedelmiaudit.hu/2011/06/cookie-k-csak-hozzajarulassal/

3 http://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX:32005F0222

által a következő területeken: információs rendszerekhez való jogsértő hozzáférés, rendszerekbe való jogsértő beavatkozás, adatokba való jogsértő beavatkozás. Ezen bűncselekményeknek szándékosnak kell lenniük, illetve bármelyikre való felbujtás, azokban való bűnrészesség, valamint bűnpártolás, illetve az elkövetésükre irányuló kísérlet is büntetendő. A tagállamoknak rendelkezniük kell arról, hogy ezeket a bűncselekményeket hatékony, arányos és visszatartó erejű büntetőjogi szankciókkal sújtsák. Súlyosbító körülménynek minősül, ha egy bűncselekményt szerint bűnszervezetben követték el, illetve az súlyos kárt vagy alapvető érdeksérelmet okozott. Másfelől az illetékes igazságügyi hatóság enyhébb szankciót is alkalmazhat, amennyiben a bűncselekmény csupán csekély kárt okozott. A kerethatározat a jogi személyek felelősségének megállapítására vonatkozóan is javasol kritériumokat, és meghatározza a felelősségük megállapítása esetén kivethető szankciókat. A kerethatározat fogalommeghatározásokat tartalmaz (pl.: információs rendszer, számítógépes adatok, jogi személy illetve a jogosulatlanul fogalmát). A kerethatározatnak megfelelően vette át a magyar szabályozás is az információs rendszer szóhasználatát a bűncselekményeknél.

Az Európai Unióról szóló és az Európai Unió működéséről szóló szerződés 83. cikk (1) bekezdése pedig kimondja, hogy:

„Az Európai Parlament és a Tanács rendes jogalkotási eljárás keretében elfogadott irányelvekben szabályozási minimumokat állapíthat meg a bűncselekményi tényállások és a büntetési tételek meghatározására vonatkozóan az olyan különösen súlyos bűncselekmények esetében, amelyek jellegüknél vagy hatásuknál fogva a több államra kiterjedő vonatkozásúak, illetve amelyek esetében különösen szükséges, hogy az ellenük folytatott küzdelem közös alapokon nyugodjék. Ezek a bűncselekményi területek a következők: terrorizmus, emberkereskedelem és a nők és gyermekek szexuális kizsákmányolása, tiltott kábítószer-kereskedelem, tiltott fegyverkereskedelem, pénzmosás, korrupció, pénz és egyéb fizetőeszközök hamisítása, *számítógépes bűnözés* és szervezett bűnözés.”

Erre tekintettel „A polgárokat szolgáló és védő, nyitott és biztonságos Európa” című 2010-ben kiadott a tamperei és hágai programot követő *ún. stockholmi program* az Európát érintő jövőbeli kihívások között említi a számítógépes bűnözést.

2011-ben *az Európa Parlament és Tanács 2011/92/EU számmal Irányelvet* fogadott el a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről. Ezzel összefüggésben 2012-ben kezdetét vette egy nemzetközi összefogás „Globális szövetség a gyermekek online szexuális kizsákmányolása ellen”, amelyhez az uniós országokon kívül más országok is csatlakoztak.

2013. január 11-től kezdte meg működését *a számítástechnikai bűnözés elleni európai központ (EC3)*, amely az európai polgárok és vállalkozások számítástechnikai bűnözéssel szembeni védelméhez nyújt segítséget. A központot az Európai Rendőrségi Hivatal (Europol) hágai székhelyén hozták létre. A számítástechnikai bűnözés elleni központ megnyitása fontos változást jelez a számítástechnikai bűnözés uniós kezelési módjában. Először is, a központ hosszú távon és átfogó módon gondolkodik. Egybegyűjti a szaktudást és az információkat, támogatja a bűnügyi nyomozásokat és elősegíti az egész Unióra kiterjedő megoldásokat. [4]

