HADMÉRNÖK

XII. Évfolyam 1. szám – 2017. március

EGYSÉGES EURÓPAI KIBERTÉR? AZ EURÓPAI UNIÓ KIBERBIZTONSÁGI POLITIKÁJÁNAK FEJLŐDÉSE

SINGLE EUROPEAN CYBERSPACE? THE DEVEOPMENT OF THE EUROPEAN UNION'S CYBER SECURITY POLICY

MOLNÁR Dóra

(ORCID: 0000-0002-1476-5253)

molnar.dora@uni-nke.hu

Absztrakt

A kiberbiztonság a biztonság nagyon dinamikusan fejlődő olyan új területe, amely egyre veszélyesebb fenyegetéseket rejt magában. Ezidáig csak az egyes nemzetállamok próbálták meg saját kiber infrastruktúrájukat megvédeni – több-kevesebb sikerrel –, egységes, európai szintű szabályozás nem létezett. A tanulmány felvázolja, hogy az elmúlt évtizedben az Európai Unió milyen lépéseket tett a kiberbiztonsági szabályrendszer és az egységes európai digitális piac megteremtése terén, és röviden ismerteti a 2016-ban elfogadott két legfontosabb jogforrást, az adatvédelmi rendeletet és a hálózatbiztonsági irányelvet. Ezek előremutató lépések ugyan, de valójában a stratégiák és a szabályozók gyakorlati megvalósulása fogja tudni igazolni, hogy e lépések elegendőek-e ahhoz, hogy az Unió sikeresen meg tudjon birkózni a kibertérben jelentkező egyre nagyobb számú és egyre súlyosabb fenyegetéssel.

"A tanulmány a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés" elnevezésű kiemelt projekt keretében működtetett Egyed István Posztdoktori Program keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült."

Kulcsszavak: *kiberbiztonság, Európai Unió, adatvédelem*

Abstract

Cybersecurity is a very dynamic new sector of security that involves more and more dangerous threats. So far only national states themselves tried to protect their own cyber infrastructure – with more or less success –, a single, Europe-wide regulation has not existed. The study outlines what steps the European Union has taken in the creation of regulations and of a single European digital market in the past decade and briefly describes the two most important sources of law adopted in 2016, the General Data Protection Regulation and the NIS directive. Although, these are steps forward, but only practical implementation of strategies and sources of law will be able to verify if these measures are sufficient enough for the European Union to successfully cope with the growing number of more and more serious cyber threats.

„The work was created in commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled „Public Service Development Establishing Good Governance" in (the) István Egyed Postdoctoral Program."

Keywords: *cyber security, European Union, data protection*

A kézirat benyújtásának dátuma (Date of the submission): 2017.01.31.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.02.30.

BEVEZETÉS

Az elmúlt évben számos olyan fejlemény következett be, amelyek az európai kiberbiztonságot új alapokra helyezték. Talán a 2016-os év volt az, amikorra az Európai Unió felkészültté vált arra, hogy tagállamai kezébe olyan iránymutatásokat legyen képes adni, amelyek segítségével mind a tagállamok önállóan, mind pedig az Unió mint egész képes a kibertérben jelentkező fenyegetések hatékony kezelésére.

A tanulmány célja az, hogy felvázolja az európai szabályrendszer legfontosabb pilléreit, amelyek kijelölik a tagállami kötelezettségeket és mozgásteret saját kiberbiztonságuk megteremtéséhez. Terjedelmi korlátok miatt kizárólag az Európai Unió keretei között megalkotott jogforrásokat mutatom be és elemzem, a többi szervezet szabályrendszerével egy későbbi részben foglalkozok.

TÁRSADALMI HÁTTÉR

Az Európai Unió és az uniós polgárok egyre növekvő mértékben vannak kitéve a kibertérből származó fenyegetéseknek. Ráadásul, egyre gyakrabban válnak a térség és polgárai kiszemelt célponttá, köszönhetően többek között annak, hogy ez európai számítógépes infrastruktúra igen fejlett, a számítógépes hálózatok valamennyi szektort átszövik, az azokon tárolt adatok köre és mennyisége fokozatosan növekszik, mindez pedig vonzó terepet kínál a számítógépes bűnözőknek. Ezért *egyre fontosabbá és sürgetőbbé válik egy összehangolt, komplex európai szabályrendszer megalkotása*, amely a gyakorlatban kész szcenáriókat kínál az államoknak mind a kibertámadások megelőzéséhez, mind pedig a bekövetkezett akciók következményeinek hatékony és gyors kezeléséhez. Államok elszigetelt, önálló szabályrendszerének megalkotása már nem elegendő, hanem olyan közös európai – és elsősorban uniós – fellépésre van szükség, amely az országhatárokon átnyúló hálózat- és információbiztonsági fenyegetések és incidensek kezelésére képes, mert az ilyen akciók képesek lehetnek akár az Unió egészére is kihatással bírni. Mindez pedig a lakosság biztonságérzetének nagymértékű (további) csökkenéséhez vezethet, és *a kiberfenyegetések a migráció jelentette fenyegetéssel hasonló szintre kerülhetnek.* Ugyanakkor nem szabad figyelmen kívül hagyni azt sem, hogy a kibertér egy határokat nem ismerő, szabad mozgást lehetővé tevő globális tér – hasonlóan magához az Európai Unióhoz -, amely működésének egyik alappillére a személyek szabad mozgásának biztosítása. Ezért *elengedhetetlen egy közös, biztonságos európai kibertér létrehozása*, amely nemzeti, közösségi és nemzetközi szinten történő stratégiai és operatív együttműködés további fejlesztésével érhető el.

Nem túlzás, ha azt állítjuk, hogy az európai lakosság még nincs teljesen sem felkészülve, sem felkészítve a kibertérből származó veszélyekkel szemben. Az Eurobarométer által publikált, kifejezetten a kiberbiztonsággal foglalkozó felmérés érdekes képet fest az európai piacról. Bár az internethasználat tagállamonként igen eltérő,[1] az uniós polgárok átlag 63%-a napi szinten használja az internetet és mindössze 24% annak a kisebbségnek aránya, amely egyáltalán nem használja (ki) a világháló adta lehetőségeket.[2] [1] Egész Európa internethasználata még ennél is magasabb, 73%-os. [2] Ez a világátlag (50%) felett van, de ne felejtsük el, hogy igen elmaradt térségek adatai is részét képezik a felméréseknek. Az a

[1] Az északi államok e területen is élen járnak, kiemelten Norvégia, Svédország, Dánia és Hollandia (94-94%), míg a legelmaradottabb államok között tartják számon Romániát és Bulgáriát e vonatkozásában is (alig 50%-kal).

