

TANULMÁNYOK A TECHNOLÓGIA- ÉS CYBERJOG NÉHÁNY AKTUÁLIS KÉRDÉSÉRŐL

Tanulmányok a technológia- és
cyberjog néhány aktuális kérdéséről

30.

Sorozatszerkesztő:

Koltay András – Nyakas Levente

Tanulmányok a technológia- és cyberjog néhány aktuális kérdéséről

Szerkesztette:

Klein Tamás

Médiatudományi Intézet

2018

A kiadványt támogatta:



Minden jog fenntartva.

© Klein Tamás, Szabó Aliz, Tóth András

© Nemzeti Média- és Hírközlési Hatóság Médiatanács Médiatudományi Intézete, 2018

Tartalom

Előszó	9
Klein Tamás: Az online diskurzusok egyes szabályozási kérdései	11
1. Az internetes kommunikáció jogi előkérdése – a jogi szabályozhatóság dilemmája	11
2. Az internetes tömegkommunikáció hatása a nyilvánosság szerkezetére	13
2.1. A technológia hatása.....	13
2.2. A kapuőrök alkonya?.....	15
2.3. A szolgáltatók tevékenysége és differenciálódása	17
2.4. A jog kihívásáról általában	17
3. Az internetes kommunikáció sajátosságai	18
3.1. Anonimitás.....	18
3.2. Határok nélküiség, decentralizált hálózat.....	19
3.3. Az online diskurzusok kulturálatlansága	20
4. A tárhelyszolgáltató felelőssége a harmadik személyek jogellenes tartalmaiért – Az érdekek összebékítésének nemzetközi modelljei.....	21
5. Keresőmotor-szolgáltatók és az internetes szólásszabadság	26
5.1. A találati lista szólásjellege Európában és az Egyesült Államokban	28
5.2. Az automatikus keresési javaslat (autocomplete) és a szolgáltatói felelősség.....	29
6. Az internetes nyilvánosság új színtere: a közösségi hálózatok, platformok – a közösségi média	31
6.1. A közösségi hálózatok jogi kihívásairól általában	32
6.2. A közösségi platformon közzétett vélemény jellege: a „like” alkotmányos megítélése	33
6.3. A közösségi oldalak szolgáltatóinak szabályozási tevékenységével összefüggő jogi problémák	34
7. Következtetések	39
Klein Tamás: A web 2.0. egyes szabályozási kérdései	41
– különös tekintettel az alkotmányjogi vonatkozásokra	41
1. Bevezetés	41
2. A közösségi hálózatok és a szólás szabadsága	42
3. Frekvenciaszűkösség után szűrőbuborék? – a személyre szabott tartalomkínálat csapdája.....	45
4. Valótlan hírek a vélemények piacán – álhírek a demokratikus nyilvánosságban.....	47
Tóth András: A web 2.0 versenyjogi vonatkozásai	51
1. Bevezetés	51
2. A Web 2.0 versenyjogi szempontból jelentős jellemzői	52
3. Adat alapú piaci hatalom?	53
4. A versenyjog, mint az adatvédelem eszköze	56
5. Az online platformokkal kapcsolatos versenyjogi kérdések	58
5.1. Árjellegű korlátozások és visszaélések.....	58

5.2. Nem árjellegű korlátozások és visszaélések	60
---	----

Tóth András: Hálózati és információs rendszerek biztonsága európai szabályozásának alapjai

67

1. Bevezetés.....	67
2. Fogalmi keretek	67
3. A HIR szabályozásának rendszere és jellemzői.....	69
4. Az Európai Unió HIR biztonsági szabályozása	70
4.1. Az EU szabályozás fejlődése.....	70
4.2. HIR ellenálló képességére vonatkozó EU szabályozás	73
4.3. HIR biztonságát szolgáló adatvédelmi rendelkezések	83
5. Összegzés	87

Klein Tamás: A felhőszolgáltatások egyes jogi kérdései – különös tekintettel az Európai Unió szabályozására

89

1. Prológus	89
2. A felhőszolgáltatások információtechnológiai alapjai.....	91
2.1. A felhőszolgáltatások fogalmi meghatározhatósága.....	91
2.2. A felhőalapú szolgáltatások működési elve	92
2.3. A 'felhő földrajz' – az adattárolás helye.....	93
2.4. A felhőszolgáltatások legfontosabb előnyei a felhasználók számára	94
2.5. A felhőszolgáltatások és az IKT-szektor fejlődési lehetősége.....	95
2.6. A felhőszolgáltatási modellek tipológiája	96
2.7. A felhőalapú technológia jogilag releváns sajátosságai.....	98
2.8. A felhőszolgáltatás társadalmi és gazdasági haszna.....	99
2.9. EU perspektíva – A számítási felhőben rejlő potenciál felszabadítása Európában... 100	
3. A felhőalapú szolgáltatások adatvédelmi jogi összefüggései.....	101
3.1. A felhőszolgáltatások általános adatvédelmi kockázatai	101
4. Az Európai Unió adatvédelmi jogi szabályozási kerete és a felhőszolgáltatás kihívása ... 103	
4.1. Az Európai Unió szabályozásának jogi forrásai és a jogalap	103
4.2. Az alkalmazott nemzeti jog meghatározása.....	104
4.3. Nemzetközi adattovábbítások.....	105
4.4. A biztonságos adatkikötő (Safe Harbor) és a megfelelő védelmi szint elve.....	107
4.5. Az adatvédelem és adatbiztonság technikai és szervezési intézkedései a felhőalapú szolgáltatásokban	111
4.6. A felhőjogviszony alanyai.....	114
4.7. Felelősség a felhőjogviszonyban	117
5. A felhőszolgáltatás, mint tárhelyszolgáltatás	119
6. Epilógus.....	121

Klein Tamás - Szabó Aliz: A cybercrime, mint infokommunikációs jogi probléma

123

1. Néhány előkérdés	123
2. A cybercrime fogalmi kérdései.....	126
2.1. A jelenség első kutatói	127
2.2. A számítógépes bűncselekmények csoportosítása.....	127

3. A számítógépes bűnözés történeti fejlődése.....	128
3.1. Az első számítógépes bűncselekmények	129
3.2. A kiberbűnözés jellemzői	129
3.3. A technológiai fejlődés konzekvenciái.....	132
4. Nemzeti jogforrásaink.....	134
4.1. A Nemzeti Kiberbiztonsági Stratégia	134
4.2. Magyarország Digitális Gyermekvédelmi Stratégiája.....	135
4.3. Magyarország Digitális Oktatási Stratégiája	135
5. Nemzetközi jogforrások	136
5.1. A Számítástechnikai Bűnözésről Szóló Egyezmény és újragondolása.....	136
5.2. Az Európai Bizottság biztonsági stratégiája	137
5.3. További kiemelkedő nemzetközi dokumentumok	137
5.4. General Data Protection Regulation (GDPR) – a jövő	138
6. EU-s jogforrások	139
6.1. Az Európai Unió számítógépes bűnözésre vonatkozó jogforrásai	139
6.2. European Cybercrime Centre	141
7. A csúcstechnológiai bűnözés elleni harc régen és ma.....	142
7.1. A Nemzeti Kibervédelmi Intézet megalakulása.....	143
8. Az online-tér devianciái.....	144
8.1. Cyberbullying	145
8.2. Adathalászat: phishing, pharming.....	148
9. A jogellenes tartalmak és a cybercrime viszonya	150
9.1. Az egyes tartalmak közötti különbségtétel.....	151
9.2. Az internetszolgáltatók felelőssége	152
9.3. A hiperlink (hiperhivatkozás) mint a jogsértés eszköze	153
9.4. A jogellenes tartalmak blokkolása.....	153
10. Mary esete a kiberbűnözéssel.....	154
11. Néhány megállapítás és egy de lege ferenda javaslat	158

Előszó

A Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar Infokommunikációs Jogi Tanszéke néhány évvel ezelőtt elhatározta, hogy olyan kutatóműhely kíván lenni, ahol a tanszéki oktatók az ambiciózus joghallgatókkal együttműködve, évről évre programjára tűz egy-egy aktuális kutatási témát, amely az infokommunikációs jog és az új technológiák jogi szabályozásával kapcsolatban újszerű, és amely foglalkoztatja a nemzetközi jogtudományi gondolkodást.

A 2016-2017-es akadémiai évben Tanszékünk kutatását az Igazságügyi Minisztérium a „Jogászképzés színvonalának emelését célzó Programok” keretében támogatta. A kutatási programunk címeként „A (demokratikus) nyilvánosság legújabb szerkezetváltozásának hatása a sajtószabadság tartalmára - változás a változatlanóságban?” címet választottuk. Az eredeti szűk tematikájú lehatároláshoz képest, utóbb szélesebb vizsgálati perspektívát alkalmaztunk. Az Infokommunikációs Jogi Tanszék kutatói a kutatás keretében hat, plurális tematikájú tanulmányt készítettek el, amelyeket jelen kötetben teszünk közzé. Az eredeti kutatási célkitűzés eredményeit „Az online diskurzusok egyes szabályozási kérdései” című tanulmányban foglaljuk össze.

Ebben a kötetet bevezető tanulmányban az internet technológiájának a nyilvánosság szerkezetére gyakorolt hatását vizsgáljuk: elemezzük a közvetlen közzététel technológiája hatására bekövetkezett változást a kapuőrök évszázados szerepkörében, a tartalom- és tárhelyszolgáltatói szerepek egymásba olvadásának folyamatát, a keresőmotorok forgalomirányítói és a közösségi média szolgáltatóinak tartalomszabályozó tevékenységét. A web 2.0 nyilvánosságának sajátosságait, különösen egyes alkotmányjogi és versenyjogi dilemmáit egy-egy, egymás érvkészletét (is) kiegészítő tanulmányban vizsgáljuk. Az alkotmányjogi nézőpontot érvényesítő munkában olyan, jogilag releváns kérdéseket exponálunk, amelyek komoly veszélyeket jelentenek, az egyéni véleménynyilvánítás individuális jogára és a demokratikus diskurzusokra (szűrőbuborék és a fake news jelensége). A versenyjogi elemzésben kitérünk az adatalapú piaci hatalom kérdéseire, a versenyjogot pedig, mint sajtóságos adatvédelmi eszközt mutatjuk be. Külön tanulmány foglalkozik a hálózati és információs rendszerek biztonságára vonatkozó európai szabályozás alapjaival. Ebben részletesen mutatjuk be a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló 2016/1148/EU irányelvet, valamint az elektronikus hírközlési adatvédelmi rendelet-javaslatot. A felhőszolgáltatások (cloud computing) adatvédelmi jogi kérdéseit bemutató tanulmányban elsősorban európai perspektívából vizsgálódunk, kitérünk a felhőszolgáltatásokban rejlő adatvédelmi kockázatokra, az EU-n kívüli harmadik országokba történő adattovábbítások személyes adatokat érintő veszélyeire és a felhőjogviszonyok egyes felelősségtani összefüggéseire is. A cyber-bűnözés információtechnológiai aspektusait vizsgáló tanulmány társszerzőségben készült, annak megírásában joghallgató kollégánk is közreműködött.

A technológia- és cyberjog egyes aktuális kérdéseit felvonultató kötet összeállítása során természetesen nem törekedtünk a teljességre, nem kívántuk bemutatni a téma valamennyi jogilag releváns aspektusát, csupán néhány, a szerzők által azonosított és jelentőségük miatt kiválasztott csomópontot fókuszáltunk.

Az egyéves tanszéki kutatómunka gyümölcseit összefoglaló kötet az Infokommunikációs Jogi Tanszék oktatóinak (Tóth András tanszékvezető egyetemi docens és Klein Tamás egyetemi tanársegéd) és két joghallgatónak a munkája (Bartha Bence két tanulmány elkészítésében

végzett fontos kutatómunkát, Szabó Aliz pedig szerzőtársunkként működött közre). Olvasóink elé azzal a reménységgel tárjuk a témáiban sokszínű, hat tanulmányt tartalmazó kötetet, hogy abban mindenki megtalálja az érdeklődésének megfelelő témakört, valamint bízunk abban is, hogy egy-egy szemponttal hozzájárulhatunk napjaink jogtudományi diskurzusainak pluralitásához.

Ezúton köszönjük az Igazságügyi Minisztérium kutatáshoz nyújtott támogatását.

Budapest, 2017. október 30.

A szerkesztő

Az online diskurzusok egyes szabályozási kérdései

KLEIN TAMÁS*

A nyilvános diskurzusok alkotmányosan igazolható szabályozásának kérdésköre, az elmúlt évtizedek értelmezési kánonjához képest, amely jórészt a kizárólag az államtól való negatív szabadságban ragadta meg a szólás- és sajtószabadság problematikáját, napjainkban egészen új perspektívából vizsgálható. Az internetes nyilvánosság technológiai adottságai és azok társadalmi következményei révén új, részben még meg nem válaszolt kérdések megfogalmazására és válaszok keresésére sarkallja a tudományt és a jogalkotókat.

Az internetes nyilvánosság szabályozási kérdései mélyen gyökereznek sajátosságaiban, ezért röviden kitérek a technológia kérdéseire és az azzal szorosan összefüggő sajátosságokra. Ezt követően három alapvető, a demokratikus diskurzusokban meghatározó jelentőségű és jogilag releváns online platformot emelek be a vizsgáldásom fókuszába, amelyeknél egy-két specifikus szabályozási kérdést részletesebben is elemzek.

1. Az internetes kommunikáció jogi előkérdése – a jogi szabályozhatóság dilemmája

Az internet – bármennyire is katonai célú fejlesztésnek köszönhetjük a létét – mára a modern interperszonális és tömegkommunikáció, valamint az információ szabad áramlásának szimbólumává vált. Az internetes nyilvánosság állami szabályozása tartalmi összetevőinek meghatározása előtt, arra az elméleti előkérdésre kell választ adni, hogy technikailag lehetséges-e és alkotmányos (alapjogvédelmi) szempontból megengedhető-, vagy még inkább szükséges-e az online kommunikációs tér állami szabályozása? A technikai szabályozhatóság kérdés elsősorban nem jogi jellegű, ezért arra nem térek ki. Az alapjogi nézőpontból vizsgált szabályozhatósági vitában alapvetően két nézet csatázik egymással. Az egyik az internet romantikus felfogásaként azt vallja, hogy az internet technológiája által teremtet nyilvánosság a tömegkommunikáció egy minőségileg új korszakát jelenti. A tömegdemokráciákban korábban jelenlévő hozzáférés szűkösségének kérdése végleg megoldódik, hiszen az internet – mint minden idők legdemokratikusabb médiuma – képes megteremteni a politikai diskurzusok korábban soha nem tapasztalt pluralitását. Az internetes nyilvánosság e felfogása okszerűen tagadja az állami szabályozás megengedhetőségét, és azt az online piactér mechanizmusaira bízta. Az erre vonatkozó érvelés szerint, az online vélemények mindenki számára korlátozásmentesen, szabadon hozzáférhető piaca önmagától megoldja a más tömegkommunikációs eszközök esetén jelentkező, az állami szabályozás szükségességét megalapozó problémákat, különösen a hozzáférés korlátos voltát. Mindezek alapján az internet ugyan nem jogmentes terület, de fegyelmező hivatalt, cenzúrát nem tűr.¹ Azok tehát, akik az internet technológiája biztosította nyilvánosságban a szólássza-

* Egyetemi tanársegéd, Károli Gáspár Református Egyetem, Állam- és Jogtudományi Kar Infokommunikációs Jogi Tanszék. E-mail: klein.tamas@kre.hu.

1 POLYÁK Gábor – MAJTÉNYI László: A szabadság hazai hagyományának megtagadása – új médiatörvények Magyarországon. *Közjogi Szemle*, 2011/1. 3–4.

badság utópiájának a megvalósulását üdvözltek, az állami be nem avatkozás korszakát vizionálva elutasították az állami szabályozás alkotmányos lehetőségét. Ezzel szemben realistább az az általunk is támogatott nézet, amely mindamellett, hogy elfogadja az internetes kommunikáció demokratikus fejleményeit, érzékelve az online nyilvánosság társadalmi valóságát és speciális kihívásait, síkra száll az interneten keresztül zajló kommunikáció megfelelő szabályozása mellett.² Ennek megfelelően például a tiltott gyermekpornográfia (vö. Btk. 204. §) nem válik büntetlenné pusztán azért, mert azt nem hagyományos kommunikációs csatornákon keresztül, hanem az interneten, esetleg azon belül is az új médián keresztül terjesztik. Ahogy az interneten megjelenő tartalmak sem egy jogmentes senkiföldjén jelennek meg, úgy az internetes sajtótermékek tulajdonosai sem mentesülnek a más médiumokkal együtt való tulajdonlás esetén, a tulajdonosi korlátoknak való megfelelés kötelezettsége alól: a véleménynyilvánítási monopólium kialakítását az állam az online nyilvánosságban sem köteles eltérni, még ha sokkal kevésbé tűnik ez lehetségesnek az internet esetében. Az azonban már egy további kérdés, hogy az állami szabályozás mennyire képes beváltani a hozzá fűzött reményeket egy olyan szabályozási környezetben, ahol a jogi kötelezettségek címzettjei sokszor globális szolgáltatók, amelyeknek semmilyen, jogilag releváns kapcsolatuk nincs a szabályozni kívánó állammal.

Az internet – amiként arra az Alkotmánybíróság is rámutatott – nem jogmentes terület. Az interneten történő emberi tevékenység – így a kommunikációs tevékenység is –, függetlenül annak technológiai háttérétől, a jogi szabályozás tárgya lehet, nem *terra incognita* a jog számára. Az Alkotmánybíróság az internetes médiára vonatkozó szabályozást a 165/2011 (XII. 20.) AB határozatában, a sajtótermék fogalmának megfelelő körben vizsgálta azzal, hogy mind az alapjogi védelmet kiterjesztette rá, mind pedig a korlátozhatatlanságát visszautasította: „A sajtószabadság kiterjed az internetes sajtó tevékenységére is, azzal, hogy az egyéb tömegkommunikációs formákhoz hasonlóan alkotmányossági értelemben az internetes sajtó is szabályozás alá vonható. E szabályozás differenciált megközelítést igényel.”³ Az Alkotmánybíróság ezt az alkotmányossági normák összefüggésében is megerősítette:

„Az internet nem jogmentes terület, az internetes kommunikációban tanúsított emberi magatartások és formák a jogi szabályozás tárgyát képezhetik. Alkotmányossági szempontból tehát az új technológiák által nyújtott tereken és felületeken, valamint kommunikációs csatornákon – így az interneten zajló nyilvános kommunikációban érvényesítendő az Alaptörvényben rögzített alapvető jogok és kötelezettségek. (...) a blog és komment is közlésnek minősül, s mint ilyen az Alaptörvény IX. cikk védelmi körébe esik”⁴

A szólásszabadság alapjogának érvényesülése alapvető alkotmányos követelmény, függetlenül attól, hogy a konkrét esetben a szólás a nyilvánosság *offline* vagy *online* *terrénumában* valósul meg. Az Alaptörvény I. cikke értelmében az alapvető jogok védelme az állam elsőrendű kötelezettsége. Az állam aktív intézményvédelmi kötelezettségének elsősorban jogalkotás révén (alapjogok esetében kizárólag törvényben) tesz eleget. Az intézményvédelmi kötelezettség teljesítése során a törvényhozó olyan szabályozási környezetet alkot, amely biztosítja az alapjogok érvényesülését mind az állammal szemben, mind a magánviszonyokban, közjogi

2 KOLTAY András – LAPSÁNSZKY András: Az új magyar médiaszabályozás alkotmányossági kérdései. *Iustum Aequum Salutare* VII. 2011/2. 31–141. 41.

3 165/2011. (XII. 20.) AB határozat, ABH 2011. 478. 508.

4 19/2014. (V. 30.) AB határozat, ABH 2014. 439. 453.

(vertikális) és magánjogi (horizontális) jogviszonyokban egyaránt. Amint a későbbiekben részletesen elemzett szabályozási kérdésekből kitűnik, a horizontális alapjogvédelem⁵ intézményeinek kidolgozása az internetes kommunikáció esetén, komoly kihívást jelent.

A szabályozás jövője napjaink egyik legfontosabb kérdése. Olyan új jelenségek, mint a közvetlen közzététel és az abból következő harmadik személyek tartalmáért való szolgáltatói felelősség dilemmája, a keresőmotor-szolgáltatók hagyományos keresési és innovatív prediktív tartalomkínálata, valamint a közösségi médiumok szabályozási mechanizmusai nem kevésbé, mint az új forgalomirányítók tevékenysége a személyre szabott információkínálat következtében újfent megvalósulni látszó (szubjektív) hozzáférési szűkösség, a szűrőbuborék probléma, kivétel nélkül szabályozási kihívást jelentenek. A megválaszolandó kérdésekre adható számos megoldási javaslat megfogalmazása során azonban – úgy vélem –, az alapjog magánjogi jogviszonyokban való érvényesülésének határozottabb alkalmazhatósága szükséges. Ennek a feltevésnek az igazolására is kísérletet teszek a továbbiakban.

2. Az internetes tömegkommunikáció hatása a nyilvánosság szerkezetére

2.1. A technológia hatása

Az internetes kommunikáció elterjedésével olyan új (tömeg)kommunikációs platformok jelentek meg, amelyek kétségkívül jelentősen módosították a nyilvánosság korábban kialakult struktúráját. A technológiai fejlődés következtében az egymás közötti diskurzusoknak és a tömegkommunikációnak is új, korábban nem létező csatornái, közegei alakultak ki.⁶ A tömegkommunikáció szerkezetére gyakorolt hatásában ennek a technológiai változásnak különösen nagy jelentősége van, hiszen a hagyományos nyomtatott és elektronikus média mellett olyan új eszközök elterjedését tette lehetővé, amelyek a korábbi korlátos hozzáféréshez képest bárki számára, szinte teljesen korlátlanra tették a nyilvánossághoz való hozzáférés lehetőségét. Mára nem csupán az online hírportálok, sok esetben az offline világ meghatározó médiumainak online kiadásai, 'klónjai', hanem a többnyire a társadalomban alulról szerveződő, magánkezdeményezésként működtetett fórumok működtetői, a blogszféra és a közösségi média is meghatározó szereplői a hír- és tájékoztatási versenynek, sőt releváns versenytársaivá váltak a hagyományos nyomtatott lapoknak és az offline (lineáris) médiaszolgáltatásnak. Az interneten zajló kommunikációnak ugyanakkor számos, különböző megjelenési formája azonosítható, sőt az egyes közlések alkotmányossági szempontból más-más megítélés alá tartoz(hat)nak. A szabályozásnak ebből fakadóan szükségszerűen differenciált megközelítést, a korlátozhatóság különböző mércéit kell alkalmaznia:

„(...)az internet mint kommunikációs csatorna az emberi kommunikáció egyre változatosabb formáinak lehetőségét teremti meg, amely formák közül egyre több nyilvánvalóan nem sorolható be a

5 A horizontális hatály kérdésének elméleti áttekintéséről l. GÁRDOS-OROSZ Fruzsina: Az alkotmány a magánjogi jogviszonyokban. *Rendészeti Szemle*, 2010/4., 19–34; GÁRDOS-OROSZ Fruzsina: Alapjogok alkalmazása a magánjogi jogvitákban az Európai Unióban és ennek lehetséges hatásai a magyar jogra. *Állam- és Jogtudomány*, 2010. 225–258.

6 Sándor UDVÁRY: Media revolution – Effects of technological development on freedom of expression. In: Mátyás KAPA (szerk.): *Studia Iuridica Caroliensia* 2. Budapest, Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, 2007. 197–215.

tömegkommunikáció fogalmi körébe, így ezekre nem irányadók a sajtó szabályozásánál meghatározó szempontok. A magáncélú közlések, honlapok, blogok, közösségi portálok stb. nem kezelhetők együtt a tömegek tájékoztatását vagy szórakoztatását célzó internetes újságokkal, hírportálokkal (...)”⁷

Vannak tehát olyan internetes közlések (elsősorban az azokat formulázó személyi körre tekintettel), amelyek a sajtószabadság, mások azonban a szólásszabadság alapjogának védelme alatt állnak. Annak az eldöntése, hogy a konkrét platformon és formában közzétett tartalom mely alapjog oltalmát élvezi, különösen nagy jelentőséggel bír, tekintettel arra, hogy a kommunikációs jogok csoportjába tartozó egyes szabadságjogok bizonyos megnyilvánulásaiból különböző védelmi szintek és mércék következnek.

A sajtószabadság fogalmának az új technológiára, az internetes kommunikációra való vonatkoztatása során tehát alapvető definíciós kérdésként szükséges megvizsgálnunk, hogy mely internetes megnyilvánulásokat sorolunk a sajtó-, és melyeket a szólásszabadság alapjogának tartalmi körébe. Az egyik leegyszerűsítő értelmezés szerint a sajtószabadság nem más, mint a tartalom közzétételének, továbbításának szabadsága, tehát a sajtónak mint a közlések hordozójának, továbbítójának (eszközjellegű funkció) védelmét jelenti. Ebből a felfogásból kiindulva akár valamennyi közlést továbbító, tartalmat közzétevő webes felület a sajtószabadság alanyi körébe vonható és így „sajtónak” tekinthető. Ez a megközelítés álláspontunk szerint azonban túl tágan határozza meg a sajtó fogalmát, ami értelmezésbeli zavarokat okozhat. A sajtószabadság tartalma eltérő funkciója okán, a szólásszabadsághoz képest eltérő jogokat és kötelezettségeket tartalmaz, privilégiumok és tartalomszabályozási előírások, bizonyos körben szigorúbb felelősségi szabályok gazdagítják. Ebből fakadóan alapjogvédelmi konzekvenciái vannak annak a döntésnek, hogy egy online eszközt a szólás- vagy a sajtószabadság hatálya alá tartozóként azonosítunk. A sajtószabadságnak egy jelentősen szűkebb értelmezése figyelembe veszi az alapjog társadalmi valóságát, és kizárólag az olyan tömegkommunikációs eszközöket sorolja e körbe, amelyek professzionális, meghatározott törvényi feltételeket megvalósító módon működnek. Ezen az úton jár a magyar törvényi szabályozás⁸ is, amely a hagyományos és modern tömegkommunikációs eszközök közül csak egyes, a törvényben foglalt feltételeket kielégítő instrumentumokat von a sajtó(termék) és a médiaszolgáltatás, s így implicite a sajtószabadság⁹ fogalmi körébe.¹⁰

7 165/2011. (XII. 20.) AB határozat, ABH 2011. 478, 508.

8 A sajtószabadságról és a médiatartalmak alapvető szabályairól szóló 2010. évi CIV. törvény (a továbbiakban: Smtv.), és a médiaszolgáltatásokról és a tömegkommunikációról szóló 2010. évi CLXXXV. törvény (a továbbiakban: Mttv.).

9 Alaptörvény IX. cikk (2) bekezdés, Smtv. (8. lj.) 4–9. §.

10 Smtv. (8. lj.) 1. § 6. pont. Sajtótermék: a napilap és más időszaki lap egyes számai, valamint az internetes újság vagy hírportál, amelyet gazdasági szolgáltatásként nyújtanak, amelynek tartalmáért valamely természetes vagy jogi személy szerkesztői felelősséget visel, és amelynek elsődleges célja szövegből, illetve képekből álló tartalmaknak a nyilvánossághoz való eljuttatása tájékoztatás, szórakoztatás vagy oktatás céljából, nyomtatott formátumban vagy valamely elektronikus hírközlő hálózaton keresztül. A szerkesztői felelősség a médiatartalom kiválasztása és összeállítása során megvalósuló tényleges ellenőrzésért való felelősséget jelenti, és nem eredményez szükségszerűen jogi felelősséget a sajtótermék tekintetében. Gazdasági szolgáltatás az önálló, üzletszerűen – rendszeresen, nyereség elérése érdekében, gazdasági kockázatvállalás mellett – végzett szolgáltatás. Smtv. 1. § 1. Médiaszolgáltatás: az Európai Unió működéséről szóló szerződés 56. és 57. cikkében meghatározott, önálló, üzletszerűen – rendszeresen, nyereség elérése érdekében, gazdasági kockázatvállalás mellett – végzett gazdasági szolgáltatás, amelyért egy médiaszolgáltató szerkesztői felelősséget visel, amelynek elsődleges célja műsorszámoknak tájékoztatás, szórakoztatás vagy oktatás céljából a nyilvánossághoz való eljuttatása valamely elektronikus hírközlő hálózaton keresztül. Az Smtv. sajtótermék és médiaszolgáltatás fogalmait az Mttv. is megismétli (Mttv. 203. § 60. pont és Mttv. 203. § 40. pont).

Az alkotmányos védelem (szintje) természetesen nem tehető függővé egy törvényi fogalom meghatározástól, de a sajtót érintő állami szabályozás és felügyelet normáit kétségkívül meghatározhatja a törvényi szabály, amely normákat az állam intézményvédelmi kötelezettsége körében köteles is megalkotni. Törvényi szabály nem állapíthatja meg a sajtószabadság szűkebb érvényesülési körét, mint ami az Alaptörvénybe foglalt alkotmányos normából következik. A szabadságjog védelmi övezetére tehát úgy hatnak a törvényi előírások, hogy – az alapjog az alkotmányosan megengedett korlátozhatóság keretei között – negatív előírásokkal definiálják a gyakorolhatóság peremfeltételeit.

A nyilvánosság alapvető struktúrájában az elmúlt egy évtizedben bekövetkező és napjainkban is egyre gyorsuló ütemben végbemenő kvantitatív és kvalitatív változások, a technológia következtében átalakuló kommunikációs tér, jelentékeny hatással bírnak a szólás- és sajtószabadság érvényesülésére, lényegesen meghaladva a változásoknak a folyamat kezdetén prognosztizált mélységét.¹¹

2.2. A kapuőrök alkonya?

A következő kérdés, hogy a mások véleményét közzétevő, az interneten végbemenő, széles körű társadalmi folyamatot elősegítő szolgáltatók, amelyek meghatározó szerepet játszanak a (potenciálisan) minden korábbinál plurálisabb nyilvánosság megvalósulásában, milyen elbírálás alá esnek? Különös tekintettel terheli-e őket felelősség (és ha igen, milyen, ha nem, miért nem) a harmadik személyeknek általuk üzemeltetett felületeken elhelyezett tartalmaiért? Ez a kérdés az internetes tömegkommunikáció kezdeti időszakában nem merült fel, hiszen hosszú ideig a webes technológia szabta keretek között nem volt mód közvetlen közzétételre, legfeljebb e-mail formájában, amely kétségkívül nem is jelent(ett) klasszikus értelemben vett 'közzétételt', és nem felel meg a tömegkommunikáció sajátos kritériumainak sem. Ez sokkal inkább az interperszonális kommunikáció egyik formája, amely tipikusan bipoláris (kivételes, példának okáért körüzenet esetén lehet multipoláris), s akkor a (tartalom)szolgáltató a nyilvánosságban megjelenő valamennyi tartalom tekintetében egyfajta szűrő, kapuőr szerepet tölthetett be. A kilencvenes esztendők közepéig tehát csak olyan közlések jelenhettek meg a webes nyilvánosságban, amelyeket a szolgáltató valamilyen formában, de mindenkor saját tevékeny közreműködése segítségével (aktív, szerkesztői lépéssel) közzétett. A harmadik személyek által közvetlenül elhelyezhető tartalmak technológiájának megjelenésével (elsősorban idesorolhatók a kommentek elhelyezését lehetővé tevő oldalak) a szolgáltatóknak ez a közzétételi monopóliuma és az abból fakadó feltétlen zsilipelő szerepe már nem volt abszolút, képződ(het)tek olyan tartalmak, amelyekkel megjelenés előtt nem került kapcsolatba a szolgáltató. Az internetes kommunikáció legújabb szerkezeti átalakulásával, a *web 2.0* megjelenésével pedig a tartalomszolgáltatók ezen kapuőr szerepe értelmetlenné, vagy kevésbé erős ítéletet mondva, súlytalanná kezd válni. Abban az új társadalmi nyilvánosságban, amelyben a tömegkommunikációs tér egy meghatározott szegmentumában (az internetes kommunikációban) a közzététel automatikus, közvetlen, mindenféle közvetítői beavatkozástól független, a korábbi kapuőrök, elvesztve addigi évszázados szűrő funkciójuk lényegét, lassan nyugdíjba

11 Sándor UDVARY: Digital revolution. Effects of technological development on freedom of expression. *Collega*, 2007/2–3. 331–341.

kényszerülnek. A funkció azonban új köntösben és részben új tartalommal újra megjelenni látszik az új technológiákban, így új kapuőrök kezdik átvenni ezt a feladatot, úgy, mint a keresőmotor szolgáltatók, a social media üzemeltetői vagy éppen az internetszolgáltató ISP-k.¹²

A kapuőri szerepkör annak ellenére, hogy az egyes közlések, információk publikálása már közel sem mindig egy klasszikus sajtótermék vagy médiaszolgáltatás közbejöttével történik, mégsem válik teljesen meghaladottá. A kapuőri feladat természete, jellege, funkciója, a kapuőr 'munkaköri leírása' azonban alapvetően megváltozik. Még az internetes felületeken sem válik ugyanis minden tartalom esetén súlytalanná, okafogyottá a szolgáltatóknak ez a szűrési tevékenysége/funkciója, jelentősége megmarad azokon a területeken, ahol a közzétett információ hitelessége kulcsfontosságú, ugyanis bizonyos tartalmaknak egészen egyszerűen nincs értéke a hitelesség biztosítása nélkül.