2013 augusztusában az Európa Parlament és Tanács *2013/40/EU számmal Irányelvet*[5] fogadott az információs rendszerek elleni támadásokról, amely a 2005/222/IB kerethatározat váltotta fel:

„Ezen irányelv célja, hogy a bűncselekmények tényállására és vonatkozó szankcióikra vonatkozó minimumszabályok megállapítása révén közelítse a tagállamok büntetőjogát az információs rendszerek elleni támadások terén, és hogy javítsa a tagállamok illetékes hatóságai, így a rendőrség és az egyéb bűnüldözési szakszolgálatok, valamint az Unió illetékes szakosított ügynökségei és szervei – például az Eurojust, az Europol és annak a számítástechnikai bűnözés elleni európai központja, valamint az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) – közötti

4 http://europa.eu/rapid/press-release_IP-13-13_hu.htm

5 http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv:OJ.L_.2013.218.01.0008.01.HUN

együttműködést.” Ez az irányelv megállapítja az információs rendszerek elleni támadások terén elkövetett bűncselekmények és szankciók meghatározására vonatkozó minimumszabályokat:

A közös fogalommeghatározások fontosságát hangsúlyozza ki, hasonlóan, mint a korábbi kerethatározat (információs rendszer, számítógépes adatok, jogi személy és jogosulatlanul).

A tagállamoknak közös megközelítést kell kialakítaniuk a bűncselekmények tényállás elemeire vonatkozóan az információs rendszerhez való jogosulatlan hozzáférés, illetve az adatokat érintő jogellenes beavatkozás, valamint a jogellenes adatszerzés egységes bevezetése révén „Adatszerzés különösen a kommunikáció tartalmának lehallgatása, ellenőrzése vagy figyelemmel kísérése és az adattartalmak közvetlenül, az információs rendszerhez való hozzáférés és az információs rendszer használata által történő, vagy közvetetten, elektronikus megfigyelő vagy lehallgató eszközök révén történő megszerzése.”. Továbbá a tagállamoknak a legalább a súlyosabb esetekben bűncselekménynek kell minősíteniük azokat az eseteket, amikor az irányelvben foglalt bűncselekmények elkövetéséhez felhasználnak eszközöket (pl.: számítógépes programok készítése, belépési kódok, jelszavak felhasználása az információs rendszerhez való hozzáféréshez).

Valamennyi az irányelvben foglalt bűncselekményre való felbujtás illetve az elkövetéshez nyújtott bűnsegélynek bűncselekménynek kell minősülnie. Az adatot érintő jogellenes beavatkozás és jogellenes adatszerzés esetében pedig a kísérlet is büntetendő.

Azonban az irányelv nem állapít meg büntetőjogi felelősséget abban az esetben, ha az ezen irányelvben felsorolt bűncselekmények objektív kritériumai teljesülnek, azonban a cselekményeket nem jogsértő szándékkal követték el (pl.: az adott személynek nincs tudomása arról, hogy az adott hozzáférés jogosulatlan).

A tagállamoknak hatékony, arányos és visszatartó erejű szankciókat kell alkalmazniuk, és szabadságvesztést és/vagy pénzbüntetést is magukban kell foglalniuk.

Súlyosabb szankció megállapításának van helye, ha az információs rendszer elleni támadást bűnszervezetben követik el, vagy ha a támadás átfogó, azaz jelentős számú információs rendszert érint vagy súlyos kárt okoz, abban az esetben is, ha a támadás valamely tagállam vagy az Unió kritikus infrastruktúrája ellen irányul. A tagállamoknak a jogrendszerük által a súlyosító körülményekre vonatkozóan megállapított szabályokkal összhangban súlyosító körülményeket kell meghatározniuk a nemzeti jogukban. De lege ferenda szükségesnek mutatkozik például a magyar szabályozásra nézve, hogy a minősített eseteket bővítse a szervezett bűnözés keretében.