[2] Érdekesség, hogy a világhálót használók számaránya tekintetében Izland vezeti az államok listáját, 96%-kal.

„mindössze" kifejezés tehát természetesen igen relatív, mert az uniós polgárok 24%-a is összesen 121 millió lakost jelent, tehát koránt sem beszélhetünk egy kis létszámú csoportról.

Az internethasználók magatartása azonban fokozatosan közelít afelé, amit *biztonságtudatosnak* nevezhetünk: 60%-uk legalább évente megváltoztatja a jelszavát, 61%-uk használ vírusirtó programokat, 49%-uk megnyitás nélkül törli az ismeretlen feladótól származó e-maileket és személyes adataikat is sokkal óvatosabban szolgáltatják internetes felületeken. Talán ennek is köszönhető az internethasználók körében igen elterjedt azon (tév)hit, hogy képesek saját magukat hatékonyan megvédeni a kibertérben – bár ezt leginkább a fejlett államok polgárai gondolják ekképp.

A SZABÁLYOZÁS SAROKPONTJAI

A szabályozás szükségességét már maga az Unió is felismerte, és mintegy 10 évvel ezelőtt megkezdte kiberbiztonsága kereteinek kiépítését. Mivel az EU számos fenyegetést elsősorban civil oldalról közelít meg – így a kibertérben jelentkező fenyegetéseket is –, a hangsúlyt a szabad, nyílt internet megteremtésére helyezi, amelyet elsősorban a nemzetközi együttműködés kiszélesítése, valamint a szabályozók megalkotása révén kíván elérni.

A kiberbiztonságot néhány más szakterület már megelőzte a szabályalkotás terén. Itt utalok a terrorizmus elleni uniós szabályokra, amelyek elfogadására a 2001. szeptember 11-i események következtében került sor a 2000-es évek elején, majd ehhez kapcsolódva és ezzel párhuzamosan jelentkezett az igény a kritikus infrastruktúrák és az infokommunikációs hálózatok védelme iránt,[3] végül pedig mindezek folyománya volt a digitális egységes piac megteremtése érdekében tett lépések sora.

A szabályozás legmagasabb szintjét a stratégiai szint képezi. Az Unió 2003 decemberében fogadta el első *biztonsági stratégiáját*, amely „Egy biztonságos Európa egy jobb világban. Az Európai Biztonsági Stratégia" címet viseli. [6] A dokumentum felsorolja a globális és a konkrétan Európát fenyegető kihívásokat, amelyek között ugyan nevesítve nem szerepel a kiberfenyegetések köre, azonban a nemzetközi terrorizmus és a társadalmak sebezhetőségének kiemelésével már utal a kritikus infrastruktúrára. A stratégia felülvizsgálatának hosszas folyamatában mérföldkő volt a 2008 decemberében kiadott jelentés, amely a kiberbiztonságot már mint fő kihívást nevesítette. A jelentés utal a modern társadalmak kritikus infrastruktúrától való nagyfokú függésére, amely – többek között – az internet világát is érinti. A 2003-as stratégia átdolgozása egyre sürgetőbbé vált a globális környezet gyors és nagyfokú megváltozásának köszönhetően. Az államok digitális technológiáktól való függése drasztikusan megnövekedett és az Unió számára stratégia érdekké vált, hogy polgárai számára biztosítani tudja a mindenki számára biztonságosan hozzáférhető internetet. A stratégiaalkotás folyamata lassan haladt, az Európai Uniónak mintegy 13 évébe telt az új dokumentum elfogadása. 2016 nyarán „Közös jövőkép, közös cselekvés: erősebb Európa. Az EU globális kül- és biztonságpolitika stratégiája" címmel

[3] Az első jelentős lépés a 2004-ben kiadott „A létfontosságú infrastruktúrák védelme a terrorizmus elleni küzdelemben" című bizottsági közlemény volt, amelyben a kibertámadást és a kiberterrorizmust első alkalommal hivatalos uniós dokumentumban megemlítették – még ha „csak" a kritikus infrastruktúrákkal kapcsolatosan is. [3] Ezt követte a Bizottság által 2006-ban elfogadott program a kritikus infrastruktúrák védelmére vonatkozóan (EPCIP) [4], majd a program végrehajtására vonatkozó Zöld Könyv. 2008-ban előbb egy irányelvben összegezték a kritikus infrastruktúrák védelmének kapcsolatos előrelépési lehetőségeket [5], majd felállítottak egy, a kritikus infrastruktúrák védelméért felelős európai hálózatot (European Reference Network for Critical Infrastructure Protection – ERNCIP), melynek fő feladata a tagállamok közötti információ-megosztás és a kutatás elősegítése, elsősorban a kutatóközpontokon keresztül. (Jelenleg mintegy 140 intézmény segíti a hálózat munkáját).

jelent meg az unió új biztonsági stratégiája [7], amelyben a kiberterület már nevesítve és kiemelt helyen szerepel a kihívások kezelésére szánt eszközök és szakpolitikák között.[4]

Az első dokumentumot, amely kifejezetten az információs rendszerek védelmével kapcsolatos, *2009*-ben adta ki az Unió. A *Bizottság közleménye* „Európa védelme a nagyszabású számítógépes támadások és hálózati zavarok ellen: a felkészültség, a védelem és az ellenálló-képesség fokozása" címmel jelent meg. A dokumentum a hiányosságok között kiemeli, hogy uniós szinten a kibervédelmi gyakorlatok még kezdetleges szinten állnak és a több országot átölelő gyakorlatok is igen ritkák. Ezért hangsúlyozza a más, e területen kialakult gyakorlattal rendelkező szervezetekkel – kiemelten az ENSZ-szel, a NATO-val, az OECD-vel és a G8-cal – való együttműködés fontosságát. Előremutató megállapítása volt a közleménynek, hogy szükségesnek tartotta olyan nemzeti számítástechnikai katasztrófaelhárító csoportok felállítását,[5] amelyek mind a korai előrejelzés, mind pedig az incidenskezelés terén megfelelő képességekkel rendelkeznek. A 2009-es közleményben foglaltak *felülvizsgálatára 2013*-ban került sor. A bizottsági munkacsoport jelentésében [9] már különválasztotta a kritikus infrastruktúra védelmével kapcsolatos tevékenységeket, és azokat a *megelőzés - felkészülés - következménykezelés hármas kategóriájába* osztotta. A kezdeti célok megvalósításának határidejét 2014. második felében jelölte meg.