Nilvánvalóan ilyen tevékenység a hírszolgáltatás. A hírek hitelessége, tartalmuk megbízhatósága a befogadó számára magától értetődően értékes, hiszen senki nem akar kétes hitelű, vagy egyenesen „kacsa” híreket, blöfföket olvasni. Mindezt nem teszi zárójelbe az a körülmény, hogy napjainkban elterjedtek a kifejezetten groteszk valóságértelmezési vagy nyíltan téves híreket közlő, a valóságot szándékosan félreértelmező narratívát megjelenítő internetes oldalak, „álhírlapok”. Az információk hitelességének fontosságát számos esetben várjuk el a kapuőröktől, így példának okáért a pénzpiacra befektetési stratégiánkat jobb szíjjal igazítjuk egy jó bonitással rendelkező, elismert gazdasági szaklap, honlap stb. híreihez és az azokból alkotott elemzéseihez, mint egy ismeretlen prókátor csodát ígérő prófécijához. Ugyanez áll a tudományos közleményekre is, amelyek esetében szintén meghatározó (a tudomány elismertségének biztosítása érdekében pedig parancsoló) követelmény a hitelesség. A nemzetközi tudományosságban a *peer-review* intézménye – elvileg – biztosítja ennek a várakozásnak a megfelelő teljesülését. Természetesen a professzionális, nagy tekintélyű (szak)médiumok vagy éppen a tudományos nyilvánosság elismert fórumain is előfordulhatnak visszaélések, csalások, ám ezek a botrányok éppen a hitelesség fontosságára irányítják rá a szakmai közvélemény figyelmét. A kapuőr általánosságban tehát már nem élvez kiváltságot, már nem rendelkezik azzal a monopóliummal, hogy csak rajta keresztül, az ő ellenőrzésre lehetőséget biztosító szűrői tevékenysége után juthat el a közlés a nyilvánosságba. Mindazonáltal a tudományos nyilvánosságban napvilágot látott visszaélések arra is rámutatnak, hogy a *peer-review* hitelessége is megkopni látszik. Mindennek ellenére úgy vélem, hogy a nyilvánosság szerkezetváltozása dacára (egyes területeken különösen) nem válik meghaladottá az intézményi szűrés, a kapuőröket tehát nem lehet végleg nyugdíjazni, hanem a nyilvánosság azon szegmenseiben, ahol van értéke a közlés hitelességének, szigorúbb követelményeket lehet a kapuőrökkel szemben megfogalmazni, elsősorban azt az elvárást, hogy tegyék 'korrupciómentessé' az őrzést, biztosítsák az általuk közzétett, közvetített információk hitelét.

A blogszférában, amely elsősorban a szabad véleménycsere kitüntetett virtuális terepe, az imént felvillantott, klasszikus intézményi szerep mára szinte teljesen megszűnt.

Az internetes tömegkommunikációnak új műfaja a komment, a valamely (általában szerkesztett) tartalomhoz fűzött véleményt, álláspontot tartalmazó reflexió. Az internetes nyilvánosságnak ez a lehetősége radikálisan növelte a korábban (a kapuőrök által ellenőrzött) meg lehetőségen szűkös és csupán intézményes keretek között megvalósítható hozzáférés esélyét.

12 Internet Service Provider [access provider, mailbox provider, hosting IPSs, transit IPSs, Virtual IPSs (VIPS), Free IPSs. Wireless IPS (WISP)].

A későbbiekben kitérek arra, hogy a platformszolgáltatók tevékenysége miként korlátozza a hozzáférés lehetőségét.

2.3. A szolgáltatók tevékenysége és differenciálódása

A blogsféra alapvetően megkettőzi valamennyi szolgáltató tevékenységi körét, tekintve, hogy a blogot fenntartó üzemeltető egyszerre tartalomszolgáltató (saját maga tesz közzé tartalmakat) és kvázi tárhelyszolgáltató (a saját tartalmához biztosítja az olvasók reflexióinak közzétételét, véleményének elhelyezését, tehát ebben a vonatkozásban helyet, platformot biztosít a közlés megjelenésére). Az így kialakuló kommunikációs szisztémában piramisszerűen kapcsolódik egymáshoz tartalom- és tárhelyszolgáltató, számos tartalomszolgáltató nyújt tárhelyet másoknak. A blog üzemeltetője, fenntartója, 'szerkesztője' (bár utóbbi fogalom megtevesztő lehet) a saját maga közlései vonatkozásában tartalomszolgáltatóként, míg a harmadik személyek által elhelyezett tartalmak vonatkozásában kvázi tárhelyszolgáltatóként, vagy talán pontosabban, közvetítő szolgáltatóként jelenik meg. A számos fogalmi bizonytalanság egyikeként érdemes utalni arra, hogy annak a szolgáltatónak a tevékenysége, amelynek a tartalmához kommenteket fűznek, bizonytalan jogi megítélés alá esik. Bizonyos szempontból tekinthető a technológiai tekintetben informatikai jelekből álló komment elhelyezésére tárolási helyet biztosító speciális 'tárhelyszolgáltatónak', a tömegkommunikációs folyamatban betöltött szerepére tekintettel, funkcionálisan megközelítve a kérdést viszont közvetítő szolgáltatónak, akinek csupán az a feladata, hogy a kommentet mint tartalmat érzékelhetővé és megismerhetővé teszi, közvetíti a nyilvánosság felé (ám nem ő a szerzője, és vele kapcsolatban semminemű szerkesztői tevékenységet sem végez, csupán felületén mechanikusan közvetíti). A közvetítő szolgáltatás keretében végzett *hosting* tevékenység álláspontunk szerint nem szűkíthető le a szerver szolgáltatásra, hanem az kiterjeszthető azokra a saját tartalmaik tekintetében tartalomszolgáltatónak minősülő szolgáltatókra is, akik másoknak lehetőséget biztosítanak saját felületükön történő diszkusszióra, lényegében mindazokra, akik a társadalmi vitának egy új, technológiaspecifikus térréumát fenntartják.

2.4. A jog kihívásáról általában

A nyilvánosság tehát az elmúlt egy évtizedben olyan szerkezetváltozáson ment keresztül, amelyben szükségszerűen kell újragondolnunk a sajtójog évszázados fogalmi kereteit és a hozzá kapcsolódó alkotmányos mércéket. A régi keretek közül kvantitatívan (a kommunikációra rendelkezésre álló nyilvánosság mérete, befogadóképessége és átvételi potenciálja exponenciálisan növekedett), de még inkább kvalitatívan kilépő, új struktúrájú társadalmi nyilvánosságban jelen lévő kommunikációs eszközök, csatornák hatására a rájuk alkalmazott, de egy korábbi fejlődési szinten kiérlelt fogalmak jelentése szükségszerűen átalakításra, finomhangolásra szorul az alkotmányos elvek rigorózusa és belőlük deriválható kritériumok lényegének megtartása mellett. Az internetes tömegkommunikációval a jog (saját régi fogalmainak foglyaként) sokszor nehezen tud mit kezdeni. A joggyakorlat sok esetben nem tudja a régi szabályokat az új keretek között alkalmazni, a jogi szabályozás pedig rendszerint csak kullog a technológiai fejlődés által támogatott társadalmi valóság nyomában. A jogi szabályozás tehát kizárólag

ott próbál több-kevesebb sikerrel, *ad hoc* jelleggel belépni, utánkövetéssel akadálymentesíteni, ahol hirtelen 'sűrűsödési probléma' jelentkezik. Bár számos megoldandó probléma észlelhető az internetes nyilvánosságban, napjainkban még részlegesen látszanak csupán a nemzeti jogalkotók által választható szabályozási modellek. Vannak olyan kérdések (pl. keresőmotor-szolgáltatások, tárhelyszolgáltatások), amelyekben az uniós jognak köszönhetően megközelítően egységes szabályozás jellemző (*notice and take down* eljárás), de olyanok is, ahol azonos problémára teljesen különböző válaszok születtek (keresőmotor-szolgáltatók felelőssége a keresési találatokért). A közösségi hálózatok esetében a jogi szabályozás teljes hiánya jellemző, miközben a szolgáltató mélyreható szabályozást valósít meg az általa fenntartott platformon.

Természetesen az interneten működő nyilvánosság szabályozási területén különös jelentősége van a *ius – non ius* elhatárolás kérdésének; meddig szabályozzon a jog, és honnan kapjon szerepet az ön- és társszabályozás. Erre a jogelméleti kérdésre azonban jelen írásban nem térek ki.

3. Az internetes kommunikáció sajátosságai

Az offline tömegkommunikációs szférához képest az internetes kommunikáció eltérő karakterisztikus sajátosságokkal rendelkezik. Ezek a sajátosságok kétségkívül kötődnek az adott technológiához, a technológia által determináltak. Az internetes technológia teremtette nyilvánosságban megjelenő közlések két, karakterisztikus jellemzője az anonimitás és az információáramlás határok nélkülsége. Bár az offline környezetben is volt lehetőség a személyazonosságot fel nem fedő, anonim megnyilvánulásokra, és az információk terjesztése korábban sem volt feltétlenül tekintettel az országhatárookra, mégis, az internetes közzététel mennyiségileg és minőségileg is új módon jellemzi az internetes kommunikációt. További sajátossággént szükséges megemlíteni az interneten megfigyelhető vitastílus rendkívül nagy amplitúdóját, a megszólalások formai pluralitását.

3.1. Anonimitás

Az interneten megjelenő megszólalások nagy része azonosíthatatlan forrásból, ismeretlen szerzőtől származik. Az anonimitás magától értetődőségéről azonban megoszlanak a vélemények: vannak, akik szerint a név nélküli, álneves megszólalás a világháló természetéből és szabadságából fakadó jelenség, mások úgy gondolják, hogy mint a nyilvánosság bármely más fórumán, az interneten is főszabály alóli kivételként jelenhet meg.

Az anonimitás mindazonáltal az internetes világban minden ellenkező feltételezés ellenére az esetek többségében csak látszólagos, és kizárólag a felhasználók közötti relációban értelmezhető feltétlenként. Az IP-cím alapján ugyanis mind a tárhelyszolgáltató, mind az internetszolgáltató, bűncselekmény esetében pedig a nyomozó hatóság is azonosítani tudja a felhasználót.¹³ A magánjogi jogviszonyokban, polgári jogi igények érvényesítése esetében azonban erre az azonosításra értelemszerűen nincs lehetőség.

13 Sok esetben előfordulhat, hogy a felhasználó IP-cím alapján nem azonosítható, ám ha saját eszközről csatlakozik a hálózathoz, akkor jó eséllyel összekapcsolható a tartalommal az eszköz MAC-címe alapján. A MAC-cím (Media Access Control Address) egy hexadecimális azonosító számsorozat, amellyel még a gyártás során látják el a hálózati kártyákat.

Ezzel együtt is az anonimitás napjainkban tapasztalható jelensége egy technológiai következmény, hiszen a nyilvánossághoz való hozzáférés egy gép közbejöttével valósul meg, amely nem szükségszerűen azonosítja a felhasználó személyt.¹⁴ Másfelől az internet felépítése – amint erről már szoltunk – szintén kedvez az azonosíthatatlanságnak, tekintettel a globális, államhatárokat negligáló természetére.

Ebben a technológiai adottságban az anonimitás egyfajta társadalmi szokássá is vált, az emberek a való világban rendszerint azonosítják magukat, míg az internetes kommunikáció gyakorlata egészen mást mutat. Míg az anyagi világban mindenkinek tipikusan egy személyazonossága van, addig a virtuális valóságban a valódi személyazonossággal párhuzamosan egy, vagy akár több digitális személyazonossága is lehet.

A szerző anonimitásából azonban következik egy alapvető jogi probléma. Amennyiben a szerző kiléte ismeretlen, ám az általa közzétett tartalom jogellenes, úgy kérdéses, hogy ki viseli az érte járó felelősséget? A jogellenes tartalmakhoz való viszonyrendszerben egy adott személy háromféle pozíció valamelyikében lehet. A három reláció értelmében: vagy nincs felelőssége az adott jogellenes tartalomért, vagy éppenséggel őt terheli a felelősség, egyes speciális esetekben pedig – különösen, amikor a jogellenes magatartás tényleges megvalósítójának személye nem állapítható meg – helytállni tartozik az *iniuriáért*. A jogellenes tartalom szerzőjének a kiléte számos esetben nem állapítható meg akkor, amikor egy tárhelyszolgáltató megszólalási lehetőséget, tárhelyet biztosít másoknak, hiszen közülük potenciálisan sokan nem lesznek azonosíthatóak.

3.2. Határok nélkülség, decentralizált hálózat

Az interneten zajló kommunikáció további sajátossága, hogy nincs tekintettel az állami szuverenitás területi korlátaira. Az internetes hálózatok globális működése olyan, az egész földgolyót behálózó rendszert alkot, amelyre lokális, nemzeti, állami szinten csak nagyon korlátozott mértékben van mód befolyást gyakorolni.

A technológia lényege a decentralizáltsága, vagyis, hogy különböző infrastruktúrák által létrejött centrumok, csomópontok alkotják, amelyeknek nincs centruma, nincs a rendszerben egy végső központi szuperszámítógép (szerver) vagy program, amely az egész rendszert egy meghatározott központból irányítaná. Az internet egymással lazán összekapcsolt hálózatok összessége, s mivel nincs egy megragadható magja, ellenőrzése is sokkal nehezebb, mint más platformoké. Nincs olyan központ tehát, amelynek a kontrolljával befolyásolni lehetne az információáramlást. Ez azonban nem jelenti azt, hogy egyáltalán nem lehet külső forrásból kontrollálni, befolyásolni a globális forgalomirányítók tevékenységét vagy éppen a tartalmakat.

14 Az anonimitás jelensége a sajtó megjelenése óta jelen van a nyilvánosságban. Az egykori hírlapi gyakorlat szerint a cikk írója nem jegyezte névvel írását, de az azonosíthatatlanság (volt) a célja az írói álnevek használatának is, hiszen irodalmunk nagyjai közül sokan nem akarták irodalmi munkásságukkal elismert reputációjukat hírlapi publicisztikájuk esetleges megosztó volta miatt kockára tenni. Másfelől a név nélkül vagy álneven megjelent hírlapi tartalmakért a kiadó felelőssége fennállt, így azok jogellenessége esetén, még a tényleges szerző személyének ismerete nélkül (azonosíthatatlansága esetén) is érvényesíteni lehetett a jogsértés következtében keletkező alanyi jogi igényt. Az online anonimitás során, tárhelyszolgáltatás esetén azonban nem feltétlenül van olyan jogalany, akivel szemben a kiadóhoz hasonlóan lehetne igényt érvényesíteni.

3.3. Az online diskurzusok kulturálatlansága

Az online kommunikáció jellemzője továbbá a vitastílus esetenkénti trágársága, ami többek között a hozzáférés széles körű lehetőségéből fakad. Az internetes nyilvánossághoz való hozzáférés egalizáló funkciója miatt olyanok is képesek véleményartikulálásra, akik korábban a fentebb már jelzett korlátok miatt, képtelenek voltak álláspontjukat a közbeszédben megjeleníteni. A megszólalások színvonalának színes kaleidoszkópját jól jellemzi, hogy a magas tudományos színvonalú elemzések és az azokat jellemző fogalmazásmód csakúgy megtalálható az internetes szólások piacán, mint a brutálisan trágár, sokak megbotránkozását kiváltó megszólalások. Az interneten zajló diskurzusok durvasága nyilvánvalóan több okra vezethető vissza. Ezek közül kiemelkedik az anonimitás lehetősége, hiszen a megszólaló annak tudatában fejezheti ki magát, választhatja meg stílusát, hogy személyazonossága ismeretlen marad. Egy másik, nem elhanyagolható forrásvidék azonban, hogy az 'újrademokratizált' társadalmi diskurzusokban – ahol a hivatalos média-szervezeteken kívül, sőt, sok esetben azok ellenére – az állampolgárok széles rétegei kapcsolódtak be a korábban a politikai elit és a magasán kvalifikált újságírói társadalom által monopolizált nyilvánosságba. A társadalom legkülönbözőbb csoportjainak internetes kommunikációban való részvétele során, kapuőrök hiányában ugyan javul az egyenlő hozzáférés, de egyúttal szembeötlő a diskurzusok, az érvelés színvonalának, a kifejezésmód, a stílus hanyatlása, a kulturálatlan, az ízléstelen, vulgáris, obszcén megszólalások gyakorisága. Ezt a jelenséget sokan kimért távolságtartással, elegáns közönnyel, mások azonban elemi felháborodással szemlélik, és követelik a helytelen nyelvhasználat (*inappropriate use of language*) által megmérgezett online tér kifertőtlenítését. Utóbbi álláspont azonban nézetünk szerint nem tartható, kifejezetten elitista megközelítés, és az egyenlő hozzáférés ellen hat, mintegy belső kirekesztést alkalmazva a társadalom kevésbé iskolázott, így nyilvánvalóan kevésbé választékosan fogalmazó tagjaival szemben. Egyes kutatók a kulturálatlan beszédmód online térből történő száműzését belső kirekesztésnek, vagy egyenesen az alapjog alkotmányos kisemmizésének tekintik.¹⁵ Másfelől azt is látni kell, hogy önmagában a stílus alacsony színvonala nem jelenti egyúttal a tartalom jogellenességét, és fordítva: az emelkedett stíl, a szofisztikált kifejezésmód is hordozhat súlyosan jogellenes tartalmat. A közlés stílusa lehet bántóan nyers, sokak számára zavarba ejtő vagy egyenesen megbotránkoztató, önmagában az ilyen szólások még nem adnak alapot a szabad véleménynyilvánítás korlátozására. Amint azt az Alkotmánybíróság is kifejtette 32/1992(V. 29.) AB határozatában: „[a] szabad véleménynyilvánításhoz való jog a véleményt annak érték- és igazságtartalmára tekintet nélkül védi”, a korlátozásnak tartalomsemlegesnek kell lennie, hiszen a korlátozhatóságot alkotmányosan kizárólag külső korlátok igazolhatják. A megújuló nyilvánosságban is érvényes, hogy az Alaptörvény „(...) a szabad kommunikációt – az egyéni magatartást és a társadalmi folyamatot – biztosítja, s nem annak tartalmára vonatkozik a szabad véleménynyilvánítás alapjoga. Ebben a processzusban helye van minden véleménynek, jónak és károsnak, kellemesnek és sértőnek egyaránt – különösen azért, mert maga a vélemény minősítése is e folyamat terméke (...)”.¹⁶

A társadalmi diskurzusok vitastílusának ambivalens voltát jól érzékelteti két, a Stanford Egyetem elsőéves színes bőrű hallgatói ellen irányuló online megszólalás stílusa és tartalma között érzékelhető feszültség. Az egyik hozzászóló, aki ékesszóló stílusról tett tanúbizonyságot, az alábbi hozzászólást jegyezte:

15 Vö. Iris M. YOUNG: *Inclusion and Democracy*. New York, Oxford University Press, 2000.

16 30/1992. (V. 26.) AB határozat.

„LeVon, ha nehéznek találod az itteni egyetemi órákat, tudd, hogy az nem a te hibád. Mindössze arról van szó, hogy a megerősítő intézkedés (*affirmative action* – K. T.) bomlasztó politikájának kedvezményezettje vagy, amely nem megfelelő képesítéssel, felkészültséggel és tehetséggel rendelkező fekete hallgatókat, ehhez hasonlóan magas követelményeket támazstó oktatási intézménybe helyez. A politika egalitárius célkitűzése jó szándékú, azonban alapvetően téves, figyelemmel arra, hogy az alkalmassági vizsgálatok alapján az afrikai-amerikai hallgatók szinte kivétel nélkül az átlag alatt teljesítenek, még a szocio-gazdasági különbségek korrigálása esetén is. Az igazság az, hogy nem itt van a helyed, az egyetemi éveid pedig hosszadalmas és folyamatos lecsúszást jelentenek majd.”¹⁷

Ehhez képest egy másik megszólaló sokkal szimplifikálabb stílusban adott hangot álláspontjának: „Felejs már el, dzsungelnyuszi!”¹⁸

Első pillantásra az első kijelentés együttérző és indokolt gondolatmenetnek tűnhet, valójában azonban rasszista és rendkívül kegyetlen. A jóindulatú egyetemi és munkahelyi etikai szabályok azonban valószínűleg csak a második kijelentésre csapnának le. Amennyiben a fenti két hozzászólást komment formájában vagy egy közösségi platformon tennék közzé, gyanítható, hogy ugyancsak a második megszólalás váltaná ki a platform üzemeltetőjének reakcióját. A kifinomultabban fogalmazó, jobb szociális és verbális készségekkel rendelkező beszélő effajta privilegizálása kapcsán, ismét felvetődhet a belső kirekesztésnek és a „szenvtelen, ésszerű, bizonyítékra támaszkodó” beszélő privilegizálásának a kritikája.¹⁹

Az agresszív, kulturálatlan beszédmód internetes terjedését sokan a technológiából fakadó anonimitásnak tulajdonítják, bár vannak olyan kutatások is, amelyek ezt a hipotézist cáfolják, és azt állítják, hogy nem helyénvaló fogalmazásmódot, sértő, gyalázkodó támadásokat azonos valószínűséggel tesznek közzé a magukat azonosítók és a rejtett vagy hamis személyazonosságot használók is.²⁰ A társadalomban szaporodó antiszociális megnyilvánulásoknak nem kifejezetten a személy azonosíthatatlansága az indikátora, sokkal inkább egy társadalmi elidegenedési folyamat része, amelyben a társadalom tagjai (érzelmileg) fokozatosan távolodnak azoktól a társadalmi struktúráktól és az azokat jellemző értékektől, amelyek korábban bizonyos fokú disztinkváltságot követeltek meg tőlük a kommunikáció során. Így a trágár kifejezésmód és az agresszív vitakultúra általános jelenségével állunk szemben, amelynek csak egy új kifejezési eszköze az anonim internetes közzététel lehetősége.

4. A tárhelyszolgáltató felelőssége a harmadik személyek jogellenes tartalmaiért – Az érdekek összebékítésének nemzetközi modelljei

Bár hazánkban még nem született megnyugtató megoldás a harmadik fél jogellenes tartalmáért való (tárhely)szolgáltatói felelősség körében, mégis, a probléma megoldására számos jól

17 Ian CRAM: Kulturálatlan? Érvek az „ízléstelen”, a tiszteletlen és a névtelen internetes véleménynyilvánítás védelmében. In *Medias Res*, 2015/1. 20. fordító neve (LVP) – Ipso Iure Fordítóiroda, lektorálta Reményi Édua Vénusz.

18 Uo.

19 Uo.

20 L. Richard DAVIS: *Politics Online: Blogs, Chatrooms, and Discussion Group in American Democracy*. New York, Routledge, 2005.

működő példát dolgoztak ki a nemzeti jogalkotások. Úgy vélem, hogy az Alkotmánybíróság 19/2014. (V. 30.) AB határozatából kiolvasható értelmezés sok tekintetben tévúton jár és korrekcióra szorul.²¹

A hagyományos sajtójogi gondolkodás, amely a klasszikus fogalmakkal operált (kiadó, műsorszolgáltató stb.), az analógia és a logika alapján is egyértelműen a közlésnek teret biztosító tárhelyszolgáltató felelősségét alapozta volna meg. Ez a szemlélet azonban nem vette figyelembe azt a speciális viszonyt, amely a felhasználó közvetlen közzétételi lehetősége és a tartalomnak felületet biztosító szolgáltató között fennáll. Napjainkra körvonalazódik az internetes szolgáltatók harmadik személyek tartalmáért viselt polgári jogi felelősségének néhány olyan modellértékű jellemzője, amelyek az egyes nemzeti jogalkotásokban különböző hangsúlyokkal, de konstans módon megjelennek.²² Az amerikai kontinensen (USA) egy 1996-os törvény, a *Communications Decency Act* (CDA), míg az Európai Unióban az Elektronikus Kereskedelemről szóló 2000/31/EC irányelv rendelkezett a tárhelyszolgáltatók felelőtlenségéről, vagy helyesebben feltételes felelősségéről. A CDA-t, pontosabban annak vonatkozó, 230. szakaszát sokan „az internetes tömegkommunikáció Első Alkotmánykiegészítésének” tartják.

Az amerikai megoldás, amely talán elsőként szabályozta a tárhelyszolgáltatók felelősségét – amint arra már utaltam –, a könyvárusítók responzibilitásához (*booksellers liability*) hasonló konstrukciót dolgozott ki. Az analógia nem véletlen, hiszen a könyvesbolt tulajdonosa sem ismerheti valamennyi polcain árult *opus* tartalmát, s így azokért felelősséggel sem tartozhat. Az azonban már elvárható a könyvek árusításával foglalkozó kereskedőtől, hogy amennyiben a részére egy hivatalos megkeresés (*legal notice*) érkezik, amelyből értesül valamely általa árusított könyv (véltetően) jogsértő tartalmáról, azt haladéktalanul vegye le a polcáról, szüntesse be annak további forgalmazását. Lényegileg ennek megfelelő szabály az eredetileg a szerzői jogban bevezetett,²³ de utóbb a tárhelyszolgáltatókra is kiterjesztett *notice and take down* típusú felelősség.

A könyvárusók felelősségi konstrukciójának alkalmazása megnyugtató megoldásnak bizonyult az esetek többségében, ám voltak olyan szolgáltatók, akikkel szemben méltánytalan döntéshez vezetett. Azokban az esetekben, amikor a szolgáltatók valamilyen formában szűrték és automatikusan eltávolították a sértő tartalmakat (például fórumok, hirdetőtáblák stb. üzemeltetői), nem védekezhettek a limitált felelősséggel, hiszen a bíróság az ilyen tevékenységet egyúttal a felelősség felvállalásaként is értelmezte.²⁴ A bírósági gyakorlat, amely kétségkívül megalapozott és védhető elvek figyelembevételével állított fel szigorúbb mércét

21 Vö. KOLTAY András: Az Alkotmánybíróság határozata az internetes kommentek polgári jogi megítéléséről, a tartalomszolgáltató polgári jogi felelőssége a jogsértő felhasználói tartalmakért. *Jogesetek Magyarázata*, 2015/1. 9–21.; GRAD-GYENGE Anikó: Commentare necesse est – Néhány Gondolat az Alkotmánybíróság „Komment-határozatáról”. *Glossa Iuridica*, 2015/2. 122–142.; KLEIN Tamás: A tárhelyszolgáltató „omnipotens” felelőssége, mint alkotmányjogi problematika, A harmadik személy tartalmáért való szolgáltatói felelősség az interneten. In: KOLTAY András – TÖRÖK Bernát (szerk.): *Sajtószabadság és médiajog a 21. század elején* 3. Budapest, Wolters Kluwer, 2016. 347–374.

22 Az egyes modellek kialakulását és lényegét érzékletesen mutatja be: JUDIT BAYER: *Liability of Internet Service Providers for third party content*. Victoria University of Wellington, 2007.

23 GRAD-GYENGE Anikó: Interneten elkövetett szerzői jogi jogsértések és az értesítési és eltávolítási eljárás. In: KISS Daisy (szerk.): *E-akták: Tanulmányok az internetjog világából*. Budapest, Bibó István Szakkollégium Internet-jogi Kutatócsoport, 2003. 171–199.; GRAD-GYENGE Anikó: A forgalomirányítók tevékenységének szerzői jogi kihívásai. *Infokommunikációs és Jog*, 2016/1. 14–16.

24 Vö. *Prodigy-ügy, Stratton Oakmont Inc. v Prodigy Services Co.* 1995. WL 805178 N. Y. Sup. Cr. 1995.

a tartalmakat monitorozó szolgáltatókkal szemben, amellett, hogy méltánytalan helyzetbe sodorta a többletmunkát, az erkölcsileg helyeselhető, a szélsőséges, támadó bejegyzések elleni fellépést mint társadalmi missziót vállaló szereplőket, paradox módon az internetes nyilvánosság mérgezését növelte azáltal, hogy a kockázat minimalizálására törekvő szolgáltatók nem vállalták a nagyobb felelősséget generáló szűrést.

Ezen a kedvezőtlen helyzeten segített a CDA 'jó samaritánus' kikötése (*good samaritan provision*), amely „(...) meghatározó jelentőségű lépésnek bizonyult az amerikai szólásszabadság internetes felületeken való érvényesülése vonatkozásában (...)”.²⁵ A CDA 230. szakasza ugyanis kimondta, hogy egy interaktív számítógépes szolgáltatás szolgáltatója vagy igénybe vevője semmilyen körülmények között nem felelős (mint kiadó vagy közlő) egy másik fél által közzétett tartalomért; „(...) [e]z a határozott nyelvezet az első alkotmány-kiegészítéshez hasonlóan,²⁶ kérlelhetetlen egyértelműséggel menti fel a szolgáltatókat mindenfajta tartalmi felelősség alól(...)”.²⁷ Az amerikai törvényhozás tehát a jó samaritánus klauzulával áthidalta azt a problémát, amely a harmadik felek tartalmát valamilyen formában moderáló s így bizonyos mélységű 'szerkesztői' tevékenységet is végző szolgáltatók társadalmilag hasznos, ám a jogértelmezés következményeként magasabb szintű felelősségét alapozta meg.