Az informatikai támadásokat számos körülmény megkönnyítheti, például ha az elkövetőnek alkalmazotti minőségében hozzáférése van az érintett információs rendszerek részét képező biztonsági rendszerekhez. A magyar jognak szintén feladatot tűz ki ezzel az irányelv, mert a jelenlegi szabályozás nincs tekintettel az alkalmazottak általi elkövetésre.

Továbbá az irányelv felhívja a figyelmet a személyazonosság-lopás illetve a személyazonossághoz kapcsolódó egyéb bűncselekmények elleni hatékony fellépés relevanciájára, a magyar büntetőtörvénykönyvben szükséges lenne a jövőben ennek a bűncselekménytípusnak a szankcionálása.

A hatékony prevenció érdekében a hatóságoknak együtt kell működniük a magánszférával és a civil társadalommal (pl.: ez kiterjedhet a szolgáltatók általi a potenciális bizonyíték megőrzésére, együttműködési és partnerségi hálózat kiépítésére a szolgáltatókkal és a gyártókkal).

A jogi személyek felelősségét és a velük szemben alkalmazandó szankciókat a kerethatározathoz hasonlóan tartalmazza. Továbbá a joghatósági kérdésekre is választ ad. A hatékony fellépés érdekében a tagállamok gondoskodnak saját operatív nemzeti kapcsolattartó pontjuk létrehozásáról, és arról, hogy igénybe veszik a meglévő, a hét minden napján 24 órában rendelkezésre álló operatív kapcsolattartó hálózatot. A tagállamok olyan eljárások működését is biztosítják, amelyek révén sürgős segítségkérés esetén az illetékes hatóság a kézhezvételtől számított 8 órán belül jelezheti legalább azt, hogy teljesíti-e a segítségkérést, valamint hogy ezt milyen formában és várhatóan mikor teszi. Továbbá tagállamoknak biztosítani kell egy olyan

rendszer meglétét, amely rögzíti, előállítja és rendelkezésre bocsátja ezekre a bűncselekményekre vonatkozó statisztikai adatokat.

Az irányelvet a tagállamoknak 2015. szeptember 4-ig kell implementálniuk a nemzeti jogba.

A 2012. évi C. Büntetőtörvénykönyvünk a következő bűncselekményeket rendeli büntetni, amelyek az információs rendszereket érintik: a vagyon elleni bűncselekmények között az információs rendszer felhasználásával elkövetett csalás (375.§), illetve külön csoportot képez a tiltott adatszerzés és az információs rendszer elleni bűncselekmények (422-424.§), amelyekhez tartozik értelemszerűen a tiltott adatszerzés, információs rendszer vagy adat megsértése, illetve az információs rendszer védelmét biztosító technikai intézkedés.

Konklúzióként pedig az új irányelvből idéznék, amely úgy gondolom, hogy összefoglalja és kihangsúlyozza a lényeget: „Az információs rendszerek a politikai, a társadalmi és a gazdasági interakció kulcstényezői az Unióban. A társadalom nagy- és egyre növekvő mértékben függ e rendszerektől. E rendszerek zökkenőmentes működése és biztonsága az Unióban létfontosságú a belső piac és a versenyképes és innovatív gazdaság fejlődése szempontjából. Az információs rendszerek megfelelő szintű védelmének biztosítása részét kell, hogy képezze a számítástechnikai bűnözésre adott büntetőjogi válaszokat kísérő megelőző intézkedések hatékony és átfogó keretének.” Továbbá fontos, hogy uniós és a tagállami szinten is a büntető anyagi és eljárásjogi szabályozás lépést tartson az informatikai bűnözés fejlődésével, amely a jogi szabályozás számára folyamatos kihívást jelent, és ezért szükségesek, hogy ezekre a változásokra megfelelő eszközökkel tudjanak válaszolni a jogalkotók.