Az Európai Unió kiemelt területként kezeli a *digitális vívmányok biztonságos használatá*nak elősegítését. Ennek elérésére előbb két ötéves programot indított (2000-2005.[6] és 2005-2010.[7]), jelenleg pedig a harmadik program fut, tízéves futamidővel (2010-2020.[8]). Az első ötéves program három célt tűzött ki annak érdekében, hogy Európa valamennyi államában létrejöhessen az információs társadalom: olcsóbb, gyorsabb és biztonságosabb internet biztosítása; szakemberek képzése; valamint az internethasználat fellendítése. A második ötéves periódusra megfogalmazott célok már jóval komplexebbek voltak: egy egységes európai információs tér megteremtése; az infokommunikációs szektor és a kutatások kiemelt támogatása,[9] valamint egy összeurópai információs társadalom megteremtése. A jelenleg érvényben lévő *tízéves program* fő célja a kibertér biztonságos használatának megteremtése. A menetrend felvázolja az olyan európai hiányosságokat, mint az interoperabilitás hiánya, a digitális piac töredezettsége, a kiberbűnözés növekvő mértéke, a befektetések hiánya vagy a szakképzett munkaerő hiánya, majd valamennyi probléma vonatkozásában megoldásokat javasol. A cél az volna, hogy 2020-ra az európai polgárok a lehető legszélesebb körben és a lehető legbiztonságosabb keretek között élvezhessék a digitális technológia nyújtotta előnyöket.

A Digitális Menetrend meghirdetését követően fellendült a kibertér iránti érdeklődés, és ez az uniós dokumentumokban is megmutatkozott. *2012*-ben az *Európai Parlament határozatot* fogadott el „Kritikus információs infrastruktúra védelme: a globális kiberbiztonság megteremtése felé" címmel. [13] Bár a dokumentum a tagállamokat kötelezni nem tudta, mégis olyan javaslatokat fogalmazott meg, amelyek mára ténylegesen is megvalósultak az uniós országokban. Ezek között szerepelt például a nemzeti kiberbiztonsági stratégia megalkotása, a kibervédelmi veszélyhelyzeti tervezés, az önálló kibervédelmi

[4] Részletesebben a stratégia elemzését lásd: [8]
[5] Ezek lesznek később a hálózatbiztonsági reagáló csoportok, a CERT-ek.
[6] eEurope Action Plan [10].
[7] i2010 – European Information Society for growth and employment [11].
[8] Európai Digitális Menetrend [12]
[9] A szektor kiemelt támogatására azért volt szükség, mert Európa nagy elmaradásban volt a világ vezető államaihoz képest. Míg az Egyesült Államok esetében infokommunikációs szektor a K+F költségvetés 34%-ából részesült, Japán esetében pedig 35%-ból, addig az EU vonatkozásában ez mindössze 18% volt.

szervezetrendszer felállítása vagy a vonatkozó nemzeti jogszabályok megalkotása. Innen már csak egy lépcsőfok volt az uniós kiberbiztonsági stratégia megalkotása, amelyre a következő évben sor is került. Az Unió *2013*-ban kiadta átfogó *kiberbiztonsági stratégiáját* „Nyílt, biztonságos és megbízható kibertér - Az Európai Unió kiberbiztonsági stratégiája" címmel. [14] A stratégia bemutatása és elemzése önálló tanulmány tárgya lehetne, ezért ezen a ponton csak a stratégiában megfogalmazott prioritásokat emelem ki. Ezek a következők:

- kibertámadások megelőzéséhez, feltárásához és kezeléséhez szükséges képességek kifejlesztése;
- a kiberbűnözés nagymértékű visszaszorítása
- önálló kibervédelmi politika és képességek fejlesztése az Unió közös biztonság- és védelempolitikáján belül;
- a szükséges ipari és technológiai kapacitások és feltételek megteremtése;
- önálló, uniós szintű kiberpolitika mint szakpolitika létrehozása az EU alapértékei mentén.

A stratégia megalkotása igen jelentős lépés volt az Unió részéről, a lefektetett prioritások pedig nagy ívű célokat állítanak a szervezet elé, amelyek elérése még a jövő zenéje. Ugyanakkor a stratégia csak az európai infokommunikációs rendszerek meghibásodásának és ellenük intézett támadások megelőzésére és a válaszlépésekre vonatkozik, s még az olyan kérdések is megválaszolatlanok maradnak, mint például az, hogy a Lisszaboni szerződés záradéka alapján az Európai Unió mint egész hogyan reagáljon egyik tagállamát ért kibertámadás esetén.

A kiberbiztonsági stratégiához szorosan kapcsolódik a *2015*-ben kiadott *európai digitális egységes piaci stratégia*, amely az európai társadalom átalakításáról szól. Cél az európai egységes digitális piac megteremtése, amely számos előnnyel jár: többek között az európai GDP-t 415 milliárd euróval növelné és számtalan új munkalehetőséget kínálna. A Bizottság közleménye szerint szükséges volna jobb fogyasztói és vállalkozói hozzáférést biztosítani az internetes szolgáltatásokhoz és termékekhez, amely a bizalom erősödéséhez, az indokolatlan – területalapú – korlátozások megszüntetéséhez, a digitális tartalomhoz való hozzáférés javításához és az (adó)terhek csökkenéséhez is vezetne. Azonban a digitális tér kiépülésének egyik nagyon fontos előfeltétele az uniós polgárok bizalmának elnyerése. Ehhez szükséges a kiberbiztonsági kapacitások fejlesztése úgy, hogy azokat valamennyi tagállamban azonos kondíciókkal használhassák a lakosok.

A stratégia kiemeli, hogy a digitális gazdaság óriási mértékben növekszik. A növekedés mértéke a big data ágazat esetében eléri az évi 40%-ot, amely hétszer gyorsabb, mint az informatikai piac éves növekedési üteme.