A *notice and take down* eljárás – bár lényeges előrelépés a korábbi, a szolgáltatót terhelő szinte korlátlan felelősséghez képest, és rövidtávon, valamint további jogorvoslatot nem engedő, gyorsaságát tekintve azonban mindenképp hatékony megoldást jelent a tárhelyszolgáltató felelősségének limitálása mellett a jogsérelem orvoslására is (*in integrum restitutio*) – alkalmazásával szemben több, (elsősorban elvi jellegű) aggály fogalmazható meg. Magunk itt kizárólag egyetlen, ám kifejezetten fajsúlyos alkotmányossági szempontra hívjuk fel a figyelmet. Az értesítésben foglalt tartalomra vonatkozó jogellenesség gyanújáról (értesítés) való tudomásszerzést követően, a szolgáltatónak kell eldöntenie, hogy a kérdéses tartalom valójában jogellenes-e, és vállalnia kell ennek a jogi minősítést is tartalmazó döntésnek az ódiumát. Bármilyen magatartás, így egy internetes bejegyzés, illetve tartalmának jogellenességét bár végső soron kizárólag a bíróság jogerős ítélete állapíthatja meg, a szolgáltatónak mégis ennek hiányában, saját belátására hagyatkozva kell meghoznia egy jogkérdésről a döntést, vagyis egy jövődó bírósági ítélet tartalmát kell megjósolnia, és kényszerűen minősítenie kell egy közlést anélkül, hogy arra bármilyen tényleges jogi felhatalmazása lenne. Mindezt pedig annak tudatában kell megtennie, hogy e jogkérdés esetleges téves megítélése következtében saját jogi felelősségének megállapíthatóságát teszi kockára. Másfelől azért is aggályos a szolgáltatót ilyen érdemi döntési pozícióba juttatni, mivel az eltávolítás során (megint csak tényleges *iurisdictio*s hatáskör és szakmai kompetencia nélkül) lényegében más, a szolgáltatását igénybe vevő harmadik fél véleménynyilvánítási szabadságát korlátozza.

A rendszer a szolgáltatókat – könnyen belátható módon – arra ösztönözheti, hogy a későbbi jogkövetkezmények elkerülése érdekében, az értesítést követően különösebb megfontolás nélkül, a saját kockázatuk minimalizálása és felhasználóik véleménynyilvánítási szabadságának potenciális sérelme mellett, értesítés esetén azonnal távolítsák el a kérdéses tartalmat

25 Vö. BAYER Judit: *A háló szabadsága. Az internet tartalmának szabályozási problémái a véleménynyilvánítás szabadsága tükrében*. Budapest, Új Mandátum, 2005. 32.

26 Az Első Alkotmánykiegészítéshez való hasonlítás legfeljebb részben, azzal a lényeges megszorítással tartható állítás, hogy a CDA szabályai nem minősülnek alkotmányos normának.

27 BAYER i. m. (25. l.) 32.

(*chilling effect*).²⁸ Az ilyen esetekre bőséges példával szolgál az amerikai gyakorlat, ahol az értesítést küldők sokszor visszaélészerűen gyakorolták ezt a jogukat, és a véleménynyilvánítás szabadsága által oltalmazott, ám velük szemben kritikus bejegyzések eltávolítását kérték. A szolgáltatók számos esetben – tartva az esetleges következményektől –, az értesítésről való tudomásszerzést követően eltávolították a bejegyzést.²⁹

Egy másik észak-amerikai (továbbfejlesztett) megoldás egy kanadai eredetű konstrukció, amely felismerve a *notice and take down* szabállyal szemben felvethető alkotmányossági aggályokat, továbbgondolta azt, és egy kevésbé rigorózus, de az alkotmányossági megfontolásokat talán jobban érvényesítő, eredményességben pedig hasonlóan hatékony szisztémát vezetett be. A *notice and notice* rendszer³⁰ Kanadában egy önszabályozási kezdeményezés volt, amelyben a szolgáltatók önként vállalták a sajátos kötelezettséget. A rendszer lényege abban áll, hogy a megkeresést követően nem a szolgáltatónak kell döntenie a tartalom jogellenességéről és eltávolításáról, hanem a hozzá érkezett megkeresést továbbítja a tartalom elhelyezőjének, így az ő ügykörébe utalva a problémát.³¹ Amennyiben az eredeti szerző nem nyilatkozik, úgy a szolgáltatónak lehetősége van a bejegyzés eltávolítására. A rendszer egyes alternatívái között van olyan megoldási javaslat is, amely lehetőséget teremtene a két félnek a szolgáltató általi összekapcsolására. Természetesen ennek a megoldási szisztémának számtalan olyan részletkérdése van, amely – a magyar jogi rendszerben gondolkodva – problematikus lehet. Elsősorban adatvédelmi szabályokra gondolhatunk. További kérdés, hogy rendelkezhet-e a szolgáltató a felhasználója elérhetőségével, de még inkább az, hogy az esetleges regisztráció során megadott elérhetőséget továbbíthatja-e a tartalom gazdájának? Ha azonban a felek hozzájárulnak az összekapcsoláshoz, akkor ez az aggály megszűnik. Hasonló megoldás lehet az is, hogy a szolgáltató a hozzá érkező megkeresést követően megkérdezi a felhasználójától, hogy elérhetőségét továbbíthatja-e, s amennyiben a válasz nemleges – hasonlóan a megkeresésre nem reagáló szerző esetére –, úgy a szolgáltató maga dönthetne a tartalom további sorsáról.

Ezek a megoldási javaslatok kiküszöbölik a *notice and take down* rendszerrel szembeni egyik legérzékenyebb alkotmányossági kifogást, azt tudniillik, hogy a szolgáltató jogerős bírósági döntés vagy a tartalom bejegyzőjének hozzájárulása nélkül töröljön egy esetleg jogszerű, s így a véleménynyilvánítási szabadság által védett tartalmat.

Az Európai Unió jogban az elektronikus kereskedelemről szóló, az Európai Parlament és a Tanács által hozott 2000/31/EC irányelv nem szabályozta, de nem is zárta ki a nemzeti jogokból az értesítési és eltávolítási (*notice and take down*) eljárást. Az internetszolgáltatóknak a harmadik személyek által elhelyezett tartalomért való felelősségéről a tárhelyszolgáltatást szabályozó 14. cikk világosan rendelkezett. Az irányelv megalkotásával a cél a szolgáltatók általános, mögöttes felelősségének a megszüntetése, egyáltalán a felelősségük limitálása, és helyette egy speciális eljárás (*notice and take down*) keresztül a szolgáltató (levélteli) kötelezettségének az előírása volt. Az irányelv által bevezetett felelősségi konstrukció hasonlít az amerikai szerzői jogi törvény *booksellers liability* megoldásához (a könyvkereskedők felelősségéhez), amelyet ott is kiterjesztettek a tárhelyszolgáltatókra. A 14. cikk értelmében a tárhelyszolgáltatót nem

28 Vö. The Right to Blog, Article 19. Policy Brief, 2013. 36.

<http://www.article19.org/data/files/medialibrary/37382/Right-to-Blog-EN-WEB.pdf>

29 BAYER i. m. (25. lj.) 37.

30 L. uo., 87-88.

31 L. erről The Right to Blog i. m. (28. lj.) 37.

terhelheti felelősség harmadik fél tartalmaért, amennyiben a szolgáltatónak nem volt tudomása a jogellenes tartalomról (jogellenes tevékenységről vagy információról), illetve „(...) amint ilyenről tudomást szerzett, haladéktalanul intézkedik az információ eltávolításáról, vagy az ahhoz való hozzáférés megszüntetéséről (...)”.³² Az irányelv ezzel együtt lehetővé teszi a tagállami bíróságoknak vagy közigazgatási hatóságoknak, „(...) hogy a szolgáltatót a jogsértés megszüntetésére vagy megelőzésére kötelezzék(...)”, továbbá a tagállamok belső jogukban olyan eljárási szabályokat alakíthatnak ki, amelyek rendezik a jogsértő tartalom eltávolításának vagy a hozzáférhetetlenné tételnek a módját.³³ Az irányelv egyúttal rögzíti, hogy nem lehet a szolgáltatókkal szemben ún. általános nyomonkövetési kötelezettséget előírni, így a szolgáltatók nem kötelesek a harmadik személyek tartalmait monitorozni és a jogellenes tevékenységre utaló tényeket, körülményeket vizsgálni, vagyis moderálni az internetes nyilvánosság általuk biztosított/fenntartott szelétét. Ez a szabály lényegében a szolgáltató által nem moderált harmadik személyektől származó tartalmak vonatkozásában kimondja, hogy a szolgáltatót nem terhelheti önmagában azért magasabb szintű felelősség, amiért nem szűrte, monitorozta ezeket a tartalmakat. Vagyis a jó szamaritánus kikötését az irányelv is alkalmazza.

Az Országgyűlés az irányelvet az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvényben (továbbiakban: Ekertv.) ültette át a magyar jogba. Az Ekertv. 13. §-a rendelkezik részletesen a Magyarországon alkalmazandó értesítési és eltávolítási eljárásról.

A EJEB két ítéletében vizsgálta a harmadik személy jogellenes tartalmaért viselt szolgáltatói felelősséget. A *Delfi AS v. Estonia* ügyben³⁴ a bíróság megállapította a Delfi felelősségét, majd a később tárgyalta *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt. v. Hungary* ügyben³⁵ bár megerősítette a korábban megfogalmazott alaptételét, miszerint a tárhelyszolgáltató felelhet harmadik személyek jogellenes tartalmaiért, döntésében mégis eltérő következtetésre jutott. A magyar szolgáltatónak kedvező döntést hozva a bíróság megállapította, hogy a szolgáltató felelőssége a konkrét ügyben nem volt megállapítható a tartalmihoz véleményt csatoló harmadik személyek (kommentelők) közléseiért. A strasbourgi bíróság a két ügyben hozott különböző eredményű döntésének indokolását az ügyek közötti két, alapvető különbségre vezette vissza. Egyfelől érvelt a Delfi és az MTE szolgáltatásának különbözőségével, tekintve, hogy amíg az előbbi kifejezetten üzletszerű, gazdasági tevékenysége keretében tette közzé mások tartalmait, és a biztosított kommentelés lehetővé tette ennek a gazdasági tevékenységnek (hírportál működtetése) az eredményességét volt hivatva növelni, addig az MTE esetén ilyen gazdasági érdekeltséget nem azonosított. Az Index, hasonlóan a Delfihez, gazdasági tevékenysége keretében biztosította a tartalom közzétételét, ezért az első érv elesett, de a bíróság megállapította, hogy a tartalmak nem voltak olyanok, amelyek a véleménynyilvánítási szabadság korlátozását lehetővé tették volna. A tartalmak – bár támadó jellegűek és vulgáris stílusúak voltak – nem minősültek nyilvánvalóan jogellenes beszédnek, és biztosan nem minősültek gyűlöletbeszédnek vagy erőszakra való uszításnak.

32 Az Európai Parlament és a Tanács 2000/31/EK irányelve (2000. június 8.) a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem egyes jogi vonatkozásairól („Elektronikus kereskedelemről szóló irányelv”) 14. cikk (1) bek. *Az Európai Közösségek Hivatalos Lapja* L178, 17/07/2000. (a továbbiakban: Irányelv).

33 Vö. Irányelv 14. cikk (3) bek.

34 No. 64569/09, 2015. június 16.

35 No. 22947/13, 2016. február 02.

Összességében az EJEB Delfi és MTE döntéseiből pár következtetést már levonhatunk a bíróság későbbi gyakorlatának prognózisa nélkül. A bíróság az értesítési és eltávolítási eljárást a tárhelyszolgáltatók vonatkozásában valamennyi érintett érdekére figyelemmel megfelelő eszköznek találja, de a harmadik személytől származó, súlyosan jogellenes tartalom (gyűlöletet kelt vagy közvetlen fenyegetést tartalmaz) esetén az államok jogosultak szigorúbb felelősségi szabályokat is bevezetni, ha a szolgáltató nem távolítja el haladéktalanul az ilyen tartalmakat. Míg az EJEB az MTE esetében a felelősség alóli mentesülés elégséges indokának találta a gazdasági érdekeltség hiányát, addig az Index esetében a tartalmak jogellenességének csekély voltára tekintettel, nem állapította meg a szolgáltató felelősségét.

A közvetítő szolgáltatói felelősség speciális esetét szabályozza a médiaszolgáltatásokról és a tömegkommunikációról szóló 2010. évi CLXXXV. törvény [Mttv.]. Bizonyos esetekben a Médiatek hatósági hatáskörben kibocsátott hatósági határozatában kötelezheti a közvetítő szolgáltatót a mediaszolgáltatás és az internetes sajtótermék közvetítésének felfüggesztésére.³⁶ A büntetőeljárás kódex pedig lehetővé teszi az elektronikus hírközlő hálózat útján közzétett adatok ideiglenes hozzáférhetetlenné tételét, „(...) [h]a az eljárás olyan közvédelemre indokolt, amely miatt folyik, amellyel kapcsolatban elektronikus adat végleges hozzáférhetetlenné tételének van helye, és az a büntetőeljárás folytatásának megakadályozásához szükséges (...)”.³⁷

5. Keresőmotor-szolgáltatók és az internetes szólásszabadság

A közvetítőszolgáltatók egy másik csoportjának, az internetes információtengerben az általunk keresett információk megtalálását segítő keresőmotor-szolgáltatóknak a tevékenysége is számos újszerű problémát generált. A jogellenes tartalmakért való szolgáltatói felelősség kapcsán már előzetesen érdemes leszögezni, hogy a keresőmotor-szolgáltató közvetített tartalmakhoz való viszonya bár néhány ponton hasonlít, de érdemben mégis eltér a tárhelyszolgáltatókétól. A keresőmotorokkal kapcsolatos jogi problémákat az alábbi kérdésekben összegezhetjük: lehet-e a keresőmotorok találati listáját szólásnak tekinteni, avagy jogi értelemben beszélnek-e a gépek? Ha igen, az ilyen szólas élvez-e alapjogi védelmet? Megállapítható-e az automatizált keresés eredményei alapján a szolgáltató felelőssége?

Miután az internet technológiája által létrejött nyilvánosságban sokan üdvözltek a szólásszabadság utópiájának valósággá válását, hamar rá kellett arra jönni, hogy az cybertérben megjelenő információs bőség a releváns információk megtalálásának ellehetetlenülését okozza. Az online nyilvánosságot jellemző információbőség, és még inkább az információk amorf halmaza (információs szmog) ugyanis nem segíti, sokkal inkább ellehetetleníti a minden idők legdemokratikusabbnak mondott internetes nyilvánosságban

36 Vö. Mttv. 188–189. §. A vonatkozó rendelkezések, amelyek lényegében a tartalom infrastruktúra-szolgáltató általi blokkolását teszik lehetővé, a műsorterjesztők, a közvetítő szolgáltatók közigazgatási hatósági eljárásban történő eltávolítási kötelezéséről rendelkeznek. A közvetítő szolgáltatót a Médiatek hatósági hatáskörben kibocsátott hatósági határozatban kötelezheti meghatározott mediaszolgáltatás továbbításának felfüggesztésére.

37 A büntetőeljárásról szóló 1998. évi XIX. törvény (a továbbiakban: Be.). 158/B. § (2) bek. Az ideiglenes hozzáférhetetlenné tétel két módon rendelhető el, vagy az elektronikus adat ideiglenes eltávolításával, vagy az elektronikus adathoz való hozzáférés ideiglenes megakadályozásával [Be. 158/B. §. (4) bek.].

való tájékozódást. A problémát a keresőmotorok megjelenése látszott megoldani, amelyek feladata, hogy keresési parancsok alapján a keresésnek megfelelő, releváns információkat jelenítsenek meg. Az így felkínált keresési találatokat a keresőmotor egy meghatározott találati listába rendezi. A közönséghez és a tartalomhoz való hozzáférés szempontjából annak van jelentősége, hogy a találati lista hányadik helyén jelenik meg az adott találat. Az internetes nyilvánosság 'szónokának', az online véleményt formulázónak eminensen az a célja, hogy minél eredményesebben hívja fel magára a figyelmet, minél több online felhasználóhoz jusson el az általa publikált tartalom, vagyis az minél előkelőbb helyen szerepeljen a keresőmotor által felkínált tartalmak listáján. A tartalom érzékelhető megjelenítése, az információk szmogból való kiemelkedése viszont sok esetben jelentékeny anyagi áldozatvállalás útján érhető el. Ez azonban – hasonlóan az offline nyilvánosság véleménypiacaihoz – a tőkeerős, nagy szervezettséggel rendelkező, professzionális, piaci alapon működő, profitorientált médiavállalatokat hozza kedvező helyzetbe, az általuk fontosnak ítélt, politikai, üzleti megfontolásaik mentén priorált tartalmakat, véleményeket teszi érzékelhetőbbé a felhasználók számára. Mindez bizonyosságul szolgál arra, hogy bár az internet ígérete az volt, hogy elhozza a soha korábban nem tapasztalt hozzáférést a nyilvánossághoz mind a vélemények kifejezése, mind pedig az információkhoz, plurális véleményekhez való hozzáférés tekintetében, ám a formális egyenlőség mögött a tényleges piaci pozíciók jelentékeny aszimmetriája sejlik fel. Azok a tartalmak és megfogalmazások ugyanis, amelyek a keresőmotorok találati listáján nem jelennek meg, de még azok is, amelyek nem előkelő helyre kerülnek (egyes felmérések szerint az átlagfelhasználó csupán az első három-négy találatot nézi meg), az internetes nyilvánosságban szinte vagy teljesen láthatatlanná válnak.

A keresőmotor-szolgáltató mindig más, harmadik személy tartalmát közvetíti. Az Ekertv. éppen ezért sorolja a limitált felelősségű, közvetítő szolgáltatók közé³⁸ [Ekertv. 2. § ld. pontja]. Ám a kérdés mégis az, hogy mi a tényleges kapcsolata az „(..) információk megtalálását elősegítő segédeszközöket biztosít[ó] (...)”³⁹ [Ekertv. 2. § ld. pontja] keresőmotor-szolgáltatónak az igénybe vevő találati listáján megjelenő tartalmakhoz? A közvetítő-elmélet szerint a keresőmotor-szolgáltató kizárólag közvetíti mások tartalmait, algoritmusok segítségével automatizáltan és objektíven generálja a találati listákat, míg a szerkesztélmélet tartalomközlőnek tekinti, amikor – emberek által megalkotott algoritmus segítségével – a felhasználó keresési kérelmére véleményt fogalmaz meg arról, hogy a felhasználónak melyek lehetnek a releváns találatok, és hogy azok milyen sorrendben jelenjenek meg.⁴⁰

A keresőmotorok olyan információs szolgáltatásokat nyújtanak, amelyek különleges kihívásokat és nagyfokú veszélyeket jelentenek az online nyilvánosság pluralitására. A keresőmotor-szolgáltatások szűrési tevékenységük során rangsorolnak az egyes fellelhető tartalmak között, ezáltal befolyásolják az egyes tartalmakhoz való tényleges hozzáférés esélyét, ami a közéleti viták polarizálódásához és a piaci verseny torzulásához vezethet.⁴¹

38 Ekertv. 2. § ld. pontja.

39 Uo.

40 NAVRATYIL Zoltán: A gépek nem beszélnek. A keresőmotor-szolgáltatók találati listája, mint szólás az Egyesült Államok jogfelfogása tükrében. In *Medias Res*, 2015/1. 133.

41 Vö. KOLTAY András: A sajtószabadság fogalma ma. In: KOLTAY András – TÖRÖK Bernát: *Sajtószabadság és médiaszabályozás a 21. század elején* 2. Budapest, Wolters Kluwer, 2015. 122–124.

5.1. A találati lista szólásjellege Európában és az Egyesült Államokban

A luxemburgi székhelyű Európai Bíróság 2014-ben meghozott döntése [C-131/12. sz. a *Google Spain SL és a Google Inc. v. Agencia Espanola de Protección de Datos (AEPD) és Mario Costeja González*] az európai jogrendben paradigmaticus jelentőséggel bír. A Bíróság ítélete szerint meghatározott feltételek esetén „(...) a keresőmotor működtetője köteles arra, hogy az egy személy nevére való keresés nyomán megjelenő találati listáról törölje a harmadik fél által közzétett, és e személlyel kapcsolatos információkat tartalmazó weboldalakra mutató linkeket abban az esetben is, ha ezt a nevet vagy az ilyen információkat korábban vagy egyidejűleg nem törölték ezekről a weboldalakról, mégpedig adott esetben akkor is, ha önmagában az említett oldalakon történő közzététel jogszerű (...)”. Az európai polgárnak tehát joga van a feledésbe merülésre (*right to be forgotten*); és ez nagyobb súllyal esik latba, mint a keresőmotor működtetőjének jogos érdekei, illetve mint az információszabadsághoz fűződő általános érdek.

Ezzel szemben az USA gyakorlatában a keresőmotor-szolgáltató által megjelenített találati lista szólásnak, véleménynek minősül, amelyre így kiterjed az Első Alkotmánykiegészítés hatálya.⁴²

A 2000-es esztendőek elején több amerikai alsóbíróság találkozott a különböző keresőmotorok tartalmakat rangsoroló találati listája jogi minősítésének problematikájával. Az egyik első ilyen ügyben, a *Search King v. Google* ügyben⁴³ a Search King nevű reklámügynökség azt panaszolta, hogy a Google keresőmotor az általa működtetett weblapokat a találati listán a korábbiakhoz képest hátrébb sorolta, amely neki jelentékeny mértékű kereslet-, ezáltal pedig bevételkiesést okozott. Az oklahomai nyugati kerületi bíróság azonban elutasította a Search King keresetét, azzal az indokolással, hogy a Google akkor, amikor oldalak rangsorolását végzi, a felhasználók keresési szokásainak figyelembevételével véleményt nyilvánít az adott oldalról. Az így kifejtett véleményt (rangsort) pedig az Első Alkotmánykiegészítésből fakadó alkotmányos védelem illeti meg, amely erősebb, mint a Search Kingnek okozott sérelem. Amíg a Search King elsősorban a gazdasági érdekeinek sérelmét panaszolta, addig Christopher Langdon politikai véleménye bemutatásának korlátozása miatt perelte be a Google, a Microsoft és a Yahoo szolgáltatóit.⁴⁴ Langdon több politikai tartalmú honlapot üzemeltetett, amelyek különböző bel- és külpolitikai témákat dolgoztak fel, többek között a kínai kommunista kormányzat emberi jogi jogsértéseiről. Ezeket a honlapokat Langdon szerette volna reklámozni az alperesek keresőmotor-szolgáltatásaiban, akik azonban a reklámok közzétételét megtagadták. Langdon többek között a szólásszabadsága megsértését panaszolta, ám a delaware-i bíróság éppen a keresőmotor-szolgáltatók szólásszabadságára hivatkozva utasította el a keresetet: nem kötelezhető a keresőmotor-szolgáltató olyan tartalom (értve alatta a reklámot is) megjelenítésére, amelyet nem akar közzétenni. A bíróság továbbá azt is kifejtette, hogy a szolgáltatók nem állami szervek, és magántársaságként nem kötelesek mások szólásszabadságának gyakorlására teret biztosítani.

A New York-i bíróságon lefolytatott Baidu nevű keresőmotor szolgáltatója ellen indított ügyben⁴⁵ is a – kifejezetten politikai jellegű szelekciót alkalmazó – keresőmotor-szolgáltató alkotmányos pozíciója bizonyult erősebbnek. A *Zhang v. Baidu* ügyben a kínai demokratikus változásért harcoló

42 Vö. NAVRATYIL i. m. (40. l.) 129–130.

43 *Search King v. Google Technology Inc.* Case No. Civ-02-1457-M (W.D. Okla., Jan. 13, 2003).

44 *Christopher Langdon v. Google Inc., et al.* Case No. 2007 WL 530156, Civ. Act. No. 06-319-JJF (D. Del. February 20, 2007).

45 *Jian Zhang et. al. v. Baidu.com, Inc.* Case No. 11 Civ. 3388 (JMF) (NY, 3.27. 2014).

emberi jogi aktivisták perelték be a kínai Baidu keresőmotor szolgáltatóját. A Baidu – a felperesek állítása szerint – nem csupán Kínában, de az USA-ban is blokkolta a Kínának kényes politikai tartalmakat. Additív érvként a bíróság megállapította, hogy amellett, hogy amikor a Baidu rangsorol vagy egy tartalmat egyáltalán nem jelenít meg, a véleménynyilvánítás szabadsága által védett döntést hoz, nem is lehetetleníti el a hozzáférést, tekintettel arra, hogy a tartalom az interneten más eszközökkel is megtalálható, így más keresőmotorok saját találataik között megjelenít(het)ik. A bíróság ugyan *expressis verbis* nem mondta ki, de ezzel utalt arra, hogy nincs alanyi jog egy meghatározott keresőmotor-szolgáltató keresési listáján való megjelenítés kikényszerítésére. Természetesen mindez addig nem is bír gyakorlati relevanciával, amíg a fentebb bemutatott jogértelmezés fennmarad.

A keresőmotor-szolgáltatók tevékenységét sokan hasonlítják a könyvtáros katalogizáló tevékenységéhez, így segítve a felhasználókat az interneten fellelhető információk tengerében való eligazodásban. Mára azonban egyre nyilvánvalóbbá válik, hogy az internet bábeli bibliotékájának mindentudó könyvtárosai nem is elfogulatlanok, nem csupán formális feltételeket alkalmazó automatizált algoritmusok segítségével katalogizálnak, tevékenységükben megfigyelhető, hogy üzleti, politikai determinációk mentén elfogultságról tesznek tanúbizonyságot (*search engine bias*). A keresőmotorok aktív, az online nyilvánosság összetételét befolyásoló vagy akár torzító tevékenységét a fent bemutatott esetek is alátámasztják.

5.2. Az automatikus keresési javaslat (autocomplete) és a szolgáltatói felelősség

Hasonlóan érdekes és megválaszolandó kérdéseket vet fel a keresőmotor-szolgáltató Google által működtetett automatikus kiegészítés funkció, valamint a korábbi kereséseinket rögzítő digitális lábnyom. Ezek az algoritmusok beavatkoznak az információ továbbításba, amikor ugyan közvetlen emberi beavatkozás nélkül, de kétségkívül érdemben gyakorolnak egyfajta szerkesztői kontrollt annak érdekében, hogy aktív javaslatokat generáljanak a felhasználók számára. Ezekben az esetekben a szolgáltató az emberi tényezőt, a humán *inputot* kombinálja a mesterséges intelligenciával. Az újszerű jogi kihívást ebben az esetben a keresőmotor prediktív technológiája és annak jogi minősítése jelenti.

Az *autocomplete* funkcióval a Google már nem csupán harmadik felek tartalmait jeleníti meg, nem kizárólag az internet információs óceánjából szűri ki a keresési kérésünkkel adekvátnak vélt tartalmakat a keresett kifejezés begépelését követően, hanem önmaga tesz javaslatot, vetít előre keresési javaslatot, mintegy előre megjósolja gondolatainkat, vagy éppen eredeti szándékunktól eltérő keresési javaslat generálása révén, a kezdeti érdeklődésünktől eltérő tartalmak felé fordíthatja figyelmünket. Így olyan keresési javaslatokat kínál számunkra az internetes információs svédasztal kínálatából, amelyek iránt egyébként magunktól nem érdeklődnénk. Nem pusztán egy eredményt hoz létre, hanem lényegében sugalmazza az általunk nem minden esetben elvárt eredményt. A Német Szövetségi Köztársaság elnökének felesége, Bettina Wulff nevére való keresési szándék esetén a Google automatikus kiegészítésként feltüntette az *escort* és *prostituált* kifejezéseket is.⁴⁶ A Szövetségi Legfelső Bíróság vé-

46 Felix Emeric TOTA: Google-Suche „Bettina Wulff“, Dreiundvierzig Wortkombinationen weniger. *Frankfurter Allgemeine Zeitung*, 2015. 01. 16. <http://www.faz.net/aktuell/feuilleton/google-entfernt-ergaenzungen-bei-suche-nach-bettina-wulff-13373712.html>, vagy Autocomplete-Funktion, Bettina Wulff und Google einigen sich. *Spiegel Online*, 2015. 01. 16. <http://www.spiegel.de/netzwelt/web/bettina-wulff-und-google-einigen-sich-aussergerichtlich-a-1013217.html>

gül 2013-ban úgy döntött, hogy a Google-nak törölnie kell a sérelmezett szókapcsolatot az automatikus kiegészítés javaslatai közül. Egy másik ügyben (R. S. Google elleni pere: BGH, Urteil vom 14.05.2013 – VI ZR 269/12) ugyancsak a német Legfelső Bíróság megállapította a Google felelősségét személyhez fűződő jogok megsértése miatt, amelyet a szolgáltató az *autocomplete* funkciójával valósított meg. R. S. úr egy megbecsült német üzletember volt, teljes nevének a Google-keresőbe való begépelését követően, az automatikus kiegészítés funkció a személyéhez társította a *szcientológus* és a *csalás* kifejezéseket. A bíróság többlépcsős érvelésben megállapította, hogy sérült a felperes személyiségi joga, és a szolgáltató közvetlenül felelős a jogsértésért. A bíróság kiemelte, hogy a jogsértő kifejezéseket a Google szolgáltatása, és nem egy harmadik személy kombinálta össze; a kifogásolt keresési predikcióként megjelenő kombinációt a keresőmotor hozta létre. Ugyanakkor a bíróság elvi élel azt is rögzítette, hogy a Google Inc. nem korlátlanul felelős a kifogásolt predikcióért, hiszen ésszerűtlen lenne vele szemben azt érvényesíteni, a jogsértés ugyanis véltlen hibának minősül. A bíróság a felelősség megállapítás során azzal érvelt, hogy a Google tevékenysége nem korlátozódott csupán technikai, automatikus és passzív jellegű lépések megtételére, valamint nem csupán egy információ harmadik személyek számára való hozzáféréseinek biztosítására korlátozódott. Az *autocomplete* önmagában nem jogellenes magatartás, hanem legitim üzleti szolgáltatás, de a szolgáltató felelős azért, ha a predikciók formájában felkínált keresési javaslatok, kifejezések jogellenesek. A szolgáltató azért tehető felelőssé, mert elmulasztotta azon megfelelő megelőző intézkedések megtételét, amelyek képesek lettek volna megelőzni a személyiségi jog megsértését okozó javaslatok megjelenését.

A hongkongi bíróság a *Yeung Sau Shing Albert v. Google Inc.* ügyben [HCA 1383/2012] azt vizsgálta, hogy a felperes nevének triád tag (*triad member*) kifejezéssel való kiegészítése megalapozza-e a keresőmotor-szolgáltató felelősségét? A Hongkongban nagy ismertségnek örvendő üzletember nevének a Google keresőjébe történő beírása során a személyét az *autocomplete* a kínai szervezett alvilággal hozta összefüggésbe, majd a keresési találatok között is több olyan cikk volt, amely Yeungot konkrétan megnevezett bűnbándákkal és súlyos bűncselekményekkel kapcsolta össze. A hongkongi bíróság döntésében a *common law* fogalmainak foglyaként arra kereste a választ, a Google *autocomplete* funkciója által generált prediktív javaslatok kiadói tevékenységnek minősülnek-e? A bíróság a Google-t határozottan kiadónak tekintette, mivel a vállalat automatizált rendszereket hoz létre és üzemeltet, amelyek szándéka és célja szerint generálnak tartalmakat, ezzel platformot alkot a nyilvános közlések terjesztésére és az ezen társadalmi diskurzusokban való aktív részvételre. Mindezekre tekintettel a hongkongi bíróság a gyorsított ítéletében (*summary judgment*) a Google automatikus kiegészítés funkcióját nem passzív technológiának, nem egyszerű közvetítőnek minősítette, hanem arra a határozott következtetésre jutott, hogy az „újabb kombinációkat” hoz létre, és mintegy „aggregálja” a webes tartalmakban talált adatokat, ’újraalkotja’ az aggregált adatokat a más felhasználók által korábban bevitt kifejezések alapján, és aztán ezeket javaslatokká és predikciókká ’alakítja át’. A bíróság nem osztotta azt az alperesi jogi képviselő által előadott állítást, miszerint a Google automatikus kiegészítés funkciója egy semleges eszköz, tekintve, hogy algoritmusai „(...)szintetizálják és újraalkotják a korábbi felhasználók által bevitt keresési adatokat és az internethasználók által feltöltött tartalmakat, mielőtt megjelenítik azokat (...)”.