Ez utóbbi megállapítás már előrevetítette az uniós jogalkotás *új irányát*. Hosszas, mintegy négyéves egyeztetést követően 2016-ban fogadtak el két korszakalkotó jelentőségű jogi normát, az adatvédelmi rendeletet (General Data Protection Regulation – GDPR rendelet) [15] és a NIS irányelvet (Directive on security of network and information systems) [16]. A tanulmány második felében e két jogforrást fogom értékelő-elemző módon ismertetni, mielőtt azonban erre rátérnék, az európai keretek alapjaihoz hozzátartozik a szervezetrendszer rövid bemutatása is.

SZERVEZETRENDSZER

A szervezetrendszer kiépítése már az 1990-es években megkezdődött, előbb tagállami, majd uniós szinten. Azok az államok jártak élen, amelyek a legfejlettebb információs rendszerekkel rendelkeztek, mivel a bűnözők a meglévő rendszereket kezdték el támadni a kibertérben, s ezen támadások ellen kellett megfelelően felkészülniük az államoknak szervezeti értelemben

is. Létrehozták a *hálózatbiztonsági reagáló csoportokat* (computer emergency response team – CERT), országonként más és más szervezeti felépítéssel. Mára valamennyi uniós tagállamban működnek CERT-ek kormányzati szinten, de több állam esetében ágazati CERT-ek is működnek, és az unós intézmények mellett is létrehoztak CERT-eket.[10]

Az uniós szintű építkezés alapköveként *2014*-ben hozták létre az *Európai Hálózat- és Információbiztonsági Ügynökséget* (European Network Information and Security Agency – *ENISA*), amely az Európai Unió, a tagállamok és a magánszektor közötti együttműködést segíti az információ-megosztás, a tagállamok közötti koordináció és tanácsadás területén. 2012 óta minden év októberében megszervezi az *Európai Kiberbiztonsági Hónap*ot, amely egy nemzetközi tudatosító kampánysorozat. Célja a kiberbiztonsági tudatosság növelése és a kiberfenyegetések mind szélesebb körben történő megismertetése. Ennek keretében a civil és akadémiai szféra, valamint az illetékes helyi szervek Európa-szerte mintegy 450 program közül választhatnak – 2016-ban Magyarország 22 programmal kapcsolódott az eseménysorozathoz.[11] Másik jelentős éves programja a *Cyber Europe* elnevezésű pán-európai kiberbiztonsági gyakorlat, amelyet 2016-ban negyedik alkalommal rendezett meg. Célterületei az informatika, a telekommunikáció és az információbiztonsági iparágak voltak, és konkrét technikai incidenseket kellett megoldaniuk a játékosoknak.

Tágabb értelemben a szervezetrendszer részét képezik egyrészt a kiberbűnözés elleni küzdelemmel foglalkozó szervezetek (élén 2013 óta az Európai Rendőrségi Hivatal szervezetén belül létrejött Számítástechnikai Bűnözés Elleni Küzdelem Európai Uniós Központjával), másrészt a kritikus infrastruktúra területén a Kritikus Infrastruktúra Figyelmeztető Információs Hálózat (Critical Infrastructure Warning Information Network – CIWIN) és a Kritikus Infrastruktúravédelmi Európai Referenciahálózat (ERNCIP).

Az Európai Unió maga is számos kezdeményezéssel támogatja az európai kiberbiztonság megvalósítását. Legnagyobb volumenű programja a *Horizon 2020 program [18]*, amely az Unió történetének legnagyobb K+F financiális eszköze. Hétéves költségvetése 80 milliárd euró, amely további magánszektorbeli befektetésekre ösztönöz. Ilyen a 2016 nyarán bejelentett *kiberbiztonsági köz-magán társulás* létrehozása, amely 450 millió eurót fektet be az EU K+F tevékenységébe, s várhatóan 2020-ig ezen összeg bő háromszorosa, mintegy 1,8 milliárd euró értékű beruházás valósul meg. [19] A társulás célja az együttműködés elősegítése a kutatási és innovációs folyamat korai szakaszában, és kiberbiztonsági megoldások kidolgozása a különböző ágazatok – elsősorban az energiaipar, az egészségügy, a közlekedés és pénzügyi ágazat – számára. [20]

Végezetül megemlítem, hogy az Európai Unió számos nemzetközi szervezettel aktívan együttműködik a kiberbiztonság területét érintően (is). Kiemelendő az Európai Biztonsági és Együttműködési Szervezettel (OSCE), a Gazdasági Együttműködési és Fejlesztési Szervezettel (OECD) és az ENSZ szakosított intézményével, a Nemzetközi Telekommunikációs Unióval (ITU) kialakított együttműködés. Az együttműködés lényegi pontjainak ismertetése túlmutat jelen tanulmány keretein, azt külön kívánom bemutatni.

[10] 2012-ben felállították a Bizottság és a Tanács Főtitkársága, a Parlament és a Régiók Bizottsága közös CERT-jét is (CERT-EU).

[11] 2016-ban Az Európai Bankföderáció és az Europol Európai Kiberbűnözési Központja (E3C) is csatlakozott a rendezvényhez, mert ezúttal a kiemelt témák között szerepelt a bankolás biztonsága és a mobil eszközök kártevőinek problémaköre is. [17]

A NIS IRÁNYELV

Az Európai Unió évek óta azon dolgozik, hogy Európa kiberbiztonságát megerősítse és képes legyen garantálni. Az Uniót a lépések megtételére olyan események késztették, mint például az Észtországot 2007-ben ért igen átfogó kibertámadás, az ukrán elektromos hálózat megbénítása 2015-ben vagy a kórházi rendszerek állandó megfertőzése különböző (zsaroló)vírusokkal. 2015-ben például globálisan 38%-kal több kiberbiztonságot érintő incidenst jelentettek, mint a megelőző esztendőben, és becslések szerint csak az Unióban évente 260-340 milliárd eurós kár keletkezik ilyen eseményekből. [21]

A jogalkotási folyamat az Unióra jellemző komótos tempóban haladt az utóbbi években, de 2016-ra már kézzelfogható eredményeket sikerült felmutatnia.[12] Ezek a szabályozások hiánypótlóak, mert ezidáig nem létezett olyan uniós szintű egységes szabályrendszer, amely valamennyi tagállamra vonatkozóan kötelező előírásokat tartalmazott volna. Ehelyett a tagállamok a saját érdekeik mentén maguk szabályozták ezt a támadásoknak egyre inkább kitett speciális területet, amely az európai információs piac felaprózódásához és az állampolgárok kiszolgáltatottá tételéhez vezetett. Márpedig manapság nem csak a szolgáltatások nem ismernek országhatárokat, de a bekövetkezett információbiztonsági események is kihat(hat)nak az Unió egészére, ezért a közös uniós fellépés ezen a területen igen indokolt.