A felelősség megállapítása során további eminens kérdés volt, hogy a Google, amikor egy *autocomplete* kiegészítésre tesz javaslatot, vajon minek van a tudatában? A védelem képviselője

lőjének érvelését cáfolandó – miszerint az automatizált működés miatt nem lehet kijelenteni, hogy a Google Inc. tudatában volt a saját maga tervezte eszköz által generált predikcióknak vagy keresési eredményeknek –, a bíróság hangsúlyozta, hogy „(...)a kiadó objektív felelősségére vonatkozó szabály alapján, a szükséges tudati elem nem a becsületsértő tartalom ismerete vagy a becsületsértés szándéka, hanem sokkal inkább az, hogy az alperes aktívan elősegítette vagy szándékosan közreműködött-e a becsületsértő tartalom harmadik fél számára történő hozzáférhetővé tételében, függetlenül attól, hogy volt-e tudomása a kérdéses anyag becsületsértő jellegéről (...)”.⁴⁷

A Google az automatikus kiegészítés és a kapcsolódó találatok funkcióval vitán felül aktívan beavatkozik az információtovábbításba, nem pusztán a tartalmak passzív közvetítője. Algoritmus alapú, de az emberi beavatkozást is lehetővé tévő kontrollt gyakorol az online tér információs tengerében, aktív javaslatokat generál a felhasználói számára. Ebben az esetben a humán *inputot* összekapcsolja a mesterséges intelligenciával.

A fentiekből álláspontunk szerint egyértelműnek látszik, hogy amíg a keresőmotorok találati listájának és az azért viselt szolgáltatói felelősség megítélésében nincs egységesen elfogadott joggyakorlat, sőt az Egyesült Államok és az Európai Unió eddigi judikaturája jól érzékelhető divergenciát mutat, addig az automatikus kiegészítés és a kapcsolódó keresések körében ha nem is egységesnek, de összebékíthetőbbnek látszik a szolgáltató felelősségét elismerő bírói gyakorlat.

Álláspontom szerint a keresőmotorok automatikus kiegészítés funkciója által felkínált, harmadik személytől származó jogellenes tartalmak vonatkozásában a szolgáltató felelőssége körében megfontolásra érdemes az értesítési és eltávolítás rendszer *mutatis mutandis* alkalmazhatósága.

6. Az internetes nyilvánosság új színtere: a közösségi hálózatok, platformok – a közösségi média

A közösségi hálózatok társadalmi diskurzusokban betöltött szerepe, a szólásszabadság érvényesülésére gyakorolt hatása mára oly meghatározóvá vált, hogy sokak véleménye szerint „(...) a Facebook több hatalommal rendelkezik annak meghatározására, hogy ki szólhat [...], mint bármely legfelsőbb bíróság, király vagy elnök(...)”.⁴⁸

A közösségi platformok *differentia specificája*, hogy a közzétett tartalmakat többnyire a felhasználóikból álló közösség hozza létre és szerkeszti. A kifejezés (*social media*) 2006-ban terjedt el, amikor a Wikipedia, amely maga is egy közösségi média, először definiálta a jelenséget: „(...) a közösségi média az a média, amit elsődlegesen egy közösség, mint csoport formál, közösségi szinten, nem pedig írók, újságírók és a médiavállalatok összessége (...)”.

47 Vö. Anne CHEUNG: Becsületsértés automatikus keresési javaslat által. A keresőmotorok felelőssége az automatikus kiegészítések korában. In *Medias Res*, 2015/2. Ipso Iure Fordítóiroda, lektorálta: Reményi Édua Vénusz, 270–289.

48 Jeffrey ROSENT idézi Marjorie HEINS: The Brave New World of Social Media Censorship. 127 *Harvard Law Review* (2014) 325.

2015-ben az Encyclopædia Britannica által szerkesztett Merriam–Webster úgy határozta meg a közösségi médiát, mint az elektronikus kommunikáció ama formája, amelyen keresztül az emberek online közösségeket hoznak létre abból a célból, hogy információkat, ötleteket és személyes üzeneteket osszanak meg.⁴⁹

6.1. A közösségi hálózatok jogi kihívásairól általában

A kommunikációs szektorban tapasztalható technológiai fejlődésnek egy új állomását jelentik a közösségi elven működő hálózatok. A közösségi oldalak mára olyan új kommunikációs eszközökként működnek, amelyek nem csupán a személyközi (interszónális) kommunikáció meghatározó fórumaivá váltak, de a felhasználók jelentékeny része tömegkommunikációs eszközként is tekint rájuk; sokan az általuk használt közösségi oldalakról szerzik be a társadalmi folyamatokra vonatkozó információikat (közösségi média). Az internetes kommunikáció egy korábbi szakaszában a hagyományos levelezést felváltotta az e-mail, amit most vált fel a közösségi médiában küldött azonnali üzenetküldés, beszélgetés (*chat*). A Bell-féle telefont a mobiltelefon, majd mára egyre inkább a közösségi szolgáltatón keresztül kezdeményezhető (videó)hívások helyettesítik. Az okoseszközök megjelenése egyben technológiai konvergenciát is előidézett, mivel az okostelefonok a hagyományos telefonálás mellett böngészésre, közösségi hálózaton való kapcsolattartásra, beszélgetésre, fényképes és hang adatrögzítésre, helyzetmeghatározásra és még számtalan további funkcióra használhatóak.

A közösségi média számos új jogi kérdést hozott a felszínre, egyúttal több, korábban is létező jogi problémát helyezett új összefüggésrendszerbe. Példának okáért a közösségi média használatával a felhasználó sokkal könnyebben, szinte észrevétlenül valósíthat meg személyiségi jogi jogsértést, mint más módon. A felgyorsult kommunikációs térben egy mások által közzétett tartalom megosztása is okozhatja más személyiségi jogának megsértését, ezáltal megalapozhatja a felhasználó jogi felelősségét. Például egy (jogellenes) tartalom megosztásával (posztolás), ami technikailag nem több egy kattintásnál, megvalósítható a jóhírnév megsértése⁵⁰ vagy éppen a rágalmozás vétsége büntető törvénykönyvi tényállása is, tekintettel arra, hogy a más rágalmozó tényállításának a továbbadása híresztelésnek minősül.⁵¹

A Győri Ítéltábla eseti, másodfokú ítéletében⁵² foglalkozott egy Facebookon szervezett tüntetés megosztásával, illetőleg a megosztó felhíváshoz kapcsolt kommentjével. A kifogásolt tartalom két önkormányzati ingatlan elidegenítésével volt kapcsolatos, és azt állította, hogy a szerződések megkötése nem volt jogszerű. A bíróság az ügyben úgy foglalt állást, hogy a tüntetésre való felhívás tartalma burkolt tényállítást valósított meg, míg annak a megosztása valótlan tény híresztelésének minősül. A bíróság a megosztás műfajával kapcsolatban kifejtette, hogy az megfelel a híresztelés fogalmának, mivel az egy adott személy nyilatkozatának, gondolatának továbbítása akkor is, ha az híven közli az eredeti nyilatkozatot. Ebből az következik, hogy hasonló esetben a megosztó felelőssége attól függetlenül beáll, hogy ő maga nem fűz hozzá semmit a megosztott, valótlan, az adott személy társadalmi megítélését hátrányo-

49 Merriam-Webster: Dictionary and Thesaurus. www.merriam-webster.com

50 Vö. Ptk. 2:45. § (2) bek.

51 Vö. Btk. 226. § (1) bek.

52 Győri Ítéltábla Pf.I.20.065/2015/4/I.

san befolyásoló tényállításhoz. Hasonlóképpen nem feltétele a felelősség beállásának, hogy hány személy fér hozzá a megosztás folytán a jogsértő tartalomhoz, ahogyan az sem, hogy ezáltal ismételten sor kerül-e a jogsértő tartalom újabb megosztására, vagy sem. Utóbbiaknak a lehetséges szankciók megállapításakor van jelentőségük.

Érdekes szempontként vizsgálta a bíróság, hogy a megosztó személy a megosztott tartalommal milyen viszonyban áll, és köteles-e ellenőrizni annak hitelességét. Az alperes úgy érvelt, hogy a felgyorsult kommunikációs térben tapasztalt társadalmi jelenség, a közösségi hálókön kialakult kommunikációs gyakorlat szükség szerint limitálja a tartalmat megosztó személy felelősségét annak esetleges jogellenes voltáért. Összehasonlítva a professzionális sajtótermékekkel, médiaszolgáltatókkal, a közösségi médiában véleményt alkotók jelentékeny része nem rendelkezik az előbbiekre jellemző szaktudással, ezt a tartalmat észlelő felhasználók is tudják, így az elvárható megfontolás, körültekintés mércéje is alacsonyabb velük szemben. Az alperesi érvelés végül hivatkozott a közügyek vitatásához fűződő, kiemelkedő alkotmányos értéktartalomra is. Az ítéletábra nem osztotta az alperesi álláspontot, és megállapította a jogellenes tartalomért való felelősségét.

De hasonlóan fokozódik a képmáshoz való személyiségi jog potenciális megsértésének a lehetősége, miközben számos esetben a felhasználó tudata nem fogja át a magatartásának a jogi konzekvenciáit, szándéka nem irányul jogellenességre.

Bár a fent hivatkozott ügy még nem zárult le véglegesen, tanulságaként érdemes leszögezünk, hogy a felgyorsult és globalizálódott kommunikációs tér működése első látásra nem észlelhető veszélyeket hordoz. Az általunk posztolt tartalom pillanatokon belül válhat sokak által megismert 'közkinccsé' (vö. a mémesedés folyamatával), miközben a tartalom feletti rendelkezésünk – vagyis annak a kontrollja, hogy ki osztja meg, milyen céllal, milyen hatást vált ki egy adott környezetben, tehát mi lesz a társadalmi hatása – teljes mértékben megszűnik.

6.2. A közösségi platformon közzétett vélemény jellege: a „like” alkotmányos megítélése

A vélemények védelme alkotmányos szempontból független attól a körülménytől, hogy azokat milyen platformon, offline vagy online fogalmazzák meg. A Legfelső Bíróság az Egyesült Államokban több döntésében is egyértelművé tette, hogy az interneten közzétett szólás alkotmányossági szempontból azonos védelemben részesül, mint az offline környezetben megjelenő tartalom.

A Facebookon végbemenő kommunikációs folyamat egyik sajátos eszköze egy gomb, a „like” (tetszik) gomb. A „like” gomb megnyomásával kifejezett véleményalkotás némiképp analógiát mutat a szimbolikus beszéddel, amikor egy jelkép használatával fejezzük ki álláspontunkat. A „like”-olás esetén is lényegében ez történik, egy meghatározott tartalommal való azonosulásunkat fejezzük ki szavak nélkül, egy gomb megnyomásával.

A *Bland v. Roberts* ügyben (2013 WL 5228033) az Egyesült Államokban a Negyedik Kerületi Fellebbviteli Bíróság a Facebookon történő „like”-olást is szólásnak, véleménynyilvánításnak minősítette, amiből egyenesen következik, hogy kiterjed rá az Első Alkotmánykiegészítés alkotmányos oltalma. A szóban forgó ügyben a hamptoni seriff választási kampánya után hat, korábbi beosztottjának újbóli kinevezését azon az alapon tagadta meg, hogy azok a kampány során a másik jelöltet támogatták. Az eljárás során Bobby Blandnek és öt társának azt kellett

bizonyítania, hogy a kinevezésük megtagadása összefüggésben volt a kampány során kinyilvánított szimpátiájukkal. Ennek során két felperes vonatkozásában a bíróság megvizsgálta a Facebookon kifejtett tevékenységüket is. A két beosztott „like”-olta a másik seriffjelölt kifejezetten a választás kampányára létrehozott Facebook-oldalát. Miután a seriff tudomást szerzett erről, figyelmeztette a dolgozóit, hogy ne támogassák kihívóját, máskülönben elveszíthetik a munkájukat. A bíróság úgy ítélte meg, hogy ez alapján megállapítható, hogy az esetükben a Facebook-tevékenységük okozta politikai bizalomvesztés vezetett a hivatalvesztésükhöz.

A bíróság érvelése szerint azért minősülhet a „like” alkotmányosan védett értéknek, mivel a felhasználó profilján megjelennek azok az oldalak, amelyeket a „like” gomb megnyomásával kedvel. Más felhasználók Facebookra való belépésükkor az idővonalukon egyből szembesülnek azzal, hogy mi történt ismerőseikkel, milyen tartalmakat tettek közzé, osztottak meg, vagy milyen más egyéb tevékenységet végeztek a közösségi oldal keretein belül. Amikor a felperesek kedvelték a kihívó jelölt oldalát, ez megjelent nem csupán a saját idővonalukon, de ismerőseik idővonalán is. Ez a bíróság jogértelmezésében egy közleménnyel ér fel, hiszen a felhasználó idővonalán szó szerint az jelenik meg, hogy kedveli valamelyik jelöltet. Az a körülmény pedig, hogy ezt a véleménynyilvánítást a felperes egy gomb megnyomásával valósítja meg vagy azt begépelve és közzétéve jeleníti meg, a védelem szempontjából nem bír relevanciával.

6.3. A közösségi oldalak szolgáltatóinak szabályozási tevékenységével összefüggő jogi problémák

A közösségi oldalakat üzemeltető platformszolgáltatók működése sok tekintetben túllép a klasszikus állami jogi szabályozás joghatósági kérdésén. A szolgáltatások határok nélkülisége csak hozzájárul ahhoz, hogy a közösségi platformok a nemzetállami szuverenitás tanára épülő állami jogalkotási dokumentumokkal szemben, bizonyos esetekben rezisztensek maradjanak. Egyúttal a közösségi platform szolgáltatói rendszerint maguk alkotnak szabályokat, amelyekkel lényegében meghatározzák a véleménynyilvánítás kereteit, a kimondhatóság határait, és ezen mechanizmusokhoz illeszkedő, normasértés esetén alkalmazható eljárásokat is bevezetnek. A szolgáltatók által alkotott szabályok lényegében egy sajátos ’tartalomszabályozást’ hoznak létre, és e regulák, mondhatnók az állami médiaszabályozások platformon történő leképeződései.

A közösségi platformok közül sok tekintetben kiemelkedik a Facebook közösségi oldal, ezért alább ennek a szabályozási tevékenységét, valamint annak egyes elemeit mutatjuk be.

A Facebook Jogi és Felelősségi Nyilatkozata (a továbbiakban: Nyilatkozat) tartalmazza azokat az alapvető szabályokat, amelyek a szolgáltató és a felhasználó közötti magánjogi jogviszony alapjait adják. A Facebook és a felhasználó között a szolgáltatás használatával vagy az ahhoz való hozzáféréssel létrejött jogviszonyt alapjaiban meghatározza a Nyilatkozat. Amennyiben valaki felhasználóként regisztrál a Facebook nevű közösségi hálóra, a regisztráció részeként elfogadja a szolgáltató által egyoldalúan felállított belső szabályzatokat (illetve, amint a tájékoztató fogalmaz, „(...) a Facebook használatával ezeket a feltételeket elfogadod(...)), hiszen ez feltétele a közösségi platform használatának.

A Nyilatkozat 15. pontja foglalkozik a szolgáltató és a felhasználó közötti viták megoldásával, amelynek értelmében a felhasználó minden, a Nyilatkozatból vagy a Facebookból

eredő vagy azokhoz kapcsolódó, a fogyasztó és a szolgáltató között fennálló követelést, keresetet vagy kárigényt kizárólag az Amerikai Egyesült Államok észak-kaliforniai bíróságán vagy a San Mateo megyében lévő állami bíróságon keresztül köteles rendezni, és vállalja, hogy minden ilyen követelés peres úton való rendezése céljából aláveti magát ezen bíróságok illetékességének. Kalifornia Állam joga irányadó a Nyilatkozat és bármely, a felhasználó és a Facebook között felmerülő követelés vonatkozásában, a jogszabályi rendelkezések ütközésére vonatkozó rendelkezésekre való tekintet nélkül⁵³.

Az esetleges jogellenes tartalmakért viselt felelősséget pedig teljes egészében áthárítja a felhasználóra:

„(...) Ha az Ön Facebookon fennálló tevékenységeivel, tartalmaival vagy információival kapcsolatban bárki ellenünk követeléssel él, Ön kártalanít és mentesít bennünket az ilyen követeléssel kapcsolatban felmerülő minden kártól, veszteségtől, bármilyen fajta kiadástól (beleértve az ésszerű jogi költségeket és díjakat). Habár biztosítunk szabályokat a felhasználói magatartásra vonatkozóan, nem ellenőrizzük vagy irányítjuk a felhasználók tevékenységeit a Facebookon, és nem vagyunk felelősek a felhasználók által a Facebookon továbbított, vagy megosztott tartalomért vagy információért. Nem vagyunk felelősek semmilyen sértő, kifogásolható, obszcén, törvénytelen vagy más kifogásolható tartalomért vagy információért, mellyel Ön találkozhat a Facebookon. Nem vagyunk felelősek a Facebook-felhasználók sem online, sem offline magatartásáért (...)”⁵⁴

Bizonyos esetekben a szolgáltató megszüntetheti a közösségi szolgáltatás használatának a lehetőségét is: „(...) Ha megsérti jelen Nyilatkozat tartalmát vagy szellemiségét, vagy egyéb módon számunkra kockázatot teremt, illetve lehetséges jogvitának tesz ki bennünket, akkor az Ön számára részben vagy egészben megszüntethetjük a Facebook használatának lehetőségét. Önt e-mailben vagy a fiókjához történő következő hozzáférési kísérlete során fogjuk értesíteni. Ön is bármikor törölheti a fiókját vagy letilthatja alkalmazását (...)”⁵⁵

Tekintettel arra, hogy a Facebook egy, az Egyesült Államokban működő szolgáltató, a Nyilatkozat 16. pontja speciális szabályokat állapít meg azokra a felhasználókra, akik az Egyesült Államoktól különböző államban kerültek kapcsolatba a szolgáltatásával. Így például a felhasználó hozzájárul ahhoz, hogy személyes adatait az Egyesült Államokba továbbítsák és ott dolgozzák fel.

A Nyilatkozat mellett meg kell említenünk egy másik, kiemelt fontosságú szabályzatot, a Közösségi Alapelveket (*community standards*).

A közösségi oldalak üzemeltetői kontroll alatt tartják az egész közösségi hálózatot, látják és befolyásolni tudják a felhasználók online tevékenységét, és következtetni tudnak offline életükre is. Annak fejében, hogy a közösségi hálózatokon a minden korábbinál szélesebb nyilvánosság biztosítja a polgárok hozzáférését, ezek a szolgáltatók kontrollálják a hálózati életünk szinte minden mozzanatát, a közzétett adatainkat, és maguk állapítják meg azokat a közösségi szabályokat, amelyeket a felhasználóknak be kell tartaniuk.

53 Vö. Facebook Jogi és Felelősségi Nyilatkozat 15.1. alpont (jogviták peres rendezésére kizárólagos illetékesség kikötése).

54 Uo., 15.2. alpont (szolgáltatói felelősség limitálása a felhasználói tartalmakért).

55 Uo., 14. pont (Megszűnés).

A Facebook a tiszteletteljes viselkedésre ösztönzésre vonatkozó alapelveinek áttekintő összefoglalójában a szolgáltatást olyan helyként definiálja, ahol mindenki megoszthatja véleményeit másokkal, és felhívhatja figyelmüket a számára fontos kérdésekre. Ebből eredően előfordulhat, hogy a felhasználó a sajátjától eltérő véleményekkel találkozhat. A Facebook elismeri, hogy az ellentétes nézőpontok megjelenése fontos beszélgetésekhez vezethet a nehéz témákkal kapcsolatban. Ám ahelyett, hogy mindebből a diskurzusok széles körű szabadsága mellett foglalna állást, rögzíti, hogy „(...) [a]nnak érdekében, hogy jobb egyensúlyt teremtsünk sokszínű közösségünk szükségletei, biztonsága és érdekei között, bizonyos típusú kényes tartalmakat eltávolíthatunk, vagy korlátozhatjuk közönségüket (...)”. Végso esetben pedig fenntartja magának a jogot, hogy azt, aki nem tartja be ezeket a szabályokat, akár törölheti is a – virtuális valóság általa kontrollált – platformjáról, mintegy a felhasználó ’online halálát’ okozva. A közzétett vagy megosztott vélemények között tehát a szolgáltató vállaltan szelektál, az egyén pedig nemigen hivatkozhat szabad véleménynyilvánításának a jogellenes korlátozására, tekintettel arra, hogy a közösségi platform igénybevétele, a regisztrációval átruházta a tartalom feletti ellenőrzés jogát az üzemeltetőre. Ez az a pont, amely alapvetően alakítja át a politikai diskurzusok alkotmányjogi szerkezetének korábban bemutatott rendszerét: a feje tetejére állítva azt. A magánszolgáltató által alkalmazott tartalomszűrés lehet ugyan, hogy alkotmányosan elfogadott, legitim korlátozások mentén valósul meg, mégis, a magáncenzúrát megvalósító gyakorlat végső soron képes lehet a társadalmi közvitát torzítani, tematizálni, akár politikai, akár gazdasági vagy más érdekből. A Facebook ugyanis amikor úgy dönt, hogy egy tartalmat töröl, vagy akár egy felhasználó profilját törli a közösségi hálózatról, nincs semmilyen jogilag szabályozott indokláshoz kötve, eljárásában nem jutnak érvényre az állami processzusokban feltétlenül érvényesülő garanciák.

Az elmúlt esztendőkből – szinte észrevétlenül – a Facebook a saját közösségi szabályzataival, így különösen a közösségi alapelveivel és az adatkezelési szabályzatával egy olyan globális szabályozóvá vált, amely tartalomszabályozást végez, ám annak érvényesítését objektív eljárási garanciák nélkül valósítja meg. A szerződésből levezetett joglemondás, helyesebben a szolgáltatónak szűrés jogosultsággal való felruházása, a szólásszabadság online határainak meghatározására való felhatalmazása kapcsán azonban szükségszerűen felvetődik a magánjogi szerződések tartalmának alkotmányossági kérdése. Álláspontom szerint ez az új jelenség megerősíti az alapjogok horizontális hatályának elismerését proponáló nézeteket.

A Facebook közösségi irányelveiben olyan tartalomszabályozást valósít meg, amely sok tekintetben azonos az államok által kidolgozott médiaszabályozásokból ismert rendelkezésekkel.

A közösségi alapelvek lényegében „(...) a médiaszabályozás (értsük utóbbi alatt az állami normaalkotást) klasszikus tárgyköreit, problémáit tárgyalja, és alkot azokban határokon átvíelő érvényességgel, tartalmi és eljárási normákat (...)”.⁵⁶ A Facebook az általa fenntartott közösségi hálóban kimondható vélemény határait, a szólásszabadság korlátait szabja meg – magánjogi alapon álló – normarendszerével, hiszen meghatározza, mely szólásokat nem tolerálja a közösségen belül. Ilyenek például az erőszakos és fenyegető tartalmú közlések (ide tulajdonképpen a közrendet, közbiztonságot, tulajdont, személyes biztonságot fenyegető tar-

56 NYAKAS Levente: *A Facebook leporolt közösségi irányelvei: globális versus nemzeti médiaszabályozás?* A Média-tudományi Intézet blogja, 2015. április 8.
http://mtmi.hu/cikk/708/A_Facebook_leporolt_kozossegi_iranyelvei_globalis_versus_nemzeti_mediaszabalyozas

talmakat/szólásokat sorolja a Facebook), az erőszakos, durva beszéd és meztelenséget ábrázoló tartalmak (ez a kiskorúak védelmének, a közérkölcsek kérdésének feleltethető meg) vagy éppen a gyűlöletbeszéd.⁵⁷

A tartalmi szabályokhoz hasonlóan, rendkívül fontos kitérnünk a közösségi alapelvekbe ütköző tartalmak kezelési mechanizmusára és a Facebook által alkalmazott szankciók körére. Ezek tulajdonképpen hasonlóak az államok eljárásjogi normáihoz, ám egy fontos ponton mégis eltérnek azoktól. Az állami eljárási szabályok szigorúan kötött, eljárási garanciákkal körbehatárolt eljárásrendet állapítanak meg, ezzel szemben a Facebook által lefolytatott belső vizsgálatok (*review*) ismeretlen rendben zajlanak. Az általános eljárási rend lényege, hogy egy belső normába ütköző tartalom esetén – amelyet többnyire bejelentésre észlel a Facebook –, elindul a belső vizsgálat, majd amennyiben megállapítást nyer a Facebook normáját sértő tartalom, az eltávolításra kerülhet vagy akár a felhasználó törlésével is járhat.

Hasonlóan elgondolkodtatók a Facebook kollíziós normái, amikor egy közzétett tartalom vonatkozásában a Facebook valamely normája ütközik egy adott állami jogalkotó által létrehozott jogi szabállyal. Itt két alapeset létezhet: vagy a tartalom nem sérti a Facebook normáit, de a nemzeti jogot igen, vagy fordítva. A kérdés különösen akkor válik lényegessé, amikor a Facebook megállapítja, hogy az adott tartalom nem sérti a közösség normáit, majd ezt követően arról dönt, hogy ténylegesen sérti-e a helyi jogot (sic!). Amennyiben ez utóbbit megállapítják, akkor adott tartalmat ugyan nem távolítják el, viszont blokkolják az inkriminált szöveg elérhetőségét az érintett államból.

Mindebből arra következtethetünk, hogy „(...) a Facebook úgy viselkedik, mint bármely más szuverén állam: a szólásszabadságot érintő normákat bocsát ki, azok betartását ellenőrzi, sőt, kollízió esetén, saját normáit részesíti előnyben, bizonyos kompromisszumok mellett (...)”⁵⁸ Ez különösen problematikus annak fényében, hogy a Facebook egy globális közösségi háló, amely a multikulturális világ különböző kultúrájú és jogrendszerű államaiban élő, közel kétmilliárd polgárának biztosít közös agorát.

Alkotmányjogi összefüggésben, különösen az alapjogkorlátozás szempontjából annak van jelentősége, hogy a Facebook mint transznacionális szuverén 'normaalkotó' melyik kulturális közegben (nemzeti jogban) kialakult érvényes normarendszer alapján dönt a szólásszabadság korlátairól? Talán az USA-ban érvényes normák és gyakorlat alapján, amire a székhelyéből és alávetési nyilatkozatából következtetni lehet? Vagy globális helyzetét és hatalmi pozícióját érzékelve, az államok szabályozásától teljesen függetlenül hoz létre új, leginkább a médiaszabályozás körébe eső normákat, melyek valamennyi – különböző társadalmi, kulturális háttérrel, jogi szocializációval és állampolgársággal rendelkező – felhasználóra érvényesek? A kérdésre egyértelmű választ adni nem tudunk, tekintve, hogy a normák megalkotásának motivációjára, folyamatára a transzparencia hiánya miatt nem láthatunk rá. Választ erre leginkább csak úgy kaphatnánk, ha transzparens lenne a Facebook normaalkalmazási gyakorlata, azaz a bejelentések nyomán olyan nyilvános döntések születnének, melyekből kiderülne, hogy a Facebook milyen indokok mentén talált egy tartalmat közösségi irányelvekbe ütközőnek vagy annak megfelelőnek?

A közösségi alapelvek fontos részét képezi a tiszteletteljes viselkedés ösztönzése, ennek részeként a meztelenség, a gyűlöletbeszéd és az erőszakos, durva tartalom tilalma. A meztelen-

57 Vö. uo.

58 Uo.

ség, amelynek tilalma nyilvánvalóan elsősorban a gyermekek szellemi, erkölcsi fejlődésének védelmét szolgálja, sok esetben céljával ellentétes alkalmazásának lehetünk tanúi.

A közösségi alapelvek alkalmazása gyakorta okoz indokolatlan korlátozást. Ilyen eset volt, amikor Alaura Weaver feminista blogger (*Bad-ass Motherblogger*) a női intimhygiénáról szóló blogját szerette volna fizetett poszt formájában reklámozni a Facebookon.⁵⁹ A Facebook azonban megtagadta a reklám közzétételét, először arra hivatkozva, hogy a blogban szereplő képen szereplő fürdőző nők túl sok fedetlen bőrt engednek láttatni, és az sértené a közösségi alapelvekben megfogalmazott, meztelenséget érintő politikáját. Miután a blogger lecserélte a kétséges képet Hüpatia filozófusnő képmására, a Facebook a Reklám Iránymutatására hivatkozva utasította vissza a hirdetés közzétételét. Bár a reklám közzétételét kétszer is elutasította a szolgáltató, érdemben egyik alkalommal sem indokolta meg annak valódi okát.

Hasonlóan tiltotta le a Facebook a Cancerfonden oldalát, amely a mellrák veszélyeire és a szűrővizsgálatok fontosságára szerette volna felhívni a figyelmet. A rendszer azonban törölte a hirdetésüket, mert az szexuális és felnőtteknek szóló tartalmat népszerűsített. A tiltást érdemlő esetben nem fényképfelvétel volt a kifogásolt tartalom, hanem egy rajz, amely két egymás melletti kört ábrázolt oly módon, hogy mindegyik körben három egymásban lévő kör volt látható, amelynek geometriai látványába bele lehetett képzelni két női mell kontúrját.

Koppenhágában, a Balti-tenger partján, egy szikla tetején áll Hans Christian Andersen egyik legismertebb meséjének főhősét, a kis hableányt formázó szobor. A műalkotás a tengerpart egyik legnépszerűbb turistalátványossága. A szoborról készült fényképfelvételt osztotta meg egy dán politikus, ám váratlanul a közösségi oldal törölte a tartalmat.⁶⁰ Az indoklás szerint a kis hableányról készült fotó sérti a meztelenség tilalmát, még akkor is, ha a felvételen egy szerzői mű látható. A közösségi oldal utóbb tisztázta a meztelenségről szóló iránymutatását, és a meztelenséget ábrázoló szerzői műveket ábrázoló képek közzétételét engedélyezik.

Miközben a közösségi oldalak felhasználói egyértelműen információs alapjogaikat gyakorolják a bejegyzések elhelyezésével, szerkesztésével, letöltésével, az oldalakat fenntartó cégek 'szabályzatai' alapján elvégzett törlések alkotmányossága már nehezen ellenőrizhető, hiszen a kormányzati szervek által végzett cenzúrával ellentétben, a közösségi média privát világában zajló folyamatok az oldalakat fenntartó cégek mérlegelési jogkörébe tartoznak. Így, habár sok esetben a közösségi média oldalak szabályzatai olyan, például pornográf, gyűlölködő vagy sértő tartalmakat tiltanak, amelyek bizonyos feltételekkel alkotmányosan korlátozhatók, e cégek maguk döntenek el, mi minősül pornográfának, gyűlölködőnek vagy sértőnek, és ezzel a kommunikációs alapjogok védelmi szintjét is saját belátásuk szerint alakítják.⁶¹

Amint a fenti összefoglalóból is látható, az állami szabályozás vagy önszabályozás, nemzeti vagy globális tartalomszabályozás kérdése a közösségi hálózatok vonatkozásában nem dőlt el. Az államok szabályozását és jogalkalmazását joghatósági problémák korlátozzák, míg a globális szolgáltatói szabályozási mechanizmusok által való működtetés bizonyos körben üdvözlendő, de nem jelent valódi megoldást, hiszen nem rendelkezik az alapjogkorlátozás

59 Kate Ng: Woman gets censored by Facebook because she blogs about periods, 'Women's health shouldn't be a taboo subject'. *Independent*, 2015. 11. 07. www.independent.co.uk/news/media/online/woman-gets-censored-by-facebook-because-she-blogs-about-periods-a6725176.html

60 Denmark: Facebook blocks Little Mermaid over 'bare skin', BBC, 2016. 01. 04. www.bbc.com/news/blogs-news-from-elsewhere-35221329.