Az így kialakuló egységes európai szabályozás egyik pillére a *2016*. július 6-án az Európai Parlament által jóváhagyott (és augusztus 8-án hatályba lépett) *Irányelv a hálózati és információs rendszerek biztonságáról* (Directive concerning measures for a high common level of security of network and information systems across the Union – a továbbiakban: NIS irányelv). [16] Ez az első olyan, uniós szintű kiberbiztonsági szabályozás, amely képes lehet megakadályozni az európai infrastruktúra elleni kibertámadásokat. Az irányelv fő célja a nemzeti szabályok közös nevezőre hozása úgy, hogy kötelező biztonsági minimumokat ír elő valamennyi tagállam számára, s ehhez közös intézményi rendszert és szabályozást bevezetését írja elő.

Az irányelv *alanyi hatálya* kettős: az alapvető szolgáltatást nyújtók köre (azaz a kritikus infrastruktúra) és a digitális szolgáltatás nyújtó köre, vagyis akik ellen intézett támadás a legközvetlenebbül képes kihatni a lakosságra. Az első csoportba tartozók körét a tagállamok olyan kritériumok alapján határozzák meg, hogy a nyújtott szolgáltatás társadalmi vagy gazdasági szempontból alapvetőnek minősíthető-e, a szolgáltatás nyújtása hálózati és információs rendszerektől függ-e és egy esetleges incidens képes-e zavart okozni a szolgáltatás nyújtásában (5. cikk (2) bek.). Ezek alapján ide sorolhatók például az ivóvízellátó cégek, az energiavállalatok, a közlekedési vállalatok, az egészségügyi szolgáltatók, a banki szolgáltatást nyújtók vagy a digitális infrastruktúrák. Természetesen, ha egy kiberbiztonsági incidens egy ilyen vállalatot érint, de a támadás például csak a kommunikációs részlegére hat ki és az alapvető szolgáltatás nyújtását nem befolyásolja, akkor ez nem esik az irányelv hatálya alá. Ugyanakkor egy biztonsági esemény hatásának vizsgálatánál mindig alapvető

[12] A NIS irányelv esetében például már 2013-ban megszületett az első javaslat (2013/0027 (COD). A távközléssel és az információs társadalommal foglalkozó munkacsoport (WP TELE) előkészítő munkáját követően az Európai Unió Tanácsa 2013. július 6-án irányadó vitát folytatott le az irányelvtervezetről. A TTE Tanács előbb 2013. december 5-i ülésén, majd 2014. június 6-i ülésén vitatta meg az addigi eredményekről szóló jelentéseket. 2014 végén és 2015. április 30-án háromoldalú egyeztetésre került sor a Tanáccsal és a Parlamenttel, de még ekkor is lényegi különbségek voltak a két fő szerv álláspontja között. Végül 2015. június 29-re sikerült megállapodniuk az alapelvekről, amelyek már bekerültek a az irányelvtervezetbe. 2015. december 18-án pedig a COREPER közbenjárásával rögzítették az informális megállapodás főbb pontjait. [22] [23] [24].

szempontok, hogy a szolgáltatás kimaradása hány embert érint, mennyi ideig tart és földrajzi értelemben mennyire kiterjedt.

Az alanyi kör másik csoportjába azok a digitális szolgáltatók tartoznak, amelyek fontos, de nem nélkülözhetetlen szolgáltatásokat nyújtanak. Ilyenek például a kereső- és felhőszolgáltatók vagy az online piacterek. A szolgáltatásnyújtók köre nem korlátozódik az Unió területére, a lényeg, hogy a szolgáltatás nyújtására az EU területén kerüljön sor. Így olyan nagy világcégekre is kiterjed az irányelv hatálya, mint például a Google, az Amazon vagy az eBay. Ugyanakkor érdemes megemlíteni, hogy bár az irányelv korábbi tervezetében szerepelt, a végleges szövegből mégis kikerült a közösségi szolgáltatást nyújtók köre, tehát például a Facebook-ra nem vonatkoznak az irányelvben lefektetett szabályok.

Az irányelv mindkét alanyi kör számára vonatkozóan előír két kötelezettséget: egyrészt olyan hálózat- és rendszerbiztonságot kell garantálniuk, amely a rájuk leselkedő kockázatokkal arányos mértékű, másrészt pedig az illetékes hatóságok felé incidens-bejelentési kötelezettségük is van. Az alapvető szolgáltatást nyújtók esetében ezen felül további biztonsági garancia, hogy a tagállami hatóságok ellenőrizhetik, hogy a szolgáltatásnyújtók milyen biztonsági lépések megtételét tervezik és ezeket ténylegesen is valósítják-e.

A tagállamoknak valamennyi, az irányelvben szereplő kötelezettségnek 2018 májusáig eleget kell tenniük. Összegezve az irányelvben előírt legfontosabb előírásokat, azok a következők:

- Minden tagállamnak meg kell alkotnia a saját hálózat-és információbiztonsági stratégiáját.
- Minden tagállamban fel kell állítani egy, a számítógép-biztonsági eseményekre szakszerűen válaszolni képes gyorsreagálású kibervédelmi szakértői csapatot, ún. CSIRT-et (Computer Security Incident Response Team).[13] (Magyarország e kötelezettségnek már korábban eleget tett.)[14]
- A nemzeti CSIRT-ekből fel kell állítani egy uniós CSIRT-hálózatot, amelynek kötelezően valamennyi tagja lesz valamennyi CSIRT.
- Uniós szinten is létre kell hozni egy olyan Együttműködési Csoportot (Contact Group), amely a nemzeti hatóságok és CSIRT-ekből felépülő CSIRT-hálózat közötti stratégiai együttműködést támogatja és segíti. Ezzel az irányelv az első olyan közösségi szabályozás, amely kötelező együttműködést ír elő a (nemzeti) intézmények számára.[15] Ennek azonban előfeltétele a tagállamok közötti bizalom kiépülése, amelynek idő kell.
- Az irányelv átültetésére és végrehajtására ki kell jelölniük egy nemzeti hatóságot.
- Szektoronként pontosítani kell azon kritériumokat, amely alapján egy vállalat az irányelv hatálya alá tartozik, majd a szolgáltatói kört nevesíteni kell. Ezt a

[13] Elterjedt a CERT kifejezés használata is (Computer Emergency Response Team). A kettő mára szinonimává vált; az EU-ban inkább a CSIRT, Magyarországon inkább a CERT kifejezést használják. Az eltérés oka abban keresendő, hogy a CERT kifejezés mára speciális szellemi tulajdonjogi védelem alá esik.