61 LÁNCOS Petra Lea: *Facebook és a szűrés hatalma*. A Médiatudományi Intézet blogja, 2015. november 25. www.mtmi.hu/cikk/820/Facebook_es_a_szures_hatalma

mércéinek jogállami garanciáival, sok esetben önkényesnek, de legalábbis átláthatatlannak bizonyul. Az internetes tartalomszolgáltató általi szűrés a közönséget teszi kiszolgáltatottá, a társadalmi diskurzusokban pedig bizonyos információkhoz való hozzáférés lehetőségét korlátozhatja (magáncenzúra) az egykor minden korábbinál szélesebb hozzáférést ígérő internetes nyilvánosságban.

7. Következtetések

Az elmúlt évtizedeket az információs társadalom korának szokás nevezni, ahol a legfontosabb társadalmi kohéziós malter az információ, a tudás, szemben a korábbi évszázadokra jellemző kohezív tényezőkkel, mint a feudalizmus személyközi viszonyait meghatározó személyes hűség, lojalitás vagy az ipari társadalmakban domináns szervező erőként megjelenő tőke. A 21. századi társadalom azonban már nem csupán információs jellegű; jellegadó vonása már nem önmagában az, hogy az információn alapuló tudás az egyéni és a társadalmi haladás kulcsa. Az információ jellege alapján olyan információ, amelyet a digitális világban meghatározó jelentőségű platformokról szereznek be. Ezt a társadalmat hálózati társadalomként (*network society*) vagy legújabban platformtársadalomként (*platform society*) is szokták nevezni, ahol az online térben domináns platformok szolgáltatói határozzák meg vagy legalábbis befolyásolják az információk összetételét.

A platformok között is van néhány olyan domináns online piaci szereplő, amelyek önmagukban képesek meghatározni az internetes nyilvánosság működési mechanizmusait. Az öt nagy szolgáltató, a Google, a Microsoft, a Facebook, az Apple és az Amazon a nyilvánosság online terében betöltött megkérdőjelezhetetlen, piacvezető szerepük (bevételükre és a felhasználók számára is tekintettel) következtében az online nyilvánosság diskurzusainak vitán felül meghatározó szereplői. Ezek a platformok olyan jelentékeny befolyással bírnak (mindegyik egy meghatározott szolgáltató platformon piacvezető), hogy saját működési szabályaik (felhasználási feltételek, közösségi irányelvek), szabályozási elveik (közösségi alapelvek) az online nyilvánosságra komoly befolyást gyakorolnak. Napjainkban az online nyilvánosság információs szupersztrádjának forgalomirányítói e platformszolgáltatók. Valójában azonban még ennél is többek; a nyilvánosságban megjelenő információk összetételét is nagymértékben képesek befolyásolni. Saját szabályozási mechanizmusukban, működési-szabályozási politikájuk révén meghatározzák a nyilvánosság összetételét, az abban megjelenni képes és az onnan kiszorulni kénytelen vélemények körét. A platformszolgáltatók az általuk használt matematikai-informatikai algoritmusok révén képesek meghatározni az információáramlás jellemzőit, a nyilvánosságban érzékelhetően megjelenő információk összetételét, az információk közötti priorálás vagy éppen szelekció szempontjait. Emellett azonban arra is rámutattunk, hogy a matematikai algoritmusok, a mesterséges intelligencia, az emberi közrehatás szintén jelen van ezeken a platformokon, sőt érdemben befolyásolja is az online nyilvánosság platformjain hozzáférhető információk összetételét.

Ezek a szolgáltatók amellet, hogy felhasználóiknak meghatározott online szolgáltatást nyújtanak, olyan mechanizmusokat is működtetnek, amelyek *prime face* nem nyilvánvalóak: üzleti tevékenységük keretében további mechanizmusokat működtetnek, mint például az életünk különböző megnyilvánulásainak (számítógépes) adatokká alakítása, az egyébként nem érzékelhető jelenségek adatokon keresztül érzékelhetővé tétele (*datafication*), vagy éppen

a szolgáltatásuk során nyert adatokat üzleti értéké, árucikké alakítják át (*commodification*). De az egyik leglényegesebb működési aktivitásuk, hogy az információtömegben szelektálnak, algoritmusuk segítségével rangsorolják, szelektálják az online tartalmakat. Sok esetben a mesterséges intelligenciát kombinálják a humán közrehatással, ami csak tovább nehezíti jogi megítélésük problémáit.

Az online diskurzusok szabályozása összetett feladat, és napjainkban még jórészt megválaszolatlan kérdés. Nem kétséges ugyanakkor, hogy az online nyilvánosság nem lehet szabályok nélküli Vadnyugat. A demokratikus társadalmak nem adhatják fel az alkotmányos rendszerük vívmányait, különösen a demokratikus alapértékeket, az emberi jogok érvényesítését az online térben. A nyilvánosság online tereinek szabályozása több szereplő szoros, felelős együttműködésének eredményeként lehet csupán célravezető. Az állami szerepvállalás önmagában nem elegendő; mint egy kard nélküli lovag, az esetleges voluntarista szabályozási kísérletei a technológia sajátosságaiból fakadóan, eleve kudarcra vannak ítélve. Amennyiben azt szeretnénk, hogy a demokratikus diskurzusok torzításmentesen érvényesüljenek az internetes nyilvánosságban, úgy szükség van az állam szabályozására. Ennél azonban sokkal nehezebb kérdés, hogy milyen mértékben és mely pontokon szükséges az állami beavatkozás. Ugyanakkor az állam szabályozási vágyát nagy elővigyázatossággal kell korlátok közé szorítani. Egyfelől a közérdek érvényesítése feltétlenül megköveteli a jogi megoldásokat, másfelől egy olyan, folytonosan változó, fejlődő területen, mint az internetes kommunikációs szféra, a túlértékelt állami szerepvállalás óriási kockázatot hordoz, és több kárt okozhat, mint amennyinek az elhárítására vállalkozott. Azt is tudatosítanunk kell továbbá, hogy az internet speciális technológiája miatt a nemzeti jogalkotás aligha lehet sikeres, a szabályok megalkotását kétségkívül globális szintre kell emelni. Az európai szabályozásnak jó keretet adhat az Európai Unió jogalkotási mechanizmusa.⁶² Mindazonáltal nem vitás, hogy az államnak van szerepe a szabályozásban, de mellette komoly szerep hárul a szolgáltatókra és a felhasználókra egyaránt.

A szolgáltatókkal szemben a legfontosabb elvárás a transzparens működés biztosítása lenne, amit a jövőben megalkotott jogi szabályozási rendszer mellett a felhasználók határozott és egyértelmű érdekérvényesítése kényszeríthet ki. A különböző platformok felhasználóinak felelőssége nem csekély, divatos fordulattal élve tudatos fogyasztóvá kell válniuk. Sőt elsősorban nem fogyasztóknak, hanem felelős *citoyennek*, a demokratikus közvitát mint a demokratikus társadalmi rend oxigénjét az online 'környezetszennyezéstől' védelmező polgároknak kell lenniük, akik nem áldozzák fel a demokratikus diskurzusok működését saját kényelmük oltárán, és nem engedik, hogy Huxley szép, új világa az új hálózati, vagy ha tetszik, platform-társadalomban valósággá váljék. Még akkor sem, ha a fent bemutatott bírói gyakorlat nem feltétlenül ebbe az irányba mutat.

Az online szólásszabadságot, az interneten végbemenő disputákat oltalmazó állami intézményvédelmi kötelezettség megvalósításának konkrét eszközeit azonosítani az egyik legnagyobb kihívás, hiszen a szolgáltatások globális jellege túlmutat az állami szabályozás területi hatályán és a nemzeti jogalkalmazás joghatósági korlátain. A magánszolgáltatók alapjogot korlátozó hatalma pedig – meggyőződésem szerint – minden korábbinál élesebben veti fel a szólásszabadság horizontális hatályának széles körű elismerését.

62 Vö. KOLTAY i. m. (41. lj.) 136–137.

A web 2.0. egyes szabályozási kérdései – különös tekintettel az alkotmányjogi vonatkozásokra

KLEIN TAMÁS

1. Bevezetés

A web 2.0 szolgáltatások megjelenése és a társadalmi interakciókban tapasztalt rohamos tempójú terjedése az online nyilvánosságban az utóbbi évtized legnagyobb mértékű változása. A nyilvánosság szerkezetére gyakorolt hatása talán csak a könyvnyomtatás, vagy a médiaszolgáltatás őstípusának számító *broadcasting* megjelenéséhez mérhető. Azonban míg a Gutenberg, majd később a Marconi-galaxisok is elsősorban a nyilvánosságban elérhető információ volumenében eredményeztek radikális növekedést, illetőleg az információ eljuttatásának új és társadalmi szinten hatékonyabb közvetítését eredményezték, és ez részben igaz a webes tartalmak eredeti formájú megjelenésére is, addig a web 2.0 a nyilvános fórum alapvető struktúrájában hoz újdonságot. A web 2.0 a polgárok interperszonális kommunikációs modelljére, magánérinkezéseire és a demokratikus diskurzusokra is olyan megtermékenyítő hatással volt, amely kérlelhetetlenül hat a nyilvánosság korábbi szerkezetére, létrehoz a nyilvánosság egészét tekintve egy új réteget és megváltoztatja az egyes szereplők kommunikációs folyamatokban elfoglalt pozícióját. A web 2.0 alapvető vonása, hogy a felhasználók nem csak passzivitásra kárhoztatott alanyai, fogyasztói, hanem aktív részesei lehetnek a netes tartalom alakításának és alakulásának, dinamikus módon maguk hozhatnak létre, oszthatnak meg információkat, adatokat, tartalmakat. A nyilvánosságnak ebben a szerkezetében megváltozik a korábbi kapuőrök évszázados szerepe, és megjelennek olyan új közvetítők, akik a platformot kínálják a nyilvános diskurzusokat aktívan alakító felhasználói működéshez és kommunikációs hidat képeznek ennek az új szerkezetű nyilvánosságnak a szereplői között, például összekapcsolják a tartalmat keresőket és kínálókat, az ismerősöket. A web 2.0 alapú szolgáltatásoknak olyan újszerű technológiai jellemzői vannak, amelyek több alkotmányjogi kérdést is felvetnek. Az egyik ilyen aspektusként kell utalni a szólásszabadság klasszikus értelmezése előtt álló kihívásra.

Az adattárolás (ide értve a felhasználók személyes adatainak tárolását is) a web 2.0 platformokon (tekintettel arra, hogy hálózatos szerkezetben működnek) már nem egy, a felhasználó ellenőrzése alatt álló, fizikailag is rendelkezésére álló és ellenőrzése alatt tartott eszközön (pl. számítógép) valósul meg, hanem felhő alapú szolgáltatások tárhelyein, a felhasználóktól távol történik. A platformok használatáért a felhasználók első pillantásra úgy érzékelhetik, nem kell használati díjat fizetni (ti. a szolgáltatások igénybevételéért az ellenszolgáltatás tipikusan nem pénzbeli), ellenben a felhasználók online tevékenységük után hátrahagyott üzleti értékkel bíró adataikat, digitális lábnyomukat (*digital footprint*) a platform működtetője üzleti céllal, reklám céljára, az ebben érdekelt társaságoknak értékesíti. A felhasználók és szolgáltatást kínálók visszajelzéseket adnak és kapnak, amelyek orientálják a többi felhasználót, illetve szolgáltatást kínálót (vö. *datafication*, *commodification*). A felhasználói szokások, az online tevékenység monitorozása (keresések, megosztások alapján meghatározott érdeklődési kör) során olyan értékkel bíró adatok keletkeznek, amelyek kereskedelmi forgalomban értékesíthetők.

Az interneten minden ingyenesen elérhető ígérete tehát csak mítosz, súlyos árat fizetnek a felhasználók minden ingyenesnek hitt keresés kezdeményezése, megosztás klikkelése során.

A web 2.0 kifejezés olyan internetes szolgáltatásokat felölelő gyűjtőfogalom (*genus proximum*), amelyek elsősorban a közösségi aktivitásra, kooperációra épülnek, ahol a felhasználók egyszerre befogadók és megosztók: közösen készítik a tartalmakat és/vagy osztják meg egymás információit. Ellentétben a korábbi nyilvánossági modellel, amelyben a tartalmat a szolgáltatást nyújtó fél biztosította (könyv- lapkiadók, médiaszolgáltatók, internetes portálok), a web 2.0 típusú szolgáltatásoknál a szerver üzemeltetője többnyire csupán az infrastruktúrát biztosítja, a tartalmat maguk a felhasználók hozzák létre, teszik hozzáférhetővé, és véleményezik. A felhasználók a web 2.0 modellű nyilvánosságtérben (folyamatos) interakcióban vannak egymással, és eseti, vagy tartós kommunikációs kapcsolatot alakítanak ki egymás között. A felhasználók ilyen aktivitása a nyilvánosságnak egy hálózatos modelljét alakította ki, amelynek napjainkban legmagasabb szervezettségű megvalósulása a közösségi hálózatok, médiumok (*social network, social media*) rendszere.

Tim O'Reilly szerint a web 2.0-s szolgáltatások meghatározott, és az alábbiakban röviden bemutatott, karakterisztikus jellemzőkkel rendelkeznek.¹

- A web maga a platform: web 2.0 esetén a cél olyan alkalmazások fejlesztése, melyek webes felület segítségével képesek a normál asztali alkalmazások tulajdonságait és teljesítményét nyújtani (például ilyen a web szövegszerkesztője, a Google Docs).
- Az adat, mint hajtóerő: a felhasználó rendelkezik az információval, amit saját maga szerkeszthet, és tehet közzé. Ezért is nevezhetjük a web 2.0 alkalmazásokat adatvezérelt rendszereknek.
- Partecipáción (bevonódáson) alapuló tervezés: a nyilvánosságban érzékelhető jelenségeket, eseményeket a felhasználó irányítja, a felhasználó aktív, nélkülözhetetlen közreműködésével (bevonódás) jönnek létre a web 2.0 tartalmak.
- Komponensalapú fejlesztés: az alkalmazások gyakran nem egy fejlesztő tevékenysége eredményeként, hanem több közreműködő közös teljesítménye révén alakulnak ki.
- Laza szervezeti struktúra: amelyet a tartalom és szolgáltatás közzététele tesz lehetővé (Creative Commons, „Some rights reserved”, Open Source Culture).

2. A közösségi hálózatok és a szólás szabadsága²

A közösségi oldalakat üzemeltető szolgáltatók működése, sok tekintetben túllép a klasszikus jogi szabályozás joghatósági peremfeltételein. A szolgáltatások határokon átvelő, globális jellege miatt, a közösségi platformok szabályozása a nemzetállami szuverenitás tanára épülő állami jogalkotási dokumentumokkal nem lehetséges. A közösségi platform szolgáltatói rendszerint maguk alkotnak szabályokat, amelyekkel meghatározzák a szolgáltatási

¹ Tim O'REILLY: *What is Web 2.0?* O'Reilly Media, Inc. 2009.

² A közösségi hálózatok szabályozási kérdéseiről ld. e kötetben részletesebben Az online diskurzusok egyes szabályozási kérdései c. tanulmányt, továbbá: PAPP János Tamás: Az én házam az én váram – A szólásszabadság érvényesülése a közösségi médiában. In: KOLTAY András – TÖRÖK Bernát (szerk.): *Sajtószabadság és médiajog a 21. század elején* 3. Budapest, Wolters Kluwer, 2016. 403-425. és PAPP János Tamás: A közösségi oldalak felhasználási feltételeinek jogi természete. In: KOLTAY András – TÖRÖK Bernát (szerk.): *Sajtószabadság és médiajog a 21. század elején* 4. Budapest, Wolters Kluwer, 2017. 187-212.

platformjukon a véleménynyilvánítás kereteit, a kimondhatóság határait. A szolgáltatók által alkotott szabályok lényegében egy sajátos 'tartalomszabályozást' hoznak létre.

A közösségi platformok közül sok tekintetben kiemelkedik a Facebook közösségi oldal, ezért röviden ennek a közösségi médiumnak a közösségi alapelvein (*community standards*)³ keresztül mutatok rá néhány problémára.

A közösségi oldalak üzemeltetői kontroll alatt tartják az egész közösségi hálózatot, látják és befolyásolni tudják a felhasználók online tevékenységét, és következtetni tudnak offline életükre is. Bár a közösségi hálózatokon a minden korábbinál szélesebb nyilvánosság biztosítja a polgárok hozzáférését, a szolgáltatók azonban kontrollálják hálózati életünk szinte minden mozzanatát, a közzétett adatainkat, és maguk állapítják meg azokat a közösségi szabályokat, amelyeket a felhasználóknak be kell tartaniuk.

A Facebook a tiszteletteljes viselkedés ösztönzésére vonatkozó alapelveinek áttekintő összefoglalójában a szolgáltatást olyan helyként definiálja, ahol mindenki megoszthatja élményeit másokkal, és felhívhatja figyelmüket a számára fontos kérdésekre, ezért előfordulhat, hogy a felhasználó a sajátjától eltérő véleményekkel is találkozik. A Facebook elismeri ugyan, hogy az ellentétes nézőpontok megjelenése fontos beszélgetésekhez vezethet a nehéz témákkal kapcsolatban, ám ahelyett, hogy mindebből a diskurzusok széleskörű szabadsága mellett foglalna állást, rögzíti, hogy „(...) [a]nnak érdekében, hogy jobb egyensúlyt teremtsünk sokszínű közösségünk szükségletei, biztonsága és érdekei között, bizonyos típusú kényes tartalmakat eltávolíthatunk, vagy korlátozhatjuk közönségüket (...)”. Végso esetben pedig fenntartja magának a jogot, hogy azt, aki nem tartja be ezeket a szabályokat akár törölheti is – a virtuális valóság általa kontrollált – platformjáról. A közzétett, vagy megosztott vélemények között tehát a szolgáltató vállaltan szelektál, a felhasználó pedig nem igen hivatkozhat a szabad véleménynyilvánításának a jogellenes korlátozására, tekintettel arra, hogy a közösségi platform igénybevételével, a regisztrációval átruházta a tartalom feletti ellenőrzés jogát az üzemeltetőre.⁴ Ez az a pont, amely alapvetően alakítja át a politikai diskurzusok alkotmányjogi szerkezetének korábban klasszikus rendszerét: a feje tetejére állítva azt. A magánszolgáltató által alkalmazott tartalomszűrés nem kizárt, hogy alkotmányosan elfogadott, legitim korlátozások mentén valósul meg, mégis a magáncenzúrális gyakorlat végső soron képes lehet a társadalmi közvitát torzítani, tematizálni, akár politikai, akár gazdasági, vagy más érdektől vezérelve. A Facebook ugyanis, amikor úgy dönt, hogy egy tartalmat töröl, vagy akár egy felhasználó profilját törli a közösségi hálózatról, nincs semmilyen jogilag kötött indokoláshoz kötve, eljárásában nem érvényesülnek az állami processzusokban feltétlenül érvényesülő garanciák. A szerződésből levezetett joglemondás kapcsán azonban szükségszerűen felvetődik a magánjogi szerződések tartalmának alkotmányossági kérdése. Álláspontom szerint, ez az új jelenség megerősíti az alapjogok horizontális hatályának elismerését proponáló nézeteket.

Az elmúlt esztendőkből, szinte észrevétlenül a Facebook saját közösségi szabályzataival (különösen a közösségi alapelveivel, és adatkezelési szabályzatával) egy olyan globális szabályozóvá vált, amely tartalomszabályozást végez, ám annak érvényesítését objektív eljárási garanciák nélkül valósítja meg.

3 Közösségi alapelvek, www.facebook.com/communitystandards#

4 Vö. Jogi és Felelősségi Nyilatkozat, www.facebook.com/legal/terms

A közösségi alapelvek tehát lehetővé teszik, hogy a Facebook bizonyos típusú kényes tartalmakat eltávolítson, vagy korlátozza közönségüket. Ez bizonyos esetekben sértheti a szólás-szabadság tartalomsemleges védelmének alkotmányos követelményét.

„(...)A szabad véleménynyilvánításhoz való jog a véleményt annak érték- és igazságtartalmára tekintet nélkül védi. Egyedül ez felel meg [...] az ideológiai semlegességnek. [...] A véleménynyilvánítás szabadságának külső korlátai vannak csak; amíg egy ilyen alkotmányosan meghúzott külső korlátba nem ütközik, maga a véleménynyilvánítás lehetősége és ténye védett, annak tartalmára tekintet nélkül. Vagyis az egyéni véleménynyilvánítás, a saját törvényei szerint kialakuló közvélemény, és ezekkel kölcsönhatásban a minél szélesebb tájékozottságra épülő egyéni véleményalkotás lehetősége az, ami alkotmányos védelmet élvez. Az Alkotmány a szabad kommunikációt – az egyéni magatartást és a társadalmi folyamatot – biztosítja, s nem annak tartalmára vonatkozik a szabad véleménynyilvánítás alapjoga. Ebben a processzusban helye van minden véleménynek, jónak és károsnak, kellemesnek és sértőnek egyaránt, különösen azért, mert maga a vélemény minősítése is e folyamat terméke.”⁵

A Facebook, amikor szabályozza az elfogadható és elfogadhatatlan beszédet, akkor magánjogi alapon álló normarendszerével az általa fenntartott közösségi platformon kimondható vélemény határait, a szólásszabadság korlátait szabja meg, hiszen meghatározza azon szólások körét, amelyeket nem tolerál a közösségen belül.

A tartalmi szabályokhoz hasonlóan, fontosnak vélem megemlíteni a közösségi alapelvekbe ütköző tartalmak kezelési mechanizmusának és a Facebook által alkalmazott szankcióknak a kérdését is. Az állami eljárási szabályok szigorúan kötött, eljárási garanciákkal körbehatárolt eljárásrendet állapítanak meg, ezzel szemben a Facebook által lefolytatott belső vizsgálatok (*review*) ismeretlen rendben zajlanak. Az általános eljárási rend lényege, hogy egy belső normába ütköző tartalom esetén, amelyet többnyire bejelentésre észlel a szolgáltató, elindul a belső vizsgálat, majd amennyiben megállapítást nyer a Facebook-norma sértő tartalom, úgy eltávolításra kerülhet, vagy akár a felhasználó törlésével is járhat.

Nem kevésbé aggályosak a Facebook kollíziós normái, amikor egy közzétett tartalom vonatkozásában a Facebook valamely normája ütközik egy adott állami jogalkotó által létrehozott jogi szabállyal (*local law*). Itt két alapeset létezhet: vagy a tartalom nem sérti a Facebook normáit, de a nemzeti jogot igen, vagy fordítva. A kérdés különösen akkor válik lényegessé, amikor a Facebook megállapítja, hogy nem sérti az adott tartalom a közösség normáit, majd ezt követően arról dönt, hogy ténylegesen sérti-e a helyi jogot (sic)! Amennyiben utóbbi megállapításra kerül, akkor az adott tartalmat ugyan nem távolítják el, viszont blokkolják az inkriminált szólás elérhetőségét az érintett államból.

Mindebből arra következtethetünk, hogy a Facebook úgy hoz létre a szólásszabadságot érintő normákat és úgy ellenőrzi betartásukat, mint egy szuverén állam, sőt kollízió esetén saját normáit részesíti előnyben, bizonyos kompromisszumok mellett. Ez különösen problematikus annak fényében, hogy a Facebook egy globális közösségi háló, amely a multikulturális világ különböző kultúrájú és jogrendszerű államaiban élő, közel kétmilliárd polgárnak biztosít közös agorát.

„(..)A közösségi oldalak felhasználói egyértelműen információs alapjogaikat gyakorolják, egyúttal hozzájárulnak a közéleti diskurzusok pluralitásához, ezzel szemben az oldalakat fenntartó szolgáltatók «szabályzatai» alapján elvégzett törlések alkotmányossága már nehezen ellenőrizhető, hiszen a kormányzati szervek által végzett cenzúrával ellentétben a közösségi média privát világában zajló folyamatok az oldalakat fenntartó cégek mérlegelési jogkörébe tartoznak. Így habár sok esetben a közösségi média oldalak szabályzatai olyan, például pornográf, gyűlölködő vagy sértő tartalmakat tiltanak, amelyek bizonyos feltételekkel alkotmányosan korlátozhatók, e cégek maguk döntenek el, mi minősül pornográf, gyűlölködőnek vagy sértőnek és ezzel a kommunikációs alapjogok védelmi szintjét is saját belátásuk szerint alakítják(..)”.⁶

3. Frekvenciaszűkösség után szűrőbuborék? – a személyre szabott tartalomkínálat csapdája⁷

A keresőmotor-szolgáltatók, az online értékesítés platformok (web áruházak) és a közösségi hálózatok egyaránt alkalmaznak olyan informatikai megoldásokat, amelyekkel figyelemmel kísérik felhasználóik online tevékenységét, aktivitásukról a fogyasztói szokások elemzésére alkalmas adatokat gyűjtenek. A magunk után hagyott, a bevezetőben már röviden bemutatott digitális lábnyom (látogatott oldalak, keresési előzmények, közösségi kapcsolatok, tetszésnyilvánítások, egyéb reakciók, felhasználói csoport aktivitás stb.) alapján a szolgáltatók felhasználóikról kialakítanak egy *digitális személyiségprofil*, amelyből előre igyekeznek meghatározni, hogy őket milyen jellegű, milyen tematikájú tartalmak érdeklik, milyen típusú hírekkel, véleményekkel kívánnak találkozni, milyen termékek megvásárlását, vagy szolgáltatás igénybevételét érdemes számukra ajánlani. Az online tevékenységből kinyerhető információk adatelemzését követően, a felhasználói preferencia alapján személyre lehet szabni a felkínált tartalmat. Ennek a szolgáltatói tevékenységnek az egyik lényeges mozgatója a web 2.0-t jellemző üzleti modellben keresendő, hiszen a felhasználóknak ingyenesen nyújtott szolgáltatások piaci értéke abban áll, hogy ezeknek az adatoknak jelentékeny piaci értéke van. A tartalmak mellett elhelyezett kereskedelmi üzenetek, reklámok is egyénre szabottá válnak, a reklámozó partnerek hirdetéseit az arra leginkább fogékony felhasználóknál helyezi el a szolgáltató.

A kereskedelmi jellegű üzenetek egyénre szabott, célzott eljuttatása azonban csak a web 2.0 egyik kísérőjelensége. Megfigyelhető egy másik, álláspontom szerint alkotmányelméleti szempontból veszélyesebb következmény: a nem reklámcélú tartalmak egyénre fazonírozása. A szolgáltatók által hangoztatott érvelés igencsak tetszetős: az egyénre szabott tartalomkínálat megkíméli a felhasználót az információtengerben való alámerüléstől, s célzatosan azokat a

6 LÁNCOS Petra Lea: *Facebook és a szűrés hatalma*. A Médiatudományi Intézet blogja, 2015. november 25. www.mtmi.hu/cikk/820/Facebook_es_a_szures_hatalma

Különösen vitatott lehet egyes tartalmak sértő, pornográf jellegének megítélése, általános fogalmi keretek esetlegessége: amint Potter Stewart bíró fogalmazott az obszcenitás fogalmi meghatározhatóságáról, alkotmányos korlátozhatósága kapcsán: „I know it, when I see it.” [Jacobellis v. Ohio (378 U.S. 184)], vö. UDVARY Sándor: *Alkotmányos médiajog*. Budapest, KRE ÁJK, 2008. 67-69.

7 A téma részletes elemzését l. POLYÁK Gábor: *A frekvenciaszűkösségtől a szűrőbuborékig*. In: TÓTH András (szerk.): *Technológia jog*. Budapest, KRE ÁJK, 2016. 116-140.

tartalmakat ajánlja megismerésre, amelyek egyébként is – hosszas böngészés, keresgélés után – felkeltenék érdeklődését.

A sajátunktól eltérő, azzal ellentétes vélemények megismerése valóságérzékelésünknek fontos részét képezi. Az ember antropológiai jellemzője miatt ugyan általában nem szívesen szembesül a sajátjától eltérő nézetekkel, sőt egyesek saját felfogásukat az abszolút igazsággal azonosítják. John Stuart Mill a véleménynyilvánítási szabadság egyik első teoretikusa határozottan hitt a szabad közvitában, a különböző nézetek ütköztetésének értékében, a vélemények társadalmi szinten megvalósuló szabad harcában győzedelmeskedő igazságban. Az igazság felismerése, az abszolút igazságra való eljutás azonban nem csak a társadalom szintjén kívánatos. Mill azt is fontosnak véli, hogy az egyén a saját maga igazságait is megmérje mások igazságának a fényében, saját gondolatait tükröztesse másokéban. Mill, a szabadságról szóló elméleti munkájában egyértelműen rögzíti, hogy „(...) nincs tévedhetetlen ember, a vita elhallgattatása [pedig] mindig egyenértékű a csálhatatlanság feltételezésével, (...)” azzal, hogy egyesek azt feltételezik, hogy „(...) bizonyosságuk azonos az abszolút bizonyossággal (...)”.⁸ A szabad vitában, eszmecserében meg nem méretett álláspont végül halott dogmává válik és kiüresedik.

Az ember, mint racionális (értelmes és erkölcsös) lény rendelkezik azzal a – Mill szóhasználatával – tiszteletreméltó tulajdonsággal, hogy kijavítsa a saját hibáját. A hiba feltárásához azonban rendre valamiféle külső inger, empíria (tapasztalat) szükséges, amelyben a hiba felismertté, majd azonosítottá válik, és amelyet a racionálisan gondolkodni képes ember vitában képes megtapasztalni, ugyanis az ilyen vitát megjelenítő diszkuszióban fog eldőlni, hogyan is kell értelmezni a tapasztalatot.⁹

Amikor az egyén a web 2.0 nyilvánosságában nem találkozik a sajátjától különböző nézetekkel, akkor ennek az empíriából fakadó felismerésnek a lehetőségétől esik el, szélesebb összefüggésben az önkorrekció lehetőségétől. Az algoritmusok által kialakított online identitás és az arra tekintettel felkínált, személyre szabott tartalomkínálat azonban önbeteljesítő hatású. A szolgáltatást igénybe vevő felhasználó idővel elszigetelődik a sajátjától különböző álláspontoktól, információktól, hiszen a szolgáltató folyamatosan monitorozza a tevékenységét, és annak figyelembe vételével generálja a tartalmakat. A felhasználói tudatosság csak ritkán éri el azt a szintet, hogy kifejezetten a sajátjával ellentétes vélemények megismerésére is időt és fáradságot fordít, miközben Mill éppen ennek a jelentőségére hívja fel figyelmünket – máig ható érvénnyel, vagy talán érvényesebben, mint korábban bármikor. A digitális lábnyomból nyert adatokból meghatározott személyiségrajz alapján jön létre az egyénésített keresőmotor-találat, a közösségi hálózat médiatípusú felületén kínált hírfolyam, az online áruházak ajánlatai.