[14] Bár az irányelv alapján tagállamonként csak egy CSIRT felállítása kötelező, de lehetőség van arra is, hogy akár valamennyi szektorban létrehozzanak ilyen szakértői csoportokat. Magyarországon már jelenleg is több ilyen reagáló csoport működik. A kormányzati rendszerek védelmében a GovCERT, a Honvédelmi Minisztériumnál a MilCERT jött létre, de önkéntes alapon a kormányzati szektoron kívül működő HunCERT az internetszolgáltatók, a NIIF CSIRT pedig az oktatási - kutatási - közgyűjteményi intézmények eseménykezelését végzi.

[15] Ezt megelőzően önkéntes és erősen bizalmi alapon zajlott az együttműködés az illetékes tagállami szervek között.

tagállamoknak 2018 novemberéig kell megtenniük. (A kritikus ágazatokban működő mikro- és kisvállalatokra ezen előírások nem vonatkoznak.)

A szabályozás részleteinek kidolgozására és az irányelv által nevesített feladatok végrehajtására az Európai Bizottság 2016 májusában felállított egy szakértői csoportot valamennyi tagállam részvételével (Magyarországot a Nemzeti Kibervédelmi Intézet képviseli).

Az irányelv 25. cikke értelmében a rendelkezéseket valamennyi tagállamnak át kell ültetnie a nemzeti jogába. Az átültetési határidő 2018. május 9-e. Az elfogadott és kihirdetett főbb törvényi, rendeleti és közigazgatási rendelkezések szövegét pedig valamennyi tagállam köteles a Bizottsággal közölni.

Az irányelv rendelkezik a szabályozás ellenőrzésének menetéről is. A 23. cikk értelmében a Bizottság feladata, hogy értékelje a tagállamok alapvető szolgáltatásokat nyújtó szereplők azonosítására vonatkozó kötelezettségének teljesítését. Ezt 2019. május 9-ig jelentés formájában kell megtennie, amely elfogadásáról a Parlament és a Tanács dönt.

A GDPR

Az újonnan kialakuló egységes európai szabályozás második pillére az Unió általános *adatvédelmi rendelete* (General Data Protection Regulation, a továbbiakban: GDPR).[16] A korábbi adatvédelmi irányelvet[17] még 1995-ben fogadták el az Unióban, éppen a digitális kor hajnalán, ezért az abban foglalt szabályokat az elmúlt húsz év alatt meghaladta az idő, és azok hol elégtelennek bizonyultak az újszerű problémák megoldásához, hol túl tág mozgásteret adtak a tagállamoknak. A legnagyobb probléma mégis az volt, hogy az irányelv nem tudta elérni azon célját, hogy a tagállami szabályozásokat közös nevezőre hozza, így *mára 28 különféle adatvédelmi szabályozás jött létre az Unión belül.* Ez azzal járt, hogy a felhasználók egészen más védelemben részesülnek az egyik tagállamban, mint adatfeldolgozás helyén, mint egy másik országban. Többek között ezt a helyzetet hivatott orvosolni az új szabályozás, amelyet egy hosszas, mintegy négy éves előkészítő munka előzött meg. A Bizottság már 2012-ben útjára indította a reformkezdeményezést, amely az EU főszervei között létrejött kompromisszumot követően nyerte el végleges formáját. A rendelet legnagyobb jelentősége ezért abban rejlik, hogy az Unió *igen nagy lépést tehet a digitális egységes piac kialakulása felé.*

Az új szabályozás két elemből épül fel: az egyik a már említett GDPR, a másik pedig az új adatvédelmi irányelv, amely a rendőri és bűnüldöző szervek adatkezelésére vonatkozóan tartalmaz előírásokat. A továbbiakban csak röviden ismertetem a GDPR legfontosabb szabályait.

Az Európai Parlament 2016. május 4-án fogadta el a rendeletet, amely a kihirdetést követő 20. napon lép hatályba, ténylegesen azonban csak *2018. május 25-től kezdve kell alkalmazni*. A tagállamoknak és a vállalatoknak tehát két évük van a felkészülésre, amely bár első ránézésre hosszú időnek tűnhet, valójában azonban még a legfelkészültebbeknek is sok tennivalójuk van hátra.

---

[16] *Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (2016. április 27.) természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről*

[17] 95/46/EC irányelv

A rendelet *tárgyi hatálya* minden olyan adatra kiterjed, amely természetes személyt azonosít, vagy amely által természetes személy azonosítható. Ennek értelmében egyes online adatkategóriák is személyes adatnak minősülhetnek, így például a cookie ID-k, az IP-címek[18] vagy az online azonosítók. A különleges adatokra továbbra is szigorúbb szabályok vonatkoznak (kezelésükre csak az érintett kifejezett hozzájárulásával van lehetőség), és ezen adatok köre is tovább bővült *a genetikai és biometrikus* adatokkal.

A rendelet – jogforrási mivoltából fakadóan – közvetlenül alkalmazandó és valamennyi tagállamra vonatkozóan állapít meg kötelezettségeket, amely már önmagában jelzi a szabályozás fontosságát. A rendelet *személyi hatálya* azon vállalatokra is kiterjed, amelyek bár az Unión kívül működnek, tevékenységük azonban érinti az uniós polgárok személyes adatait. Ugyanakkor könnyít a szabályozás a tekintetben, hogy azon vállalatoknak, amelyek több tagállamban rendelkeznek leányvállalattal, már csak egy, a központi ügyintézés helye szerinti hatóság felé kell eljárniuk.[19] További jelentős változás, hogy a rendelet már nem csak az adatkezelőkre, hanem az ő megbízásukból eljáró adatfeldolgozókra is előír kötelezettségeket.

A GDPR tehát vonatkozik olyan, Unión kívüli vállalatokra is, amelyek Európán kívül végeznek adatkezelést. Esetükben elsősorban az adatok továbbítása lehet problémás. A rendelet alapján harmadik országba csak akkor továbbítható adat, ha az adatok megfelelő szintű védelme a célországban is biztosított. Ennek igazolására három lehetőség kínálkozik:

- A Bizottság ezt egy ún. megfelelőségi határozatban deklarálja.[20] [27]
- Egyes vállalatok kialakult adatkezelési gyakorlata is igazolhatja az adatok megfelelő szintű védelmét. A gyakorlatot a cégek a Bizottsággal kötendő modellszerződésekkel tudják szentesíteni, amelyek lényegében általános szerződési feltételek vállalását jelentik.[21] [28]
- Végül megoldás lehet a kötelező érvényű vállalati szabályok (BCR) bevezetése is. [29] Ez a cégcsoporton belüli adattovábbítást teszi lehetővé különböző államok között.

A rendelet értelmében súlyos szankciókkal sújthatók az előírásokat megszegő vállalatok. A felügyeleti hatóságok által kiszabható pénzbüntetés mértéke attól függ, hogy a rendelet mely rendelkezését sértette meg a szolgáltató. Ez legalább a vállalat előző évi *globális árbevételének 2%-a*, de legsúlyosabb esetben a bírság elérheti a 4%-ot is.[22] Emellett a vállalatnak igen szigorú átláthatósági követelményeknek is meg kell felelniük és a tájékoztatási kötelezettséggel kapcsolatos eljárások is jelentősen szigorodnak. Részletesen szabályozták továbbá, hogy adatkezelési incidens esetén a cégeknek hogyan kell eljárniuk a felügyeleti hatóságok és az érintettek felé. A hatóságokat[23] 72 órán belül értesíteni kell, az érintetteket azonban csak akkor, ha az incidens minden valószínűség szerint magas kockázattal jár rájuk nézve.

---

[18] Az IP-címek személyes adat jellegével kapcsolatos jelenlegi bizonytalanságokat olyan és ahhoz hasonló eseti döntések szüntethetik meg, mint például az Európai Unió Bíróságának döntése a Breyer v. Németország ügyben. [25]

[19] A Bizottság becslése szerint ezzel évente 2,3 milliárd eurót lehet megtakarítani. [26]

[20] Ilyen jelenleg 11 nem uniós terület esetében létezik és ilyen volt a Safe Harbor egyezmény is az Egyesült Államokkal (amelyet hatályon kívül helyezését követően a Privacy Shield váltott fel 2016 júliusában).

[21] Ezen megoldás hátránya, hogy a cégek számára nem biztosít mozgásteret és sok leányvállalattal rendelkező cégek esetében az adminisztratív teher nagyon megnövekedhet.

[22] A kiszabható pénzbírság mértéke tehát jóval magasabb, mint a Magyarországon maximálisan kiszabható 20 millió forint.

[23] Magyarországon a kijelölt hatóság a Nemzeti Adatvédelmi és Információszabadság Hatósát (NAIH).

Végül megemlítem, hogy a rendelet az *érintettek jogait* jelentős mértékben kiszélesítette. Az új szabályozás változatlanul biztosítja az érintettek számára a tájékoztatáshoz és a helyesbítéshez való jogot (azzal, hogy ezeket csak ésszerű határok között érvényesíthetik, amely az adatkezelőket védő klauzula), ugyanakkor a jogosultságok listája jelentősen kibővült. Az egyik legfontosabb a felejtéshez való jog, amely az érintett személyes adat törlése iránti kérelmét jelenti – bár ez nem abszolút jog, mert más jogalappal az adatkezelő tovább kezelheti az adatokat. Emellett az érintettnek joga van tiltakozni egyes adatkezelések ellen. Bár ez önmagában szintén nem abszolút jog, de a direkt marketing célú adatkezelések elleni tiltakozást viszont már abszolút jogként rögzítették. Az érintetteknek joga van adatai hordozására is, tehát kérésére az egyik szolgáltató köteles átadni a személyes adatait a másik szolgáltatónak. Ezen jog gyakorlati működése azonban igen kérdéses.

A rendelet az adatvédelmi szabályok érvényre juttatását is forradalmasítani kívánja, mégpedig oly módon, hogy az „egyablakos ügyintézés" megvalósítására felállítja az *Európai Adatvédelmi Tanács*ot (European Data Protection Board, EDPB). A Tanács a kijelölt tagállami hatóságok egy-egy képviselőjéből fog állni, és működésében szavazati jog nélkül részt vesz majd az Európai Bizottság képviselője is. Feladata alapvetően véleményalkotás lesz egyedi ügyek vonatkozásában.

A NIS IRÁNYELV ÉS A GDPR RENDELET KÖZÖTTI LEGFŐBB KÜLÖNBSÉGEK

Bár első ránézésre a két jogforrás nagyon hasonlónak tűnhet, ugyanis mind a kettő biztonsági előírásokat ír elő a tagállamok számára és incidens-bejelentési kötelezettséget rögzít számukra, azonban a két jogi norma más irányból közelíti meg az információbiztonság témakörét. A különbségek az alábbiakban ragadhatók meg [30]:

- A GDPR rendelet középpontjában a felhasználó mint egyén áll, mert a szabályozás célja a személyes adatok és a magánszféra védelme. Ezzel szemben a NIS irányelvben foglaltak a szolgáltatókat célozzák meg és a hálózatvédelemre helyeződik a hangsúly.
- Míg a GDPR valamennyi olyan vállalatra vonatkozik, amely az unió polgárainak személyes adatait kezeli, addig a NIS irányelv csak a legfontosabb szolgáltatókra vonatkozóan ír elő kötelezettségeket.
- Az incidens-bejelentési kötelezettség terén különbség, hogy a GDPR esetében olyan biztonsági eseményeket kell bejelenteni, amelyeknél személyes adat sérül(het), a NIS esetében pedig azokat, amelyeknél az adott szolgáltatás kerül veszélybe.