A felhasználók általában saját akaratuktól függetlenül, vagy éppen azzal ellentétben egyre inkább egy 'online véleménygetetőba' kerülnek, Cass R. Sunstein megfogalmazása szerint *kiberkaszkádok* jönnek létre.¹⁰ Ezt a jelenséget először Eli Pariser írta le, és szűrőbuboréknak (*filter bubble*) nevezte.¹¹ A szűrőbuborék egy olyan mesterségesen létrehozott, virtuális információs tér, amelyben a felhasználónak fokozatosan csökken az esélye a sajátjától különböző álláspontok, vélemények megismerésére, s így végül egy téves valóságérzékelés csapdájába kerül.

8 John Stuart MILL: *A szabadságról*. Budapest, Századvég, 1994. 25-26.

9 Vö. uo., 29.

10 Cass R. SUNSTEIN: *Republic.com 2.0*. Budapest, Wolters Kluwer, 2013. (különösen 81-91.)

11 Eli PARISER: *The Filter Bubble. What the internet is Hiding from You*. New York, The Penquin Press, 2011.

A szűrőbuborék teremtette technológiai következményként, de nem technikai szükségszerűségként kialakuló szűkösség, újra aktuálissá teszi a frekvenciaszűkösség idején kidolgozott alkotmányjogi érvelések felelevenítését. Az állami intézményvédelem új útjainak megtalálása még várat magára. A szabályozási környezet merőben más, mint a nemzeti médiapiacok frekvenciaszűkössége idején, hiszen az internet mint globális piac állami szabályozása, szinte lehetetlen vállalkozás.

4. Valótlan hírek a vélemények piacán – álhírek a demokratikus nyilvánosságban

A legújabb jelenség az álhírek, 'kamuhírek' (*fake news*) megjelenése és terjedése. Ezek a tartalmak bár feltűnnek nyomtatott kiadványokban és a lineáris médiaszolgáltatók műsoraiban is, mégis leginkább az online nyilvánosság egyes felületeire jellemzők. Amíg a hagyományos sajtótermékekben és elektronikus médiában ezek a tudatosan torzított tartalmú hírek többnyire a közönség nagy része számára érzékelhetően valótlanok, addig az internetes nyilvánosságban általában kevésbé felismerhetők. Az online platformok közül leginkább a közösségi médiában megjelenő álhírek felismerhetetlenek. Az álhírek tömege jellemzően olyan gazdasági érdekeltségű szereplőkhöz kötődik, amelyek bármilyen áron tartalmaik olvasottságának növelésére törekszenek. „Ma sajnos azok állnak nyerésre, akiknek célja a legtöbb kattintás elérése, nem pedig a legtöbb igazság kimondása, és ez megöli a gondolkodást” – fogalmazott Tim Cook, az Apple vezére.¹²

A tudatosan valótlan tartalmak az online nyilvánosságban különböző formában jelennek meg. A legtipikusabb jelenséget kamuhíreként (*fake news*) azonosíthatjuk, olyan hírek álcázott tartalmakként, amelyek szándékosan valótlan tartalmúak és céljuk a megtévesztés. Az álhírek mellett további nyilvánosságtorzító hatást eredményeznek az ún. *kattintásvadász kamuoldalak*. Ezek a valós tartalmat nem szolgáltató, tehát a nyilvánosság pluralitását nem szolgáló áldoldalak olyan népszerű, látogatott oldalak nevével, webcímével élnek vissza, amelyek óriási kattintási statisztikákat generálnak, amelyet a piac reklámelhelyezés formájában honorál a számukra. Ezek az áldoldalak azonban éppen ezzel a helyzettel élnek vissza, arra építenek, hogy összekeverjék őket más, népszerű oldalakkal. A Facebook a közelmúltban ígéretet tett, hogy a hírfolyamából megpróbálja kiszűrni az ilyen megtévesztő linkeket.

A *fake news* jelenséggel kapcsolatban, úgy vélem a legfontosabb elméleti kérdés az, hogy megilleti-e az álhíreket Milton,¹³ Mill, Meikljohn eszméi, ideái, a szólásszabadság klasszikus igazolásai alapján az alkotmányos védelem? A dilemma bár erősen teoretikus jellegűnek hathat, annak eldöntése – álláspontom szerint – végső soron az alapjog gyakorlati érvényesülése, és a demokratikus diskurzusok működése szempontjából is meghatározó jelentőséggel bír. Úgy tűnik számomra, hogy amennyiben az alkotmányos védelem szintje azonos, úgy a társadalmi diskurzusok az állami, vagy üzleti, piaci propaganda hálójába ragadnak, s olyan

12 Fake news is killing people's minds, says Apple boss Tim Cook <http://www.telegraph.co.uk/technology/2017/02/10/fake-news-killing-peoples-minds-says-apple-boss-tim-cook/>

13 A szabadelvű miltoni gondolatot állította a modern kommunikációelméleti mintákkal szembe UDVARY i. m. (6. lj.) 35.

dezintegrált nyilvánosság alakul ki, amelyben lehetetlenné válik a racionális elvek szerint szerveződő közvélemény fennmaradása. Ahogy azt az AB egy korai határozatában (máig ható érvénnyel) megfogalmazta: „(...) az egyéni véleménynyilvánítás, a saját törvényei szerint kialakuló közvélemény, és ezekkel kölcsönhatásban a minél szélesebb tájékozottságra épülő egyéni véleményalkotás lehetősége szenvedne csorbát (...)”. Hiszen a véleménynyilvánítás alapjoga a szabad kommunikációt – az egyéni magatartást és a társadalmi folyamatot – biztosítja.” A *fake news* alkotmányos védelemben részesítése pedig éppen a demokratikus közvélemény kialakulásához és fennmaradásához elengedhetetlen társadalmi folyamatot tenné diszfunkcionálissá.

„(...) Az egyéni véleménynyilvánítási szabadság szubjektív joga mellett [a szólás- és különösen a sajtószabadság alapjából] következik a demokratikus közvélemény kialakulása feltételeinek és működése fenntartásának biztosítására irányuló állami kötelezettség. A szabad véleménynyilvánításhoz való jog objektív, intézményes oldala nemcsak a sajtószabadságra, [...] vonatkozik, hanem az intézményrendszernek arra az oldalára is, amely a véleménynyilvánítási szabadságot általánosságban a többi védett érték közé illeszti. Ezért a véleménynyilvánítási szabadság alkotmányos határait úgy kell meghatározni, hogy azok a véleményt nyilvánító személy alanyi joga mellett a közvélemény kialakulásának, illetve szabad alakításának a demokrácia szempontjából nélkülözhetetlen érdekét is figyelembe vegyék. (...)”¹⁴

„(...) A szabad véleménynyilvánításhoz való jog [...] nem csupán alapvető alanyi jog, hanem e jog objektív, intézményes oldalának elismerése egyben a közvélemény, mint alapvető politikai intézmény garantálását is jelenti (...)”¹⁵

Amennyiben azonban a fenti kérdésre (a *fake news* jellegű szólások alkotmányos védelmének mércéje tekintetében) a válaszuk nemleges, vagyis a hagyományos alkotmányos kritériumok, korlátozási tesztek alkalmazását elvitatjuk a *fake news* esetében, úgy feladjuk azt az évszázados liberális alkotmányos alapjogi krédót, amely határozottan fogalmazza meg az érték- és igazságtartalmára tekintet nélkül védelmet élvező, csak *külső korlátaira* figyelemmel korlátozható szólásszabadságot.

A *fake news sui generis* korlátozhatóságával kapcsolatban továbbá adódik a kérdés, hogy milyen mércék, tesztek, definiált kritériumrendszer alapján lenne megállapítható egyes szólások *fake news* jellege? Egyáltalán ki lenne jogosult meghatározni – egy kapuőrök nélküli nyilvánosságban – hogy mi a *fake news*?¹⁶ Amennyiben a *fake news* azonosítására jogszabály által hatáskörrel felruházott magánszolgáltatók lennének jogosultak, akkor milyen intézményes garanciák védenék az online szólásszabadságot a piaci, üzleti, vagy akár politikai érdekeket is érvényesítő magáncenzúrától? A magánszolgáltatók szabályozó és/vagy tartalomszűrési tevékenységével szemben ugyanis – amint azt fentebb már jeleztük – az egyik legerősebb érv, hogy eljárásrendjükben nem érvényesülnek azok az eljárási garanciák, amelyek az online szólásszabadság érvényesülését képesek lennének biztosítani.

14 AB hat. i. m. (5. lj.) 167, 172.

15 Vö. AB hat. i. m. (5. lj.) 178.

16 Potter STEWART bíró elhíresült *bon mot*-ja ebben az esetben nem segítené a válaszadást, aki a hard-core pornográfia fogalmának meghatározási bizonytalanságával összefüggésben állapította meg a Jakobelis v. Ohio ügyben, hogy „I know it when I see it.”

Az álhírek terjedése hasonlóan komoly veszélyt jelent a demokratikus nyilvánosság egészséges működésére, mint a diskurzusok pluralitását elszíntelenítő szűrőbuborék. Az álhírek, a tudottan valótlan információkkal operáló 'tájékoztató' tevékenység súlyosan torzíthatja az egyéni véleményalkotás folyamatát, s így áttételesen a saját törvényei szerint kialakuló közvélemény¹⁷ törvényszerűségeivel visszaélve, végső soron a demokratikus eljárások torzulását is eredményezheti. Az álhírek visszaszorítását sokan a piaci szereplők, a platformok összehangolt fellépésétől várják, hiszen a szolgáltatók – különösen a közösségi hálózatok üzemeltetői – rendelkezhetnek olyan eszközökkel, amelyek eredményre vezethetnek. Ám itt visszajutunk a közösségi hálózatok szűrési tevékenységének szólás- és sajtószabadságot fenyegető problematikájához. Ha a közösségi hálózat automatikus szűrőprogramok segítségével, vagy akár emberi szerkesztési tevékenység során elkezdi szelektálni a tartalmakat, mégis ki határozza meg, hogy mi az igaz és mi nem az?

Milton szenvedélyesen érvelt a hamis tények szükségessége mellett: „Hadd birkózzon egymással igazság és hazugság, hisz ki látott már olyat, hogy az igazság szabad, nyílt küzdelemben alulmaradt volna?”¹⁸ Persze Milton gondolatát nyilvánvalóan atavizmus napjaink tudatosan gyártott hamis híreinek védelmében citálni. Mégis érdekes emlékeztetni arra, hogy Milton az Elveszett paradicsomban még az ellentmondás, a viszály, a bűn megtestesítőjének, a Sátánnak is megadja a lehetőséget arra, hogy saját szempontjait, érveit, nyílt küzdelemben megvédje. Az is igaz, hogy az online álhírekkel szemben a nyílt küzdelemben való fellépés lehetősége is kétséges, hiszen azoknak nem céljuk, hogy önmaguk igazságát egy valós társadalmi diskurzusban igazolják.

A kérdés úgy is feltehető, hogy vajon mi jelent kisebb veszélyt a demokratikus diskurzusokra, az álhírek tömeges terjedése következtében toxicizált nyilvánosság, vagy a szolgáltatók újabb kontroll funkciójának a megteremtése, esetleg egy itt nem érintett lehetőség, az alapjogok horizontális hatályú védelmének kiterjesztése?

Az online szcéna történéseit szemlélve, még az sem zárható ki, hogy a közeljövőben beköszönt a már egyszer temetett kapuőrök reneszánsza.

17 Vö. AB hat. i. m. (5. lj.) 167. 179.

18 John MILTON: *Areopagitica*, magyar fordítást l. John MILTON: *Az angol forradalom tükre*. Budapest, Gondolat, 1975. 86.

A web 2.0 versenyjogi vonatkozásai

TÓTH ANDRÁS*

1. Bevezetés

A digitalizáció az elmúlt évtizedben nem csak nagy mennyiségű adat létrejöttével járt, de megeremtetette az adatok elemzésének és felhasználásának új lehetőségeit is, amelyeket a mesterséges intelligencia megsokszorozni látszik.¹ Más oldalról az, hogy a felhasználók ennyi adatot hagynak hátra az interneten, visszavezethető a web 2.0 elterjedésére, amellyel szintet lépett az internet alapú gazdaság a 2000-es évek második felében, hiszen új üzleti modellek alkalmazására nyílt lehetőség. A web 2.0 lényege, hogy a felhasználók nem csak passzív alanyai, fogyasztói, hanem aktív részesei a netes tartalom alakításának és alakulásának, maguk hozzanak létre, osszanak meg információkat, adatokat, tartalmakat dinamikus módon.

Ebben a közegben megjelennek olyan közvetítők, akik a platformot kínálják ezen felhasználói működéshez és például összekapcsolják a tartalmat keresőket és kínálókat (pl. Google kereső, eBay, Amazon), vagy az ismerősöket (pl. Facebook).² A web 2.0 alapú felhasználásnak a legfőbb jellemzője, hogy a platformok használatáért a felhasználó alapesetben nem pénzzel fizet, hanem a hátrahagyott adatait a platform működtetője reklám célból felhasználja. Sajátos kétoldalú piac jön ezzel létre, melynek lényege a platform két oldala közötti interakció: minél több felhasználója van a platformnak, annál több hirdető jelenik meg rajta, tovább növelve a platform bevételeit, amelyből további felhasználókat vonzó tartalmakat, funkciókat tud bevezetni. A platformnak az lesz az érdeke, hogy a felhasználók figyelmének minél nagyobb szeletét ő kösse le, ezáltal több személyes adatra tegyen szert, amelyek alapján képes a hirdetőknak és a felhasználóknak maguknak is több és értékeesebb szolgáltatást nyújtani. Ez egy olyan kört indít el, amelynek a végén a piac át is billenhet az ilyen platform javára (l. Google keresője, Amazon piactere, Facebook közösségi médiája) és szinte egyeduralkodóvá válhat.

Jelen tanulmány be kívánja mutatni ezen adatalapú piacok versenyjogi szempontból meghatározó jellemzőit (2. pont), foglalkozik azzal a kérdéssel, hogy létrejöhet-e a személyes adatokra alapítottan piaci hatalom (3. pont), lehet-e a versenyjog az adatvédelem eszköze (4. pont), és milyen versenyjogi problémák merülhetnek fel a személyes adatokat felhasználó online platformokkal (5. pont).

* Tanszékvezető egyetemi docens, Károli Gáspár Református Egyetem, Állam- és Jogtudományi Kar Informatikai Jogi Tanszék. E-mail: toth.andras@kre.hu.

1 ECORYS B.V.: *Big data and competition*, Rotterdam, 13 June 2017. 11. <https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2017/06/13/big-data-and-competition/big-data-and-competition.pdf>.

2 Randal C. PICKER: Competition and Privacy in Web 2.0 and the Cloud. *Northwestern University Law Review Colloquy*, 103:1, 4.

2. A web 2.0 versenyjogi szempontból jelentős jellemzői

Az internet a 'minden ingyenes' kultúráját ajánlja.³ Az interneten működő szolgáltatás-platformok pedig ezen modellt jellemzően a hirdetési piacról tartják fenn. A platformok (pl. bankkártya elszámolási rendszer, számítógépes operációs rendszerek, média piac) nem csak az interneten léteznek, de az internet az említett modell miatt megsokszorozza az erre építő szolgáltatásokat. Éppen ezért a platformokkal kapcsolatos versenyjogi problémák is intenzíven jelentkeznek az internet világában. A platformok lehetnek kettő vagy több (multi) oldalúak attól függően, hogy hányféle csoport közötti interakciót teremtenek meg. Egy adott platform hálózati hatásnak (amely egy externália, amelyről akkor beszélünk, ha az érintettek közötti tranzakció hatásai harmadik felet is érintenek akár pozitív akár negatív irányban) köszönhetően bekövetkező gyorsan növekvő népszerűsége piaci hatalmat keletkeztethet, hiszen minél többen használják, annál vonzóbb lesz mások számára is (hálózati hatás) és ennek eredményeként létrejöhet egyfajta 'hólabda hatás', amikor egy platform válik egyeduralkodóvá.

A hálózati hatás lehet közvetlen, amikor a hatás az adott platformot használók tekintetében jelentkezik (pl. ha sokan használják ugyanazt az operációs rendszert, akkor egyre növekvő számban tudnak egymást között adatot cserélni, amely tovább növeli a platform vonzerejét). A hálózati hatás lehet közvetett is, amikor a platform növekvő jelentősége (jelen esetben példának okáért egy operációs rendszer) más csoportok tagjait is bevonzza: adott esetben azokat a fejlesztőket, akik az adott operációs rendszerre írnak alkalmazásokat. A Google például ingyenesen biztosítja a keresőmotorja igénybevételét, a felhasználó lényegében a keresett kifejezés megadásával fizet, amelyre építve aztán a Google a potenciális hirdető felé célzott hirdetések feladását teszi lehetővé. A platformokat megkülönböztethetjük aszerint, hogy azok a keresletet és kínálatot kapcsolják össze (pl. Amazon), vagy ennek egy elterjedt és fontos specializációjaként az egyik oldalon a felhasználók idejét, figyelmét lekötve, a másik oldal számára reklámokat értékesítenek (pl. Google, Facebook).

A személyes adatokon nyugvó 'ingyenes' online szolgáltatások piaci értéke 2020-ra elérheti a 300 milliárd EUR-t.⁴ A big data több mint személyes adatok tömege, mert részét képezik aggregált és anonimizált adatok is, de több millió EU-s közösségi háló, internetes kereső, online kereskedelem használatától származnak.⁵ A személyes adatok azonban egyre fontosabb eszközzé,⁶ vagyoni értékűvé válnak, a digitális gazdaság új nyersanyaga⁷ csakhogy mint a szerzői jogok, üzleti titkok, szabadalmak, miként ezt gyakran a cégek könyvei is tükrözik.⁸

3 BKartA, B6-113/15, Working Paper – Market Power of Platforms and Networks, June 2016. 3.

4 Preliminary Opinion of the European Data Protection Supervisor: Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy. March 2014. 8. (a továbbiakban: Preliminary Opinion).

5 Uo., 9.

6 Ezt a Bizottság több döntésében is megerősítette: M.4731 – *Google/DoubleClick*, M.6314 – *Telefónica UK/Vodafone UK/Everything Everywhere/JV*, M.7023 *Publicis/Omnicom*. A GVH pedig a Vj-93/2011 ING-Telenor ügyben fejtette ki, hogy a fogyasztókra vonatkozó adatok megszerzése elősegíti az áruk eladását és értékesítését.

7 Opinion 8/2016 EDPS Opinon on coherent enforcement of fundamental rights in the age of big data, 23 September 2016. 6.

8 Preliminary Opinion i. m (4. lj.) 10.

Az 'ingyenes' online szolgáltatásnak van tehát 'igénybevételi díja', amely a személyes adat átadásával valósul meg.⁹ E folyamatnak jellemzően négy lépése van: gyűjtés, tárolás, elemzés, felhasználás.¹⁰ Olyan kétoldali piac ez, ahol a platform szolgáltatója egyre vonzóbb ingyenes szolgáltatásokat fejleszt annak érdekében, hogy az őket igénybevevő felhasználók egyre növekvő tábora miatt, az ingyenes szolgáltatásokat kínáló platform a reklámozóknak aztán minél vonzóbb legyen (a növekvő felhasználók figyelméért). Ebben a közegben az ingyenes felhasználók személyes adata komoly üzleti érték, hiszen az idejükkel és figyelmükkel fizetnek a reklámozóknak, melyre figyelemmel beszélhetünk figyelmi piacokról is.¹¹

Az elektronikus kereskedelemben is növekvő szerepe van az adatoknak és az adatok elemzésének. Ezekre építve célzott reklámok, a versenytársak árainak jobb nyomon követése vagy további vásárlásokat vonzó – a korábbi vásárlások tapasztalatain nyugvó – termék és szolgáltatás értékelések és személyre szabott szolgáltatások nyújthatók.¹²

3. Adat alapú piaci hatalom?

Az eddigi versenyjogi gyakorlatban a személyes adatokon alapuló internetes szolgáltatásokkal összefüggésben leginkább az a kérdés merült fel, hogy a személyes adatok halmaza piaci hatalmat hozhat-e létre?

A francia és a német versenyhatóság közös tanulmánya szerint elvileg van lehetőség arra, hogy ún. adatbrókerektől a versenytársak olyan adattömeget szerezzenek be, amelyekre versengő szolgáltatást tudnak építeni, valójában azonban van egy olyan szintje már az ingyenes szolgáltatásokkal kiépített adatbázisoknak, amelyekhez a gyakorlatban a versenytársaknak aligha lesz ésszerű hozzáférésük.¹³ Kérdés, hogy ez esetben mindez mennyiben köszönhető magának az adatnak vagy sokkal inkább az abból levonható következtetéseknek?¹⁴ Az USA-ban tiltottak meg összefonódást fogyasztói értékelésekhez platformot kínáló szolgáltatók között, mert az adatok kombinációja olyan piacra lépési korlátot hozott volna létre, amely a piac monopolizációjával járt volna.¹⁵

Az EU-ban a *Facebook/Whatsapp* összefonódás engedélyezésére irányuló ügyben¹⁶ a Bizottság arra az álláspontra helyezkedett, hogy bár a Whatsapp nem gyűjti a felhasználói adatait, nem valószínű, hogy az összefonódás után a Facebook a reklámpotenciál kihasználása érdekében elkezdene ezt tenni, mert a kiélezett piaci verseny miatt a felhasználók elpártolnának, így egy ilyen stratégia nem lenne kifizetődő. Amellett, hogy a Bizottság megvizsgálta

9 Autorité de la Concurrence – Bundeskartellamt: *Competition Law and Data*. 10th May, 2016. 3. (a továbbiakban: *Competition Law and Data*).

10 Organisation for Economic Cooperation and Development (OECD), 'Exploring the Economics of Personal Data'. 2013.

11 L. COLANGELO Giuseppe – MAGGIOLINO Mariateresa: Data Protection in Attention Markets: Protecting Privacy Through Competition? *Bocconi Legal Studies Research Paper*. (April 2, 2017). *Forthcoming, Journal of European Competition Law & Practice*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2945085.

12 Algorithms and Collusion - Note from the European Union DAF/COMP/WD (2017) 12 14 June 2017

13 *Competition Law and Data* i.m. (9. lj.) 12.

14 Ez esetben ugyanis az adatokból értéket előállító algoritmusnak lehet a piaci pozíció köszönhető. Uo. 42.

15 OECD: Big Data: Bringing competition policy to the digital era. DAF/COMP (2016) 14, 27.10.2016., 17. (a továbbiakban: OECD (2016)).

16 Case No COMP/M.7217 - *Facebook/ Whatsapp*.

a Whatsapp és Facebook profilok esetleges összekapcsolásából fakadó versenyhatásokat is, megállapította, hogy erre nincs lehetőség, bár utóbb kiderült, hogy a felek erre vonatkozó előadása valótlan volt, amely miatt a Bizottság később bírságot szabott ki.¹⁷ Ezen túl is a Bizottság szerint üzletszerzésre alkalmas személyes adathalmazok ezen körön kívül is elérhetők lennének a versenytársak számára. Ezen kívül a Bizottság hangsúlyozta, hogy az alkalmazás (*app*) fejlesztés gyorsan fejlődő ágazat, ahol a fogyasztók váltási költségei¹⁸ és a piacra lépés korlátai alacsonyak, ezért még a hálózati hatás miatt támadhatatlannak tűnő piaci hatalom is elveszíthető.¹⁹ Mindezt a dinamikus verseny mellett érvelők a Google és a Facebook példájával szemléltetik, akik indulásukkor a Yahoo!, az AltaVista, a MySpace uralta netes piacon kellett, hogy megvessék a lábukat és látszólag esélyük sem volt olyan hálózati hatás elérésére, mint az azóta eltűnt vagy jelentőségüket elvesztett egykori piacvezetőknek.²⁰ A *Google/DoubleClick* ügyben²¹ is arra az álláspontra helyezkedett a Bizottság, hogy a személyes adatok halmaza nem tekinthető nem megkettőzhető eszköznek, hiszen a versenytársak is képesek ilyen személyes adathalmazok beszerzésére például adatbrókerektől. Ráadásul a *Microsoft/Yahoo! Search* ügyben²² beszerzett piaci információk alapján a Bizottság arra az álláspontra jutott, hogy az összefonódás révén elérhető személyes adathalmaz bővülés előnyei, egy bizonyos szint után fokozatosan csökkenő hozadékuak. A legújabb ügyek közül a Bizottság a *Microsoft/LinkedIn*²³ összefonódás kapcsán állapította meg, hogy az adattömegek összekapcsolása az adatvédelmi szabályozás miatt korlátokba ütközhet. Arra az esetre pedig, ha ilyen összekapcsolás mégis megvalósulna, a Bizottság megállapította, hogy az online hirdetési piac számára, más forrásokból is elérhetők hatalmas felhasználói adattömegek, melyre figyelemmel a fúzióban nem kell káros horizontális hatásokkal számolni.²⁴

Az adatbázisok piacra lépés szempontjából való jelentőségére példa a távközlés területén az egyetemes szolgáltatási irányelv, amely előírja a tudakozószolgálatok és telefonkönyvek szolgáltatása céljából a megfelelő információk átadását.²⁵

Amennyiben megállapítható lenne egy személyes adatokat tartalmazó adatbázisról, hogy az erőfölényt alapoz meg, akkor természetesen felmerülhet, hogy az ahhoz való hozzáférés megtagadása erőfölénnyel való visszaélés lehet. Erre a megállapításra jutott a francia verseny-

17 Mergers: Commission fines Facebook €110 million for providing misleading information about WhatsApp takeover. IP/17/1369. www.europa.eu/rapid/press-release_IP-17-1369_en.htm (a továbbiakban: IP/17/1369).

18 Ezt még az ún. multi-homing is erősítheti, amely azt jelenti, hogy ugyanazon típusú online szolgáltatást a felhasználók sokszor több szolgáltatótól is igénybe veszik. Competition Law and Data (9. lj.) 36.

19 Uo., 132. pont.

20 Competition Law and Data i.m. (9. lj.) 29.

21 Pl. M.4731 – *Google/DoubleClick*, 365., az ügyben az internetes keresők és böngészők használatára vonatkozó személyes adatok összeadódása merült fel problémaként.

22 M.5727 *Microsoft/Yahoo! Search*.

23 M.8124 *Microsoft/LinkedIn*.

24 Eleonora OCELLO – Cristina SJÖDIN: *Microsoft/LinkedIn*. Big data and conglomerate effects in tech markets, *Competition Merger Brief* 1/2017. 2.

25 Az Európai Parlament és a Tanács 2002/22/EK irányelve (2002. március 7.) az egyetemes szolgáltatásról, valamint az elektronikus hírközlő hálózatokhoz és elektronikus hírközlési szolgáltatásokhoz kapcsolódó felhasználói jogokról *Official Journal L 108*, 24/04/2002 P. 0051 – 0077, 25. cikk (2) bek.: A tagállamok biztosítják, hogy minden, az előfizetőkhez telefonszámokat rendelő vállalkozás teljesítsen minden olyan ésszerű kérést, amely a nyilvánosan elérhető tudakozószolgálatok és telefonkönyvek szolgáltatása céljából a megfelelő információk egyeztetett formában, tisztességes, tárgyilagos, költségalapú és megkülönböztetéstől mentes rendelkezésre bocsátására irányul.

hatóság 2014-ben mikor megállapította, hogy a GDF Suez visszaélt a gazdasági erőfölényével, amikor a gázpiaci liberalizáció során, a még monopol időkből rendelkezésre álló ügyfél-információk (kb. 11 millió ügyfél adata) alapján igyekezett a fogyasztókat magához kötni (közvetlen megkereséssel élt feléjük, hogy piaci alapon szerződjenek át hozzá).²⁶ A hatóság elrendelte az ügyféladatok versenytársak számára való átadását, hogy a piacra lépésüket ezzel elősegítse. Ehhez a természetes személyek esetében be kellett szerezni a hozzájárulásukat, az adatkezelés kapcsán pedig kellett egy adatfeldolgozási szerződést kötni.

Amennyiben egy adatbázist üzleti titoknak minősítünk, akkor ilyen esetben a szellemi tulajdonhoz való hozzáférésre kidolgozott, kivételes körülmények teszt alapján kellene megítélni. Ezek a kivételes körülmények akkor állnak fenn a Bíróság²⁷ szerint, ha:

- i) a szellemi tulajdonjoggal rendelkező erőfölényes vállalkozás engedélye nélkülözhetetlen egy új termékgyártáshoz, melyet a domináns vállalkozás nem nyújt, és amely iránt potenciális fogyasztói kereslet mutatkozik,
- ii) a jogtulajdonosok a másodlagos piacot maguknak tartják fenn a teljes verseny kizárásával, és
- iii) az elzárkózás objektív indokok nélkül történik.

Amennyiben nem a szellemi tulajdon, hanem a fizikai eszközökhöz való hozzáférés tesztje alapján ítéljük meg az erőfölényes adatbázishoz való hozzáférést, akkor a *Bronner* ügyben²⁸ kidolgozott teszt alapján nem elegendő annak belátása, hogy az adatbázis mint eszköz nélkülözhetetlen, de szükséges az is, hogy az a versenytársak számára ne legyen ésszerűen megkettőzhető.²⁹

E versenyjogi kényszerengedélyeztetési folyamat azonban bonyolult és hosszadalmas.³⁰ Az új adatvédelmi rendelet³¹ 20. cikke szerinti adathordozhatóság azonban megelőzheti az ilyen jellegű problémákat, hiszen a jogosult áthordozhatja az adatát egy másik adatkezelőhöz. A *Microsoft/LinkedIn*³² ügyben a Bizottság kifejezetten is utal az új adatvédelmi rendeletre,³³ amely nagyobb lehetőséget ad a felhasználóknak a személyes adataik feletti kontroll gyakorlására.

A később megemlítendő *Asnef* ügy pedig arra szolgál iránymutatóul, hogy mikor nem tekinthető versenykorlátozónak egy olyan versenytársak által létrehozott és működtetett (konk-

26 Décision n 14-MC-02 du 9 septembre 2014 relative à une demande de mesures conservatoires présentée par la société Direct Energie dans les secteurs du gaz et de l'électricité, www.autoritedelaconurrence.fr/pdf/avis/14mc02.pdf

27 Egyesített ügyek C-241/91 és C-242/91, *Radio Telefís Éireann and Independent Television Publications Ltd. v. Commission*, [1995] ECR I-743.

28 C-7/97, *Oscar Bronner GmbH & Co. KG v. Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co. and others*, [1998] ECR I-7791.

29 OECD (2016) i.m. (15. lj.) 22.

30 L. Tóth András: *Az elektronikus hírközlés és média gazdasági szabályozásának alapjai és versenyjogi vonatkozásai*. Budapest, Infokommunikáció Könyvek, HVG-Orac, 2008. 107.

31 Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (EGT-vonatkozású szöveg) *OJ L* 119, 4.5.2016.