Az értesítési kötelezettség tekintetében különbség, hogy személyes adat sérelme esetében az adott cégnek közvetlenül az érintett felhasználót kell értesítenie, míg a NIS hatálya alá tartozó szolgáltatásnyújtóknak a felügyelő hatóság felé kell bejelentést tenniük, de csak a jelentős hatásúnak minősülő hálózati incidensek esetében

KÖVETKEZTETÉSEK

Az Európai Unió az elmúlt években igen jelentős lépéseket tett az európai digitális piac megteremtése felé. A megalkotott szabályok hiánypótlóak, mert korábban nem léteztek minden tagállamra vonatkozó, kötelező és egységes szabályok a kiberbiztonság területén. Az Unió intézkedései a kiberbiztonság megteremtése érdekében egyre határozottabb formát öltenek, az Európai Digitális Menetrendben megfogalmazott lépések sorra valósulnak meg és a Kiberbiztonsági Stratégia alapján elkezdett felépülni az uniós kibervédelem intézmény- és szabályrendszere. Az a jövő kérdése, hogy ezek a szabályok képesek-e elérni a céljukat és az uniós kibertér megfelelően védetté válhat-e. Szintén nyitott kérdés az olyan új technológiák, mint a Dolgok Internete (Internet of Things – IoT) és az okos eszközök hálózata, amelyek

által kezelt adatok mennyisége és minősége is jelentősen változhat a jövőben, és ez újabb biztonsági kockázatot rejt magában.

FELHASZNÁLT IRODALOM

[1] Global internet map http://www.internetsociety.org/map/global-internet-report/?gclid=CjwKEAiA79zDBRCgyf2FgeiY-CESJABzr0BMDdAMYfp2IUkRws20s3cTN5sV-SKnzy6Mr5aju1ATVRoCRu3w_wcB#global-internet-penetration 2016. 12. 05.

[2] http://www.internetworldstats.com/stats.htm 2016. 12. 05.

[3] A Bizottság közleménye a Tanács és az Európai Parlament részére – A létfontosságú infrastruktúrák védelme a terrorizmus elleni küzdelemben. http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex:52004DC0702, 2016. 12. 05.

[4] EPCIP - http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF, 2016. 12. 05.

[5] A kritikus infrastruktúrák védelmének kapcsolatos előrelépési lehetőségeket – Tanács 2008/117/EC irányelve (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF, 2016. 12. 05.

[6] Az Európai Biztonsági Stratégia https://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf, 2016. 12. 05.

[7] Az EU globális kül- és biztonságpolitika stratégiája – 2016 https://eeas.europa.eu/top_stories/pdf/eugs_review_web.pdf, 2016. 12. 05.

[8] MOLNÁR, ANNA: Közös jövőkép, közös cselekvés: erősebb Európa. Az EU globális kül- és biztonságpolitikai stratégiája. Nemzet és biztonság, 2016/2. szám 75-85. oldal

[9] Bizottsági munkacsoport jelentése – 2013.08.28., https://ec.europa.eu/energy/sites/ener/files/documents/20130828_epcip_commission_staff_working_document.pdf, 2016. 12. 05.

[10] eEurope Action Plan http://ec.europa.eu/idabc/en/document/70/5849.html, 2016. 12. 05.

[11] i2010 – European Information Society for growth and employment http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0229:FIN:EN:PDF, 2016. 12. 05.

[12] Európai Digitális Menetrend - http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52010DC0245R(01), 2016. 12. 05.

[13] Az Európai Parlament határozata – „Kritikus információs infrastruktúra védelme: a globális kiberbiztonság megteremtése felé” http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1479216690655&uri=CELEX:52012IP0237, 2016. 12. 05.

[14] Az Európai Unió kiberbiztonsági stratégiája http://register.consilium.europa.eu/doc/srv?f=ST+6225+2013+INIT&l=hu, 2016. 12. 05.

[15] GDPR – általános adatvédelmi rendelet http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf, 2016. 12. 05.

[16] NIS – hálózat-és információbiztonsági irányelv https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive, 2016. 12. 05.

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC, 2017. 01. 16.

[17] Európai Kiberbiztonsági Hónap http://www.cert-hungary.hu/kiberhonap, 2016. 12. 05.

[18] Horizon 2020 https://ec.europa.eu/programmes/horizon2020/en/what-horizon-2020, 2016. 12. 05.

[19] Kiberbiztonság: 1,8 milliárd eurót „mozdítana meg" az Európai Bizottság. 2016. július 5. http://kamaraonline.hu/cikk/kiberbiztonsag-18-milliard-eurot-mozditana-meg-az-europai-bizottsag, 2016. 12. 05.

[20] Nagy pofont kapnak a kiberbűnözők. 2016. július 5. http://www.napi.hu/nemzetkozi_gazdasag/nagy_pofont_kapnak_a_kiberbunozok.617292.html, 2016. 12. 05.

[21] SÁGI, Gyöngyi: Közelebb jutottunk a kiberbiztonság egységes uniós szabályozásához. 2016. január 18. http://bitport.hu/ujabb-akadalyt-vett-sikerrel-az-unios-kiberbiztonsagi-torveny-tervezete, 2017. 01. 16.

[22] A kiberbiztonság javítása az Európai Unióban http://www.consilium.europa.eu/hu/policies/cyber-security/, 2016. 11. 07.

[23] Hálózat- és információbiztonság: áttörés a Tanács és a Parlament közötti tárgyalásokban. http://www.consilium.europa.eu/hu/press/press-releases/2015/06/29-network-information-security, 2016. 11. 07.

[24] EU steps up cyber security: member states approve agreement. http://www.consilium.europa.eu/en/press/press-releases/2015/12/18-cybersecurity-agreement, 2016. 11. 07.

[25] Európai Unió Bírósága: Breyer v. Németország ügy. http://curia.europa.eu/juris/liste.jsf?td=ALL&language=hu&jur=C,T,F&num=C-582/14 2017. 01. 16.

[26] GÁLFFY, Csaba: Itt az EU új adatvédelmi keretrendszere. 2015. december 16. http://www.hwsw.hu/hirek/54917/eu-adatvedelem-szabalyozas-keretrendszer.html 2017. 01. 16.

[27] http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm 2017. 01. 17.

[28] http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm 2017. 01. 17.

[29] http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm 2017. 01. 17.

[30] BOLCSÓ, Dániel: Európa készül a kiberháborúra. 2016. augusztus 8. http://index.hu/tech/2016/08/08/europa_kiberbiztonsag_halozatvedelem_nis_iranyelv/ 2016.11.07.