32 COMP/M.8124. *Microsoft/LinkedIn*, 178. pont.

33 Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (EGT-vonatkozású szöveg) *OJ L* 119, 4.5.2016.

rét esetben hitelinformációs) adatbázis, amely személyes adatokon alapul. A Bíróság szerint, amennyiben az adatbázis célja szerint olyan fontos érdekek szolgálatába állítható, mint adott esetben a banki rendszer prudens működése, akkor nem állapítható meg a versenytársak közötti együttműködés versenykorlátozó jellege, ha az adatbázisból a piaci szereplők nem tudják a másik piaci pozícióját ellenőrizni (tehát nem derül ki belőle, hogy ki a hitelezője az adósnak) továbbá az adatbázishoz bármely piaci szereplő diszkriminációmentesen csatlakozhat.³⁴

4. A versenyjog, mint az adatvédelem eszköze

Az adatvédelem megfelelő szintje a verseny nem árjellegű paramétere lehet.³⁵ Miként a termék minősége.³⁶ Egyre több olyan online alkalmazás-fejlesztés van ugyanis, amelyek kifejezetten a magas adatvédelmi szinttel kívánnak versenyelőnyre szert tenni (pl. *Snapchat*, *DuckDuckGo*). Éppen ezért lehetett a Snapchat egy, a fogyasztó megtevesztéssel kapcsolatos eljárás tárgya az USA-ban amikor kiderült, hogy az üzenetek tárolására vonatkozóan valótlan információkat adott.³⁷

Fentiekből következően, továbbá például egy összefonódás után az adatkezelés, adatvédelem szintjében bekövetkező kedvezőtlen változás (pl. több személyes adat kezelése, harmadik fél részére való továbbítása) a versenyjogi értékelés szempontjából felfogható az áremelkedéshez vagy a minőségromláshoz hasonló következményként.³⁸ A *Facebook/WhatsApp*³⁹ összefonódásban is a Bizottság az adatvédelem szintjét ilyen nem árjellegű versenyparáméternek tekintette, ugyanakkor úgy találta, hogy a kommunikációs alkalmazások esetében nem ez a legfontosabb versenytényező, ezért az adatvédelem szintjének esetleges romlása sem okozna versenyproblémát,⁴⁰ az összefonódással kapcsolatos adatvédelmi megfontolások pedig álláspontja szerint nem képezik a versenyjogi értékelés tárgyát, mert az az adatvédelmi jog körébe tartozó kérdés.⁴¹ Ezt egyébként már korábban megerősítette az Európai Bíróság az *Asnef* ügyben hozott döntésével, amely szerint „a személyes jellegű adatok érzékeny jellegével kapcsolatos esetleges kérdések önmagukban nem esnek a versenyjog hatálya alá, azokat a releváns adatvédelemre vonatkozó szabályok alapján kell eldönteni”⁴².

34 C-238/05 *Asnef-Equifax* [2006] EBHT I-11125, 61. pont.

35 Eleonora OCELLO – Cristina SJÖDIN – Anatoly SUBOČS: What's Up with Merger Control in the Digital Sector? Lessons from the Facebook/WhatsApp EU merger case, *Competition merger brief*, Issue 1/2015 – February, 6.; Opinion 8/2016 EDPS Opinion on coherent enforcement of fundamental rights in the age of big data, 23 September 2016. 13.

36 Competition Law and Data i.m. (9. lj.) 24.; Opinion 8/2016 EDPS Opinion on coherent enforcement of fundamental rights in the age of big data, 23 September 2016. 13.

37 Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False, <https://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were>.

38 Uo.

39 IP/17/1369 i.m. (17. lj.).

40 OCELLO – SJÖDIN i.m. (24. lj.) 5.

41 IP/17/1369 i.m. (17. lj.) 164. pont.

42 C-238/05 *Asnef-Equifax* [2006] EBHT I-11125, 63. pont.

Az eddigi ügyekben a Bizottság tehát nem kötötte össze az adatbázisok egy kézbe kerülését és az adatvédelem fennálló szintjének változását.⁴³ Az eddigi gyakorlat alapján (*Microsoft/LinkedIn*, *Facebook/WhatsApp* és *TeleAtlas/TomTom*⁴⁴) az a következtetés szűrhető le, hogy az adatkezelés minőségi szintjének változását a Bizottság a verseny szempontjain keresztül, közvetve értékeli. Amennyiben az adatbázis szintjén verseny azonosítható (erre jutott a Bizottság a *Google/DoubleClick*⁴⁵, *Microsoft/LinkedIn* ügyekben is), akkor a Bizottság úgy tekinti, hogy ez a körülmény visszatartja az érintettet az adatkezelés színvonalának mint versenyző paraméternek az esetleges rontásától, ha meg mégis bekövetkezik a minőségromlás, akkor a felhasználók úgy védekezhetnek ellene, hogy szolgáltatót váltanak. Mindez nem érinti a Bizottság szerint a személyes adatok védelmére vonatkozó szabályok megsértése esetén irányadó eljárásokat.⁴⁶ Mindez azért érdekes, mert az EUMSZ 7. és 16. cikke az EU intézményeire a különböző politikák összehangolásának a követelményét telepíti. Az Alapjogi Charta pedig előírja az EU intézményeinek az adatok védelméhez való jog tiszteletben tartását és alkalmazásuk elősegítését. Ebben az összefüggésben, ha a versenyjog az adatkezelés minőségének romlására rezonálna, akkor az felfogható lenne az adatvédelmi politika és jogok támogatásának is.⁴⁷ Igaz a *Facebook/WhatsApp* ügyben az amerikai FTC sem antitröszt alapon, hanem adatvédelmi szabályozóként hívta fel a figyelmét a Facebook-nak, mint vásárlónak a WhatsApp fennálló adatvédelmi rezsimjének megtartására.⁴⁸

A német versenyhatóság azonban, amikor eljárást indított a Facebook ellen erőfölénnyel való visszaélés gyanúja miatt, akkor arra hivatkozott, hogy a felhasználók adataira alapozott hirdetési tevékenységre építő piaci szereplőknek, kiemelt jelentőséget kell tulajdonítaniuk a személyes adatfelhasználás szabályairól való információadásra.⁴⁹ Meg kell jegyezni, hogy az európai versenyjogi gyakorlattól sem idegen, hogy erőfölénnyel való visszaélést állapítson meg olyan esetben, mikor a domináns szereplő valamely más szabályozással él vissza és ezzel versenyellenes hatást idéz elő.⁵⁰ Egyes szakirodalmi vélemények szerint azonban az adatvédelem szintjének védelme versenyviszonyok között sem lehet a versenyjog célja és feladata, mert annak az árra és az innovációra kell fókuszálni, az olyan nem árjellegű tényezők, mint az adatvédelem szintje pedig úgyis megtalálja az erre reflektáló jellegű szolgáltatások révén az utat az arra érzékeny felhasználók felé.⁵¹

43 COLANGELO – MAGGIOLINO i. m. (11. lj.) 6.

44 COMP/M.4854 TOM-TOM/TELEAtlas, ebben az ügyben a térképekhez való hozzáférés versenytársak számára való biztosítása volt kérdéses.

45 COMP/M.4731 *Google/DoubleClick*.

46 OCELLO – SJÖDIN – SUBOČS i. m. (35. lj.) 7.

47 Christopher KUNER – Fred H. CATE – Christopher MILLARD – Dan JERKER – B. SVANTESSON – Orla LYNKEY: When two worlds collide: the interface between competition law and data protection. *International Data Privacy Law*, 2014. Vol. 4, No. 4. 248.

48 Uo.

49 *Facebook*, Press Release, 2 March 2016.

www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/02_03_2016_Facebook.html?nn=3591568.

50 C-457/10 P *AstraZeneca kontra Commission*.

51 COLANGELO – MAGGIOLINO i. m. (11. lj.) 367.; l. még Marixenia DAVILLA: Is Big Data a Different Kind of Animal? The Treatment of Big Data Under the EU Competition Rules. *Journal of European Competition Law & Practice*, 2017. Vol. 8. No. 6.

5. Az online platformokkal kapcsolatos versenyjogi kérdések

Az online platformok az elmúlt két évtizedben drámai változásokat indítottak el a digitális gazdaságban, ma pedig a digitális társadalom számára hoznak számos előnyt.⁵² Az online platformok különféle formában és méretben léteznek; lefedik az online piacokat, a keresőket, a közösségi médiát és a kreatív tartalmakat kínáló elárusítóhelyeket, az alkalmazásokat forgalmazó platformokat, a távközlési szolgáltatásokat, a fizetési rendszereket és a közösségi gazdaság platformjait.⁵³ Az online platformok bővítik a fogyasztók számára a választékot, képesek új piacokat létrehozni, hagyományos piacok számára kihívást jelenteni nagy mennyiségű adat gyűjtése, feldolgozása révén, előnyükre kamatoztatják a hálózati hatásokat, amelynek révén – általános értelemben véve – a szolgáltatás értéke a felhasználók számával párhuzamosan növekszik.

5.1. Árjellegű korlátozások és visszaélések

Az online platformok még hatékonyabban köthetik össze a fogyasztókat és a kereskedőket, egyúttal lehetőséget adhatnak versenykorlátozásokra. Maguknak a platformoknak az árazási gyakorlata is versenyjogi problémákat vethet fel. Ez esetben alapvető kérdés, hogy maga a platform mekkora ellenőrzést gyakorol a platformon szolgáltatók fölött, másként a platform által gyakorolt ellenőrzés kizárja-e a platformon szolgáltatók függetlenségét, mint például az Uber esetében. Szpunar főtanácsnok szerint:

„(...)Az Uber platform keretében dolgozó sofőrök nem olyan saját tevékenységet fejtenek ki, amely a platformtól függetlenül létezik. Ellenkezőleg, e tevékenység kizárólag a platformnak köszönhetően létezhet, anélkül nem lenne semmi értelme.⁵⁴ Ezért álláspontom szerint tévedés az Ubert az olyan típusú közvetítő platformokhoz hasonlítani, amelyek hotelszoba lefoglalását vagy repülőjegyek megvásárlását teszik lehetővé.⁵⁵ [...] az Uber sofőrjeinek helyzetével ellentétben mind a szállodák, mind a légitársaságok olyan vállalkozások, amelyek működése teljesen független minden közvetítő platformtól, és amelyek számára az ilyen platformok csak egy eszközt jelentenek a többi között szolgáltatásaik forgalmazására. Emellett ők maguk, nem pedig a foglalási platformok határozzák meg szolgáltatásaik nyújtásának feltételeit, kezdve az árakkal.⁵⁶ A felhasználóknak egy ilyen foglalási platformon valódi választási lehetőségük van több szolgáltató között. Az Ubernél ezzel szemben e tényezőket a platform egységesített módon meghatározza.⁵⁷ Az Uber tehát nem egyszerű közvetítő az alkalmilag közlekedési szolgáltatás nyújtására kész sofőrök és az ilyen szolgáltatást kereső utasok között. Éppen ellenkezőleg: az Uber a városi közlekedési szolgáltatások valódi szervezője és üzemeltetője azokban a városokban, ahol jelen van.⁵⁸”

52 A Bizottság Közleménye az online platformok és a digitális egységes piacLehetőség és kihívás Európa számára {SWD(2016) 172 final} COM(2016) 288 final Brüsszel, 2016.5.25. 2.

53 Uo.

54 Szpunar főtanácsnok indítványa C-434/15. sz. ügy *Asociación Profesional Elite Taxi kontra Uber Systems Spain SL*, 56. pont. (a továbbiakban: Szpunar indítvány).

55 Uo., 57. pont.

56 Uo., 59. pont.

57 Uo., 60. pont.

58 Uo., 61. pont.

Szpunar főtanácsnok megjegyzi, hogy amennyiben az Uberről olyan platformnak tekintjük, amely független szolgáltatókat egyesít, az versenyjogi kérdéseket vethet fel.⁵⁹ Felmerülhet *hub-and-spoke* kartell vagy a független platformszolgáltatók közötti áregyeztetés *AC-Treuhand* alapú előmozdítása.⁶⁰

Versenyjogilag ugyanis kifogásolható, ha a platform üzemeltetője díjparitási megállapodásokat köt a platformon szolgáltatókkal, melynek értelmében ez utóbbiak vállalják, hogy nem ajánlanak máshol kedvezőbb árat, mint amelyet az érintett platformon kínálnak. Ilyenkor értelemszerűen nem a szolgáltatások árának a platform által történő meghatározásáról van szó, hanem a különböző üzleti partnerek díjszempontból való kezelésére vonatkozó kötelezettségvállalásról,⁶¹ de ettől még ez versenyjogilag kifogásolható.

Az online platformok (mint amilyen például az *Expedia* vagy a *Booking.com*)⁶² és a rajtuk keresztül szolgáltatást nyújtó eladók közti vertikális megállapodások gyakran tartalmazzák azt a korlátozást, hogy a szolgáltatás nyújtója által érvényesített ár nem lehet magasabb, mint más platformon, vagy megfordítva, más platformon nem lehet alacsonyabb az ár, mint az adott platformon kínált (*Most Favoured Nation Clause: MFN*). Egyfelől az MFN célja annak az ún. potyautas hatásnak a kivédése, amely abból fakad, hogy a platformot jelentős befektetéssel létrehozó szeretné kivédeni, ha fogyasztók pusztán összehasonlítás céljából vennék igénybe a platformját, de a terméket már egy olcsóbb fenntartású közvetítőn keresztül vagy közvetlenül az eladótól vásárolnák meg.⁶³ Az MFN eredményeként azonban egyfelől megszűnik a márkán belüli verseny, a versenytársak árai így könnyebben átláthatóbbakká válnak és ez bizonyos árközelítést is elindít. Másfelől megnehezíti a piacra lépést, hiszen egy új platform nem fog tudni betörni kedvezőbb árakkal a piacra, ennek hiányában nem tudja elérni azt a hálózati hatást, amivel már a piacon lévők rendelkeznek, nem tud annyi eladót a platformjára csábítani, így viszont nem tud a vevők számára vonzóvá válni. Mindez a platform ún. 'kétoldalú piac' jellegéből fakad.⁶⁴ Főleg a szállásközvetítések terén az utóbbi időben számos, ún. szűkített árparitációs kötelezettségvállalást tettek az érintettek a versenyjogi következmények elkerülése érdekében.⁶⁵ Ennek lényege, hogy az MFN csak az eladó saját honlapjára vonatkozik, más közvetítő platformokon lehetnek kedvezőbb versenyfeltételek.

Ezzel kiküszöbölhető, hogy a fogyasztó a platformon kiválasztott eladó termékét az eladó honlapján olcsóbban megszerezze, másrészt viszont elérhető, hogy a különböző platformok a jutalékaik terhére akciókba kezdjenek. Így kialakulhat egy árverseny, nőhet az árak átláthatósága és ezzel az áremelkedés irányába ható összefajtszás esélye. A Bizottság 2017. májusában fogadta el az Amazon kötelezettségvállalását abban az ügyben, amelyet erőfölénnyel való visszaélés miatt indított, mert az Amazon és az e-könyvek kiadói olyan árparitási megállapodást kötöttek, amely szerint az Amazon-t tájékoztatniuk kell a kiadónak a más e-könyv értékesítőkkal szemben alkalmazott kedvezőbb feltételekről és díjakról és biztosítani kell, hogy

59 Uo., 62. pont.

60 Jan KUPCIK: Why does Uber violate European competition laws? (2016) 37 *E.C.L.R.*, Issue 11.

61 Szpunar indítvány i.m. (54. lj.).

62 A szolgáltatás jellege miatt és nem a korlátozás miatt állnak itt példaként.

63 OECD: *Vertical Restraints for On-line Sales*, DAF/COMP(2013)13, 23. (a továbbiakban: OECD (2013)), www.oecd.org/competition/VerticalRestraintsForOnlineSales2013.pdf.

64 Uo.

65 Booking.com to Amend Parity Provisions Throughout Europe, <https://news.booking.com/bookingcom-to-amend-parity-provisions-throughout-europe>

legalább olyan kedvezőbb feltételekkel és díjakkal szerződjön az Amazon az e-könyv kiadókkal, mint amilyenek az Amazon versenytársai számára biztosítottak.⁶⁶ A Bizottság szerint ezzel az Amazon versenytársai nehezebb helyzetbe kerültek, miután nem tudtak innovatív megoldásokkal szerződni az e-könyv kiadókkal, miáltal az Amazon domináns helyzete tovább erősödött az angol és német nyelvű e-könyvek értékesítésének piacán.

5.2. Nem árjellegű korlátozások és visszaélések

A domináns platformok többféleképpen is kihasználhatják ezt a helyzetüket. Különösen is akkor, amikor vertikálisan integráltak, tehát maguk is nyújtanak szolgáltatásokat a platformjuk felhasználásával. Ilyen esetben versenyjogilag problémás lehet, ha saját szolgáltatásukat indokolatlanul előnyben részesítik a többi platformon szolgáltatóhoz képest. Emiatt az Európai Bizottság 2017 júniusában 2,4 milliárd EUR bírságot szabott ki a Google-ra.⁶⁷ Megállapította, hogy a Google az internetes keresés európai piacán 90%-ot meghaladó piaci részesedéssel bír. A Google azzal élt vissza erőfölényes helyzetével, hogy saját termék-összehasonlító szolgáltatásának, a Google Shopping-nak a keresési eredményeit a versenytársainál előbbre sorolta, jobban megjelenítette, kiemelte. Miután adatok szerint a Google keresési találatai első oldalán található 10 eredmény kapja az összes felkeresés 95%-át, így a versenytársak súlyos hátrányba kerültek, hiszen csökkent a hozzájuk irányuló forgalom. Olaszországban a Google azzal a feltétellel listázta csak a híroldalakat a keresőjében, ha hozzájárultak a hír aggregátorában való közzétételre. Az olasz versenyhatóság azonban ezt erőfölénnyel való visszaelésnek ítélte és előírta a Google számára, hogy szüntesse meg ezt az árukapcsolást.⁶⁸

A platformok felhasználóiról, illetve a szolgáltatás nyújtóiról adott visszajelzések fontos szabályozó szerepet töltenek be, másfelől csökkentik a szolgáltatások nyújtásával és igénybevételeével kapcsolatos bizalmatlanságot. A web 2.0-ás interakciók során ugyanis sokszor ismeretlen felhasználók és szolgáltatás nyújtók kerülnek egymással kapcsolatba, amely esetben megkönnyíti a tranzakció létrejöttét, ha tudható, hogy a múltban adott felhasználó hogyan hagyta maga után a kivett szobát (pl. Airbnb) vagy a szolgáltatás/termék kínálója valóban leszállította az árut az által hirdetett minőségben (pl. eBay). Ezzel együtt az értékelések hiánya komoly piaca lépési korlátot is képezhet azoknak, akik újonnan kívánnak megjelenni egy platformon. Különösen is aggályos lehet, ha egy domináns platform megtiltja a felhasználóinak, hogy a platformon megszerzett értékelésüket másik versenytárs platformon felhasználják. A platformok közötti átjárhatóság biztosítása fokozza a versenyt, jól mutatja ezt a Microsoft ügy.⁶⁹

A felhasználók figyelméért óriási harc folyik, hiszen aki megszerzi a felhasználó figyelmét az szerzi meg a bevételt hozó hirdetést is. A nagy figyelem aggregálók, mint például a Facebook abban érdekeltek, hogy a felhasználók minél kevesebbszer látogassanak el közösségi oldalról és lehetőleg minél több tartalmat helyben kapjanak meg. Ha hírekről van szó,

66 CASE AT.40153 E-book MFNs and related matters (Amazon).

67 Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service – Factsheet, europa.eu/rapid/press-release_MEMO-17-1785_en.htm.

68 Tim KASTEN – Sean GERLICH, The Italian Competition Authority closes investigation into an online news aggregator service following commitments (Google), 17 January 2010, *e-Competitions Bulletin* January 2010, Art. N 41251.

69 T-201/04, *Microsoft v Commission* ECR [2005] II-1491.

akkor például azokat, de ezzel csökken a hírek szállítóinak forgalma, miközben a tartalmat valójában ők állítják elő. Egyesek ezzel összefüggésben beszélnek hírlopásról,⁷⁰ mint tisztességtelen verseny cselekményről,⁷¹ hiszen más teljesítményén potyázik a vállalkozás, mint az *International News Service v. Associated Press* ügyben,⁷² amikor a hírügynökség a versenytárs tudósítóinak lefizetése árán jutott harctéri hírekhez az I. vh idején.

Különösen akkor fájdalmas ez, amikor nem valódi, hanem álhírek tartják a közösségi oldalon a felhasználót, ezzel tovább csökkentve az esélyét annak, hogy a felhasználó valaha valódi hírszolgáltató oldalának szentel figyelmet. Egyes adatok szerint például a 2016-os amerikai elnökválasztás hamis híreinek olvasottsága a Facebook-on már meghaladta a valódi hírekét.⁷³ Egyes álláspontok szerint a domináns közösségi oldalnak tennie kellene versenyjogi alapon is az álhírek terjedésével szemben, mert ez tisztességtelenül tartja meg a felhasználók figyelmét az adott platformon.⁷⁴

Az exkluzív értékesítés fontos eszköz ahhoz, hogy a gyártó – megvédve a disztribútorát a márkán belüli versenytől – biztosítsa a disztribútora számára, hogy az erőforrásait a márkák közötti versenyre koncentrálhassa. Ezzel összefüggésben az EU versenyjog elfogadja az aktív értékesítés (más kizárólagos disztribútor területének aktív marketinggel való támadása) korlátozását, viszont a passzív értékesítés (amikor a fogyasztó nem az értékesítő erőfeszítése eredményeként keresi fel a nem területe szerinti kizárólagos disztribútort) korlátozását különösen is súlyosnak minősíti. Ezzel kapcsolatosan kérdés, hogy minek minősül az online reklámozás?

Az EU versenyjog az internetet passzív értékesítési formának minősíti:

„Általánosságban, ha egy forgalmazó weboldalt használ termékek eladása céljából, az passzív értékesítési formának minősül, mivel ez ésszerű módja annak, hogy a forgalmazó elérhetővé váljon az ügyfelek számára. A weboldal használatának a saját területén vagy ügyfélcsoportján kívül is lehetnek hatásai, ez azonban a technológiából – azaz a bárholonnan megvalósítható könnyű elérhetőségből – ered. Passzív értékesítésnek minősül, ha az ügyfél felkeresi a forgalmazó honlapját, kapcsolatba lép a forgalmazóval, és ez a kapcsolat értékesítéshez – és szállításhoz – vezet.”⁷⁵

A versenyjogi gyakorlat az internet következő, különösen súlyos korlátozásait ismeri:⁷⁶

- 1) megállapodás valamely (kizárólagos) forgalmazóval arról, hogy másik (kizárólagos) területen belüli ügyfeleket megakadályoz weboldalának megtekintésében, vagy annak előírása, hogy a forgalmazó weboldalán helyezzen el a gyártó vagy más (kizárólagos) forgalmazók oldalaira mutató automatikus ügyfél-átirányítást;

70 Murdoch accuses Google of news 'theft', www.articles.latimes.com/2009/dec/02/business/la-fi-news-google2-2009dec02.

71 Kimberley ISBELL: What's the law around aggregating news online? A Harvard Law report on the risks and the best practices, www.niemanlab.org/2010/09/whats-the-law-around-aggregating-news-online-a-harvard-law-report-on-the-risks-and-the-best-practices/.

72 248 U.S. 215 (1918).

73 Craig SILVERMAN: This Analysis Shows How Viral Fake Election News Stories Outperformed Real News On Facebook, www.buzzfeed.com/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook?utm_term=.spPLNAo7y#.bkOgQZj8v.

74 Sally Hubbard, Why Fake News Is An Antitrust Problem, www.forbes.com/sites/washingtonbytes/2017/01/10/why-fake-news-is-an-antitrust-problem/2/#32b602113f0d.

75 Európai Bizottság Közleménye: A vertikális korlátozásokról szóló iránymutatás, 2010/C 130/01, 52. pont.

76 Uo.

- 2) megállapodás abban, hogy a (kizárólagos) forgalmazó szakítsa meg a vevők interneten keresztüli ügyleteit, amennyiben hitelkártya-adataik nem a forgalmazó (kizárólagos) területén belüli címet azonosítanak;
- 3) megállapodás abban, hogy a forgalmazó korlátozza az interneten keresztüli értékesítés teljes értékesítésen belüli arányát;
- 4) megállapodás abban, hogy a forgalmazó fizessen magasabb árat az interneten keresztül értékesíteni kívánt termékekért, mint azokért a termékekért, amelyeket hagyományos módon kíván értékesíteni.

A Bizottság a kettős árazásra nézve az elektronikus kereskedelmi ágazati vizsgálat jelenésében kijelenti, hogy a különböző kiskereskedők részére történő eltérő (nagykereskedelmi) árak felszámítása, általában a versenyfolyamat szokásos részének számít. Az egy és ugyanazon (hibrid) kiskereskedőre vonatkozó kettős árképzés a vertikális csoportmentességi rendelet értelmében, általában különösen súlyos korlátozásnak minősül.⁷⁷

A kettős árazásra példa a magyar kontaktlencse ügy.⁷⁸ A Vj-55/2013. sz. ügyben az eljárás alá vont csak akkor biztosította az online forgalmazóknak a jelentős árkedvezményeket, ha 30 optikai üzlettel kötöttek szerződést.⁷⁹ Ez lényegében teljesíthetetlen feltétel volt, mert az optikai üzletek nem voltak érdekeltek a tőlük független internetes kereskedők térnyerését elősegíteni.⁸⁰ A GVH a korlátozást ún. különösen súlyosnak minősítette, minthogy korlátozta, hogy a disztribútor passzívan milyen vevőkör számára értékesíthet. A GVH szerint az internetes kereskedőkkel kötendő szerződésekben kikötött kedvezményrendszer úgy volt tekinthető, mint egy megállapodás abban, hogy az internetes kereskedő fizessen magasabb árat az interneten keresztül értékesíteni kívánt termékekért, mint azok a kereskedők, akik értékesítésének zöme optikai üzleteiken keresztül történik.⁸¹ A GVH szerint önmagában az internetes kereskedők hátrányos megkülönböztetése nem volt indokolható az internetes vásárlás egészségügyi kockázataival, amelyhez képest az előírt optikai üzletszám messze eltúlzottnak minősül. A GVH szerint az internetes vásárlók széles körben vásárolnak úgy kontaktlencsét, hogy az illesztési szolgáltatásokat máshol már igénybe vették, ezért ugyanannak a már általuk ismert terméknek az újbóli megvásárlása nem jelent számukra egészségügyi kockázatot.⁸²

A GVH szerint potyautasság által okozott hátrányok enyhítésére és a fizikai üzletek támogatására – hogy azok továbbra is minőségi szolgáltatást tudjanak nyújtani – nem ellentétes a versenytörvénnyel, ha a gyártó egy fix összeget juttat havonta a hagyományos értékesítés

77 Végső jelentés az e-kereskedelmi ágazati vizsgálatról Brüsszel, 2017.5.10. COM(2017) 229 final {SWD(2017) 154 final} 37. pont

78 Vj-55/2013 sz. ügy.

79 Uo., 167.

80 Uo., 186.

81 Uo., 186.

82 Uo., 191. A Versenytanács a Vj/74/2003. sz. ügyben hozott döntésében arra hívta fel a figyelmet, hogy egyértelmű jogszabályi felhatalmazás hiányában egy szakma, egyes vállalkozások, illetve a vállalkozások társadalmi szervezetei nem vehetik át a jogszabály, az állami szabályozás funkcióit, azaz ha az általuk szükségesnek tartott jogi szabályozás nem jön létre, állami aktus nem történik meg, vállalkozások közötti megállapodással azt önkényesen nem helyettesíthetik, még abban az esetben sem, ha a vállalkozások, illetve társadalmi szervezeteik megítélése szerint piaci zavarok mutatkoznak. Ha az adott ágazatért felelős állami szervek nem teszik meg a szükséges lépéseket a piaci zavarok elhárítására, az erre feljogosított jogalkotó nem hozza meg a szükséges rendeletet, az nem hatalmazza fel a vállalkozásokat, illetve társadalmi szervezeteiket, hogy a jogalkotó helyett maguk cselekedjenek.

előmozdítása végett a kereskedőnek.⁸³ Ez az előre megállapodott juttatás azonban nem lehet változó mértékű, különösen nem emelkedhet a realizált hagyományos forgalomtól függően, mivel ez már kettős árképzést jelentene a gyakorlatban.⁸⁴

Szelektív disztribúciós rendszerben (amikor a gyártó minőségi követelményekhez köti a disztribútorrá válást) sem lehet korlátozni az internetes értékesítést.⁸⁵ Ezzel kapcsolatos ügyben⁸⁶ a *Pierre Fabre Dermo-Cosmétique* kozmetikai és testápoló termékei forgalmazási szerződéseiben kikötötte, hogy az értékesítésekre kizárólag helyiségben, okleveles gyógyszerész kötelező jelenléte mellett kerülhet sor, miközben az érintett termékek nem tartoztak a gyógyszerek kategóriájába, így tehát nem vonatkozott rájuk gyógyszerészi monopólium. A közigazgatási eljárás során a *Pierre Fabre Dermo-Cosmétique* kifejtette, hogy a szóban forgó termékek jellegüknél fogva az értékesítési helyen a teljes nyitvatartási idő alatt, gyógyszerész oklevéllel rendelkező személy fizikai jelenlétét teszik szükségessé annak érdekében, hogy a vásárló minden körülmények között személyre szabott szakértői tanácsot kérhessen és kaphasson. A Bíróság esetjogi gyakorlatában a szelektív disztribúciós rendszerek nem sértik az EUMSZ 101. cikk (1) bekezdésében meghatározott tilalmat, amennyiben a viszonteladókat egységesen meghatározott és hátrányos megkülönböztetéstől mentesen alkalmazott objektív minőségi kritériumok alapján választják ki, továbbá amennyiben a termék jellemzői a termék minőségének megóvása és megfelelő használatának biztosítása érdekében szükségessé teszik az ilyen forgalmazási hálózatot, végül pedig amennyiben a kialakított kritériumok nem haladják meg a szükséges mértéket. Az ügyben nem volt vitatott, hogy a *Pierre Fabre Dermo-Cosmétique* szelektív forgalmazási hálózata keretében a viszonteladókat egységesen meghatározott objektív minőségi kritériumok alapján választják ki.⁸⁷ Ugyanakkor a Bíróság szerint meg kell vizsgálni azt is, hogy a versenykorlátozások arányosan próbálják-e megvalósítani az egyébként jogszerű célkitűzéseket. A Bíróság szerint a *presztíztst sugalló arculat megóvására irányuló célkitűzés nem minősülhet a versenykorlátozás alapjául* szolgáló jogszerű célkitűzésnek, és így nem igazolhatja, hogy az ilyen célkitűzésre irányuló szerződéses kikötésre ne vonatkozzék az EUMSZ 101. cikk (1) bekezdése.⁸⁸ „Az alapügy tárgyát képezőhöz hasonló olyan szerződéses kikötésnek, amely az internet mint forgalmazási mód alkalmazását de facto megtiltja, legalább az a célja, hogy korlátozza az olyan végső felhasználók részére történő passzív eladásokat, akik az interneten szeretnének vásárolni, és akik a szelektív forgalmazási rendszer érintett tagjának földrajzi vonzáskörzetén kívül tartózkodnak.”⁸⁹

A harmadik felek honlapján elhelyezett célzott reklám (*banner*), amely meghatározott területeken elérhető fogyasztóknak szól, mindenképpen az aktív értékesítés körébe esik.⁹⁰ Gyakran előfordul, hogy a gyártó nem engedi meg a disztribútornak, hogy a márkát ár-összehasonlító honlapokon, piactereken szerepeltesse, illetve internetes keresők számára elérhe-

83 Uo., 214.

84 Európai Bizottság A vertikális korlátozásokról szóló iránymutatás (EGT-vonatkozású szöveg) (2010/C 130/01. (52) bekezdésének d) pontja. HL C 130/1. 2010.5.19. (a továbbiakban: Iránymutatás).

85 Uo., 54. pont.

86 C-439/09 - *Pierre Fabre Dermo-Cosmétique* EBHT [2011] I-09419.

87 Uo., 43. pont.

88 Uo., 46. pont.

89 Uo., 54. pont.

90 OECD (2013) i.m. (63.lj.) 25.

tővé tegye, amely felvetheti a passzív értékesítés korlátozását.⁹¹ A Vertikális Korlátozásokról szóló Bizottsági Iránymutatás⁹² megengedi, hogy a szállítók korlátozzák a viszonteladóknak, hogy harmadik fél online platformján árusítsanak „amennyiben a forgalmazó weboldalának harmadik fél platformja ad helyet, a szállító megkövetelheti, hogy az ügyfelek ne a harmadik fél platformjának nevét vagy logóját viselő weboldalon keresztül látogassák a forgalmazó weboldalát.”⁹³ Ennek ellenére a német versenyhatóság az Asics esetében megállapította, hogy a forgalmazók eltávolítása szelektív disztribúciós rendszerben harmadik fél online platformjának értékesítésre felhasználásától, célzatos versenykorlátozás és a *Pierre Fabre* ügyre hivatkozással (miközben az a forgalmazók saját internetes felületre vonatkozó korlátozásával volt kapcsolatos) aláhúzta, hogy ezt a márka presztízsének megőrzésére hivatkozás sem mentheti.⁹⁴ A hatóság szerint az ilyen korlátozás főleg a KKV viszonteladók értékesítési lehetőségeit szűkíti. A kérdés tisztázását szolgálhatja a Frankfurti Fellebviteli Bíróság által a *Coty* ügyben⁹⁵ kezdeményezett előzetes döntéshozatali eljárás, amely többek között a *Pierre Fabre* döntés relevanciáját vizsgálja, a szelektív disztribúciós rendszerben harmadik feles online platformon keresztüli eladás korlátozása kapcsán. Az ügy a nemzeti bíróság előtt azért indult, mert a *Coty* termékek egy forgalmazója Németországban az *Amazon.de*-n értékesített, amit a *Coty* ellentétesnek ítélt a forgalmazási szerződéssel és kérte a bíróságot, hogy tiltsa el ettől a forgalmazót. A szelektív forgalmazási rendszer szervezésére nem vonatkozik az EUMSZ 101. cikk (1) bekezdésében meghatározott tilalom, amennyiben a viszonteladókat valamennyi lehetséges viszonteladó vonatkozásában egységesen meghatározott és hátrányos megkülönböztetéstől mentesen alkalmazott, objektív minőségi kritériumok alapján választják ki, továbbá amennyiben a szóban forgó termék jellemzői a termék minőségének megóvása és megfelelő használatának biztosítása érdekében szükségessé teszik az ilyen forgalmazási hálózatot, végül pedig amennyiben a kialakított kritériumok nem haladják meg a szükséges mértéket (ún. Metro-kritériumok)⁹⁶. A Főtanácsnok álláspontja szerint a luxus- és magas presztízsű áruk forgalmazására irányuló, és elsődlegesen az említett áruk márkaimázsának biztosítását szolgáló szelektív forgalmazási hálózatok nem tartoznak az EUMSZ 101. cikk (1) bekezdésében rögzített tilalom hatálya alá.⁹⁷ A Főtanácsnok azt is világossá teszi, hogy a *Pierre Fabre* ügyben azt a szerződéses kikötést kifogásolták, amely a szerződés szerinti termékek végső felhasználók számára való internetes értékesítésének a szelektív forgalmazási hálózat keretében a szerződéses forgalmazókkal szemben előírt általános és abszolút tilalmát tartalmazta.⁹⁸ Ez ugyanakkor nem jelenti azt, hogy a Bíróság eleve az EUMSZ 101. cikk (1) bekezdésében hivatkozott kartell-tilalom hatálya alá kívánta vonni az éppen az érintett áruk márkaimázsának megóvását célzó forgalmazási rendszereket.⁹⁹

91 Uo.

92 Iránymutatás i. m. (84. lj.).

93 Uo., 54. pont.

94 Decision of August 26, 2015, case B2 – 98/11.

95 Case C-230/16: Request for a preliminary ruling from the Oberlandesgericht Frankfurt am Main (Germany) lodged on 25 April 2016 — Coty Germany GmbH v Parfümerie Akzente GmbH. (a továbbiakban: Nils WAHL főtanácsnok indítványa), curia.europa.eu/juris/document/document.jsf?text=&docid=193231&doclang=EN.

96 26/76 *Metro SB-Großmärkte kontra Bizottság*.

97 Nils WAHL főtanácsnok indítványa i.m. (95. lj.) 74. pont.

98 Uo., 79. pont.

99 Uo., 80. pont.

A *Pierre Fabre* ítéletből azt a következtetést kell levonni, hogy a különösen súlyos korlátozások (mint az internetes értékesítésnek a *Pierre Fabre Dermo-Cosmétique* ítéletben vitatott kikötésből következő teljes tilalma) miatt, a szóban forgó áruk magas presztízsű imázsának megóvására irányuló cél nem jogszerű, ami azzal a következménnyel jár, hogy nem igazolt az ilyen célt követő szelektív forgalmazási rendszer vagy kikötés mentesítése.¹⁰⁰

Miután a főtanácsnok szerint a luxus- és magas presztízsű áruk imázsának megóvására irányuló cél mindig jogszerű az alapeljárásban szereplőhöz hasonló, minőségi jellegű szelektív forgalmazási rendszer igazolása szempontjából,¹⁰¹ ezért azt kell vizsgálni, hogy a vitatott kikötést, vagyis azt, amelyik megtiltja a szerződéses forgalmazók számára, hogy kifelé látható módon harmadik fél platformokat vegyenek igénybe, igazolhatja-e konkrétan a szóban forgó termékek luxusimázsának megóvásának szükségessége. A Főtanácsnok szerint a szelektív forgalmazási hálózat feje az általa forgalmazott áruk márkaimázsának vagy magas presztízsű imázsának megóvása érdekében megtilthatja forgalmazói (akár szerződéses forgalmazói) számára, hogy kifelé látható módon harmadik fél vállalkozásokat vegyenek igénybe. E tilalom alkalmas lehet a minőségi, biztonsági, valamint az áruk eredetének azonosítását szolgáló garanciák megőrzésére,¹⁰² mert ha az áruk forgalmazása során harmadik fél platformot vesznek igénybe, akkor a szerződéses forgalmazók – ezenfelül a hálózat feje – már nem tartják ellenőrzésük alatt különösen ezen áruk bemutatását és imázsát.¹⁰³ A Főtanácsnok emlékeztet, hogy a *Pierre Fabre* döntéssel szemben, jelen ügyben a Coty nem tiltotta meg általános jelleggel az online értékesítést.¹⁰⁴ A Főtanácsnok szerint, ha Metro-kritériumok nem teljesülése miatt a megállapodás esetleg az EUMSz 101. cikk hatálya alá is esne, akkor sem volna céljánál fogva versenykorlátozónak tekinthető.¹⁰⁵ A főtanácsnok szerint az ilyen teljes internetes forgalmazásra általános jelleggel ki nem terjedő tilalom nem lehet célzatos versenykorlátozás.¹⁰⁶ A Főtanácsnok szerint továbbá a harmadik feles piactereken való értékesítés korlátozása nem jelent vevőkör felosztást sem, mert ezzel összefüggésben nem lehet eleve azonosítani a vevők olyan csoportját vagy egy olyan adott piacot, amelynek megfelelnének a harmadik fél platformok felhasználói.¹⁰⁷ A Főtanácsnok azt is kifejti, hogy az értékesítés ezen módjának kizárása nem minősül passzív eladás korlátozásnak sem, mert nem tiltja az online értékesítés minden formáját.¹⁰⁸

100 Uo., 84. pont.

101 Uo., 99. pont.

102 Uo., 102. pont.

103 Uo., 104. pont.

104 Uo., 109. pont.

105 Uo., 117. pont.

106 Uo., 118. pont.

107 Uo., 143. pont.

108 Uo., 155. pont.

Hálózati és információs rendszerek biztonsága európai szabályozásának alapjai*

TÓTH ANDRÁS

1. Bevezetés

A felhasználók számának drasztikus növekedése, a gazdasági, politikai, személyes élettér internetre való egyre nagyobb arányú áthelyeződése, a laikus felhasználók védtelensége és az információk tömeges megszerzése csakúgy, mint az azokkal való visszaélés jelentette csábítás, mára jelentősen felértékelte a hálózatbiztonság kérdését.¹ Természetesen a hálózatok és informatikai rendszerek biztonságát nem csak a rosszindulatú támadások, de a végtelen műveletek (pl. adatvesztés, műszaki hiba, természeti katasztrófák) is veszélyeztethetik. Miután az informatikai rendszerek, az ezeket kiszolgáló hálózatok, a rajtuk áramló információk mára az emberiség mindennapi életének markáns részeivé váltak, így mind a rosszindulatú, mind pedig a végtelen behatások súlyos következményekkel járhatnak (l. csak a legutóbbi *WannaCry* zsarolóvírus hatását). A fenyegetések jellege folyamatosan változik, a biztonságot érintő váratlan események pedig alááshatják a felhasználóknak a technológiába, a hálózatokba és a szolgáltatásokba vetett bizalmát, és ezáltal befolyásolhatják a fogyasztók azon lehetőségét, hogy teljes mértékben kiaknázzák az EU belső piacában továbbá az információs és kommunikációs technológiák széles körű alkalmazásában rejlő lehetőségeket.²

A tanulmány a fogalmi keretek tisztázását követően (2. pont) bemutatja a hálózati és információs rendszerek európai szabályozásának rendszerét és főbb jellemzőit (3. pont), majd az EU szabályozás fejlődését, az ellenálló képességre vonatkozó EU szabályozást különösen is a vonatkozó irányelv alapján, kitérve az elektronikus hírközlő hálózatokra és kritikus infrastruktúrára vonatkozó európai többlet követelményekre, valamint az adatvédelmi rendelkezésekre (4. pont).

2. Fogalmi keretek

A kibertér a minket körülvevő elektronikus világ, amely a globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttese.³ A kibertér (mint kiemelt gazdasági és társadalmi folyamat) fejlődésének és működésének a

* A szerző köszönetet mond Bartha Bencének a KRE-ÁJK hallgatójának a tanulmány elkészítéséhez nyújtott közreműködéséért.

1 KERECSENDI András: *Hálózatbiztonság*. Eger. Médiainformatikai Kiadványok, 2013. 15. http://www.incedy.hu/~hupi/tananyag/halozati_biztonsag.pdf.

2 526/2013/EU rendelet az Európai Unió Hálózat- és Információbiztonsági Ügynökségről (ENISA) HL L 165/41. 2. preambulumbekzdés.

3 A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti. I. Magyarország Nemzeti Kiberbiztonsági Stratégiája 1139/2013. (III.21.) Korm. határozat 3. pont.

kulcsa a bizalom fenntartása, amely nem képzelhető el a kiberteret alkotó elektronikus információs rendszerek, valamint ezen rendszereken keresztül tárolt, kezelt, továbbított adatok és információk biztonsága nélkül. Miután tökéletes biztonság nem létezik, ezért a kiberbiztonság a kibertérben létező *kockázatok kezelésére* alkalmazható *széles* politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező *kockázatok elfogadható szintjét* biztosítva, a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működtetése érdekében.⁴

A kiberbiztonság fenntartásának egyik eszköze az elektronikus hálózati és információs rendszerek biztonsága, amely tág értelemben az adatok, információk kezelésére használt eszközök (hardver, hálózat), eljárások (szoftver, folyamatok), személyek együttesét lefedi,⁵ szűkebb értelemben csak az elektronikus hírközlő hálózatokat,⁶ az adatok kezelését végző eszközöket és az ezeken továbbított adatokat jelenti.⁷ Mind a szűkebb, mind pedig a tágabb meghatározás lefedi azonban az adatok és információs rendszerek biztonságát. Előbbi az adatok bizalmasságát, sértetlenségét (hitelességét) és rendelkezésre állását, utóbbi az információs rendszer elemeinek sértetlenségét (rendeltetésszerű használat biztosított) és rendelkezésre állását jelenti.⁸ A hálózati és információs rendszerek biztonsága tehát az adatok és az információs rendszerelemek olyan *állapota*, amelyben azok *védelme* az összes számításba vehető fenyegetésre nézve teljes körűen, folyamatosan a kockázatokkal arányosan (tehát a védelem költségei arányosak a fenyegetéssel okozható károkkal) megvalósul.⁹ A hálózati és információs rendszerek biztonsága az arra való *képességet* jelenti, hogy *ellenálljon* mindazon fenyegetéseknek, amelyek veszélyeztetik annak rendelkezésre állását, hitelességét, sértetlenségét, bizalmasságát,¹⁰ amelyek a legfőbb érték – a kibertér fejlődéséhez szükséges társadalmi bizalom – kialakításának zálogai.¹¹

A hálózat és információ biztonság, tehát a szűken vett kiberbiztonság, amely nem foglalja magába a kiberbűncselekmények tilalmát, de kiterjed az elektronikus hírközlő hálózatokra vonatkozó adatvédelmi (tárolt, továbbított, kezelt adatok biztonsága)¹² és hálózatok ellenállását növelő szabályokra.

A hálózati és információs rendszerek (HIR) biztonsága lényeges, hiszen ezek létfontosságú szerepet játszanak korunk társadalmi és gazdasági rendjében, a szándékos, illetve egyébként ártalmas cselekmények pedig alááshatják a bizalmat és súlyos károkat okozhatnak a gazda-

4 L. Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 1. § 26. pont. (a továbbiakban: 2013. évi L. törvény).

5 Uo., 1. § 14b. pont.

6 Ahogyan azt a 2002/21/EK irányelv 2. cikk a) pontja meghatározza: olyan átviteli rendszer, esetleg kapcsoló vagy útválasztó eszköz, valamint egyéb erőforrás, – ideértve a nem aktív hálózati elemeket is – amely lehetővé teszi a vezetéken, rádióhullámon, optikai vagy egyéb elektromágneses úton történő jelátvitelt, beleértve a műholdas hálózatokat, a helyhez kötött (vonal- és csomagkapcsolt, beleértve az internetet) és mobil földi hálózatokat, az elektromos vezetékrendszereket, annyiban, amennyiben azokat jelek továbbítására használják, a rádióműsor- és televízióműsor-terjesztő hálózatokat, valamint a kábeltelevízió-hálózatokat, a továbbított információtípusra tekintet nélkül.

7 L. Európai Parlament és a Tanács 2016/1148 Irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről, (a továbbiakban: Irányelv) 4. cikk (1) bekezdés.

8 2013. évi L. törvény (4. lj.) 1. § 15. pont.

9 Uo.

10 Uo., 4. cikk (2) bekezdés.

11 Uo., 2. preambulumbekkezdés.

12 Ahogyan azt az 2002/58/EK „elektronikus hírközlési adatvédelmi irányelv” meghatározza.

ságnak is.¹³ A HIR szabályozás célja a kibertér fejlődéséhez szükséges társadalmi *bizalom*¹⁴ elfogadható kockázati szinten tartása.

3. A HIR szabályozásának rendszere és jellemzői

Az élet egyre több dimenziójának (politikai, kulturális, gazdasági, személyes) digitális térbe helyeződése (a kibertér kialakulása) tény, amelynek pozitív hatásai csak annyiban tudnak megnyilvánulni, amennyiben az ott tárolt, közvetített adatokkal nem történik visszaélés (pl. lehallgatás, adatlopás, rombolás), illetve azok védve vannak a vétlen károsodástól is. Másként, az online tér jólétet eredményező továbbfejlődése a felhasználók bizalmától függ. A bizalom fenntartása pedig igényli a biztonságot.¹⁵ A biztonság biztosítása jellemzően eljárási, módszertani kérdés. Különösen is akkor, ha elfogadjuk, hogy nem létezik tökéletes biztonság az informatikai rendszerek esetében sem. Ekkor felértékelődik a kockázat csökkentése és annak előzetes felmérése. A HIR biztonság-szabályozása lényegében a hálózatok működésének (integritásába, külső behatástól mentességébe) biztonságába vetett bizalmat veszélyeztető kockázatok mérséklésének eljárásrendjét jelenti.

A HIR biztonságára három egymást kiegészítő szabályrendszer vonatkozik: (i) adatvédelmi, (ii) bűncselekményi tilalmak és (iii) a hálózati vagy információs rendszerek ellenállási képességének a fejlesztésére vonatkozó előírások. Ez utóbbi a szűken vett HIR biztonság szabályozás, amelynek célja véletlen vagy rosszindulatú műveletekkel szembeni védelem. Ilyen műveletek irányulhatnak a tárolt vagy továbbított adatok és ezen hálózatokon továbbított szolgáltatások elérhetőségére, hitelességére, integritására (az adatok külső behatástól mentessége) és biztonságára. Ezek a biztonsági incidensek az alábbi csoportokba oszthatók:

- Elektronikus kommunikáció lehallgatása, adatainak másolása vagy módosítása
- Engedély nélküli hozzáférés a számítógéphez és a számítógépes hálózathoz
- Romboló hatású támadás az interneten (pl.: DNS szerveret érintő, túlterheléses)
- Rosszindulatú szoftverek (pl. vírusok)
- Identitás rablás
- Természeti katasztrófák, szoftver/hardver hibák, emberi tévedés/mulasztás

Jelen tanulmány az *adatvédelmi* és szűken vett hálózati vagy információs rendszerek *ellenállási képességére* vonatkozó szabályozási elvárásokkal foglalkozik.

A HIR ellenálló képességére vonatkozó szabályozás jellemzője, hogy miután a fenyegetések és veszélyek nem küszöbölhetőek ki teljes mértékig, továbbá nem rendelkezünk megfelelő elrettentő mechanizmussal (a szándékolt támadások például gyorsak, nehezen észrevehetőek és az elkövetők felderítése a technikai és globális jellege miatt nehézségekbe ütközik), ezért a szabályozás eszközrendszerében jelzési mechanizmus, megelőzés, együttműködés és a legjobb gyakorlatok cseréje szerepel. Miután a fenyegetések is globálisak, ezért a fellépés is hatékonyabb lehet a nemzetinél magasabb szinten, amely az EU-ban uniós szintű szabályozás létrehozását indokolta. Ezért a HIR biztonság szabályozását alapvetően az *EU oldaláról* tekintjük át.

13 2013. évi L. törvény (4. lj.) 1. és 2. preambulumbekkezdés.

14 Uo., 2. preambulumbekkezdés.

15 Ez megjelenik Magyarország Nemzeti Kiberbiztonsági Stratégiájában is. 1139/2013. (III.21.) Korm. határozat 8. pont.

4. Az Európai Unió HIR biztonsági szabályozása

4.1. Az EU szabályozás fejlődése

4.1.1. A szabályozás szükségességének felismerése, kezdeti javaslatok

Az elektronikus hírközlő hálózatokon keresztül megvalósuló, megbízható és biztonságos információközlés egyre inkább központi kérdés a gazdaság és a társadalom egésze számára. Műszaki hibák, balesetek, támadások egyaránt következményekkel járhatnak a fizikai infrastruktúra azon elemeinek működésére és rendelkezésre állására nézve, amelyek fontos szolgáltatásokat – beleértve az elektronikus kormányzati vagy energetikai szolgáltatásokat – tesznek elérhetővé az Európai Unió polgárai számára. Éppen ezért az Európai Bizottság már 2001-ben javaslatot fogalmazott meg az európai hálózati és információs rendszerek biztonságának közös európai megközelítésére.¹⁶

A Bizottság szerint: „(...) A biztonság egyre inkább kulcsfontosságú tényezővé válik, hiszen a kommunikáció és az információ áramlás alapja a gazdasági és társadalmi fejlődésnek (...)”.¹⁷ A biztonság megteremtése egy összetett és bonyolult folyamat. A biztosítandó területet növeli az a tényező, hogy az infokommunikációs technológiák jelentős része magánkézben van. Az egyes felhasználók számára ugyanolyan fontos a személyes adataik és az *'online personality'* védelme, mint az állami, kormányzati rendszerekben tárolt adataik biztonsága. Éppen emiatt a diverzitás miatt, az adekvát válasz megtalálása a biztonsági kihívásokra egy rendkívül összetett feladat.¹⁸ A biztonság, összetettségéből adódóan, komplex megvalósítást igényel. A helyesnek és eredményesnek vélt eszközöket a Bizottság fel is sorolja. Ezek a „(...) tudatosság növelése, egy európai figyelmeztető rendszer felállítása, technológiai támogatás, támogatni a piacorientált szabványok és tanúsítványok kialakítását, kormányzati információs biztonság megteremtése és a globális együttműködés (...)”.¹⁹

A Bizottság szerint a HIR rendelkezések szükségesek az adatvédelmi és bűncselekményi tilalmak mellett. A HIR a hálózati vagy információs rendszerek ellenállási képessége a biztonság egy meghatározott szintjén a véletlen vagy rosszindulatú műveletekkel szemben. Ilyen műveletek irányulhatnak a tárolt vagy továbbított adatok és ezen hálózatokon továbbított szolgáltatások elérhetőségére, hitelességére, integritására (az adatok külső behatástól mentessége) és biztonságára.

4.1.2. A biztonságos információs társadalomra irányuló stratégia: „párbeszéd, partnerség, felvértezés és felelősségvállalás”

A Bizottság 2006-ban újabb közleményt adott ki, amely további lépésekre ösztönöz. „(...) A nemzetközi, európai és nemzeti szinten megtett erőfeszítések ellenére a biztonság kérdése

16 Communication from the Commission: Network and Information Security: Proposal for an European Policy Approach COM(2001)298.

17 Uo., 2.

18 Uo., 6.

19 Uo., 4.

továbbra is komoly problémákat vet fel (...).²⁰ Megemlíti a hálózatokat fenyegető veszélyek új irányait és céljait.

„Az illegális adatbányászat terjed – egyre inkább a felhasználók tudtán kívül – miközben gyorsan növekedik a rosszindulatú szoftverek (malware) variációinak száma (és fejlődésük gyorsasága). A kéretlen elektronikus levelek jó példaként szolgálnak erre a folyamatra: vírusok, csalárd és bűntetendő cselekmények hordozójává válnak, például a kémprogramok (spyware), az adathalászat (phishing).”²¹

A folyamatosan fejlődő technikai háttérrel párhuzamosan bővül a rosszindulatú támadások szintere is. Az információs rendszerek nagymértékű elterjedése és általánossá válása, jelentős kihívások elé állítanak minden szereplőt, különösen a közigazgatást, a közszektort. A vállalkozásoknak a versenyképességük függhet a megfelelő biztonságtól és tudatosságtól. A magánszemélyek pedig ugyanúgy veszélyeztetettek, hiszen ugyanazokat a hálózatokat használják, mint az előző két szereplő.

Szükséges a biztonsági kultúra javítása a köz- és a magánszféra bevonásával. Ennek három pilléréként – a közlemény címében is szereplő – párbeszéd, partnerség, felvértezés és felelősségvállalást jelöli meg ekkor a Bizottság. Ennek keretében el kell indítani egy széleskörű társadalmi vitát. Össze kell gyűjteni a megoldási javaslatokat (a Bizottság erre felkéri az Európai Hálózat- és Információbiztonsági Ügynökséget (ENISA) (erről a szervezetről lentebb részletesen is lesz szó). Továbbá „(...) [a] Bizottság meg fogja kérni az ENISA-t, hogy vizsgálja meg egy európai információcsere és riadó rendszer kivitelezésének lehetőségét, az elektronikus hálózatokat fenyegető meglévő és jövőbeni veszélyekre való hatékony reagálás megkönnyítése érdekében (...)”²² A Bizottság szerint elő kell segíteni a tudatosságot, képzési programokat kell indítani, szabványokat kell kialakítani, megfelelő kezelési módszereket kell kidolgozni. „(...) Az EU-ban az informatikai rendszerekkel és hálózatokkal kapcsolatos biztonsági kihívások felismerése és az azoknak való megfelelés valamennyi érdekelt teljes elkötelezettségét teszi szükségessé (...)”²³ Mindezt a hálózat- és információbiztonság egy magasabb szintre emelésének érdekében.

4.1.3. A digitális menetrend

2010-ben a Bizottság kiadta a digitális menetrendre vonatkozó közleményét.²⁴ Erre az időpontra, az információs technológiák térnyerése még (az addigiaknál is) nagyobb méreteket öltött. A Bizottság kiemelt szerepet tulajdonított a hálózat- és információbiztonságnak és kiemeli azt, hogy a felhasználóknak bízniuk kell e használt rendszerekben. Meg kell őket védeni az itt fellelhető veszélyektől, ezen a területen is fel kell lépni a megjelenő bűnözés ellen. „(...) Az ilyen fenyegetések elhárítása és a védelem megerősítése a digitális társadalom közös

20 A Bizottság közleménye: A biztonságos információs társadalomra irányuló stratégia: „párbeszéd, partnerség, felvértezés és felelősségvállalás” COM(2006) 251 végleges. 4.

21 Uo., 4-5.

22 Uo., 9.

23 Uo., 10.

24 A Bizottság közleménye: A Digitális menetrend COM (2010) 245 végleges.

felelőssége, melyből – belföldön és világszerte egyaránt – ki kell venniük a részüket mind az egyéneknek, mind a magán- és állami szervezeteknek (...).²⁵ A dokumentum további lépésekre sarkallja az EU-t, illetve a tagállamokat.

4.1.4. *European Cybersecurity Strategy 2013*

2013-ban ez Unió kiadta saját kiberbiztonsági stratégiáját²⁶. Az elmúlt két évtizedben az internethasználat folyamatosan bővült. A szabályozók ezt követték is. Az Unió szervei folyamatosan adtak ki dokumentumokat a kibertér biztonságosabbá tételére vonatkozó elképzeléseikkel kapcsolatban. A Bizottság folyamatos javaslataival és közleményeivel segítette ezt a folyamatot. A jogalkotásban is megjelentek irányelvek és egyéb jogi eszközök a harmonizáció érdekében. Ez a stratégia, azonban még szorosabbra kívánja fűzni az együttműködést. „(...)A konkrét intézkedések célja növelni az információs rendszerek ellenálló képességét az internetes támadásokkal szemben, visszaszorítani a számítástechnikai bűnözést, továbbá megerősíteni az EU nemzetközi kiberbiztonsági szakpolitikáját és kibervédelmét (...).²⁷

A dokumentum szerint a felhasználók még mindig nem bíznak eléggé a kibertérben. Nem használják eléggé ezt a közeget életük megkönnyítése érdekében. A kiber-online térben lévő potenciált ki kell használni. Azonban ehhez biztonságossá kell tenni azt. Az eddigi biztonságossá tételi törekvések továbbfejlesztésére van szükség a Bizottság szerint. „(...) Az Európai Unió alapértékei ugyanolyan mértékben vonatkoznak a digitális világra, mint a fizikai világra. [...] Az Európai Uniónak olyan internetes környezetet kell biztosítania, amely mindenki számára lehetővé teszi a lehető legnagyobb mérvű szabadságot és biztonságot (...).²⁸ Ez az új stratégia ennek elérésére ad egy öt pontos tervet, javaslatot. Meghatározza az elsődleges intézkedéseket, ezek a következők:

„(...)a kibertámadásokkal szembeni ellenálló képesség elérése; a számítástechnikai bűnözés drasztikus csökkentése; kibervédelmi politika és képességek kifejlesztése a közös biztonság- és védelempolitika (KBVP) tekintetében; kiberbiztonsági ipari és technológiai erőforrások kifejlesztése; összefüggő nemzetközi szakpolitika létrehozása a kibertér vonatkozásában az Európai Unió számára, és az Unió alapértékeinek támogatása.”²⁹

A kibertámadásokkal szembeni ellenálló képesség elérése érdekében, a tagállamok számára több kötelezettség keletkezik. „(...)A HIR illetékes nemzeti hatóságok kijelölése; jól működő, hálózatbiztonsági vészhelyzeteket elhárító csoport (CERT) létrehozása; és a HIR-re vonatkozó nemzeti stratégia és nemzeti együttműködési terv elfogadása (...).³⁰ A Bizottság továbbá

25 Uo., 19.

26 EU Cybersecurity plan to protect open internet and online freedom and opportunity - Cyber Security strategy and Proposal for a Directive, www.ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security.

27 Uniók kiberbiztonsági terv a nyílt internet, valamint az online szabadság és lehetőségek védelmére, europa. http://europa.eu/rapid/press-release_IP-13-94_hu.htm

28 Az Európai Unió külügyi és biztonságpolitikai főképviselője: Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér 4.-5.

www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=JOIN:2013:0001:FIN:HU:PDF.

29 Uo., 5.

30 Uo., 6.

kéri a Parlamentet és a Tanácsot az információ- és hálózatbiztonságra vonatkozó egységes irányelv elfogadására.

4.2. HIR ellenálló képességére vonatkozó EU szabályozás

A HIR *ellenálló képességét* növelő szabályozás eszköztára:³¹ globális megközelítés (EU szintű szabályozás van, amely figyelembe veszi a tagállamok alapvető biztonsági érdekeit, akik megtehetik a szükséges intézkedéseket a saját védelmük érdekében³²), minimum standardok, információcsere, együttműködés, kritikus infrastruktúrák szigorúbb védelme.

4.2.1. A HIR irányelv

A 2013-ban javasolt irányelv 2016-ban került elfogadásra. Az Európai Parlament és a Tanács 2016/1148/EU Irányelve³³(a továbbiakban: Irányelv) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szól. Az Irányelv folytatja azt a logikát, hogy az együttműködést fokozni kell, miként a kiberbiztonsági stratégiának is ez volt a célja, az Irányelvnek is ez a központi eleme.

„(...)A meglévő képességek nem elegendőek ahhoz, hogy garantálják a hálózati és információs rendszerek magas biztonsági szintjét az Unión belül. A tagállamok felkészültségi szintje nagyon különböző, ami sokféle megközelítés alkalmazásához vezetett az Unióban. Ez a fogyasztók és a vállalkozások egyenlőtlen védelmét eredményezi, továbbá aláássa a hálózati és információs rendszerek biztonságának általános szintjét az Unión belül (...).”³⁴

Az Irányelv egyik legnagyobb innovációja, hogy az eddig ágazatspecifikus szabályozások mellé, megteremt egy ágazatokon felüli általános minimumot. A tagállamoknak lehetőségük van az eddigi, meglévő szabályok alkalmazására. Azonban „(...) [a] tagállamoknak tájékoztatniuk kell a Bizottságot az ilyen lex specialis-ra vonatkozó rendelkezések alkalmazásáról (...).”³⁵ Fontos, hogy ezek a meglévő szabályok ugyanolyan (vagy magasabb) biztonsági szintet biztosítsanak. Másik újítása a szabályozásnak, hogy még inkább szorosabbra fűzi az együttműködést. Az eddigi önkéntes gyakorlatokat felváltja egy szabályozott, kötelező együttműködés.

a) Az Irányelv tárgya és hatálya

Az Irányelv a belső piac működésének javítására hivatkozva kötelezettségeket állapít meg a tagállamok felé. Ennek célja, hogy egy egységes, magas színvonalú hálózat- és információ-

31 L. 2013. évi L. törvény (4. lj.) 6. preambulumbekkezdés.

32 Uo., 8. preambulumbekkezdés.

33 Irányelv i.m. (7. lj.).

34 Uo., 5. preambulumbekkezdés.

35 Uo., 9. preambulumbekkezdés.

biztonság jöjjön létre. Ezek a kötelezettségek egyértelműen az együttműködést és reagálást, majd a közös fellépést helyezik előtérbe. Az Irányelv személyi hatálya átfogja a tagállamokon felül az alapvető szolgáltatást nyújtó szereplőket, a digitális szolgáltatókat, továbbá magát az Unió egyes szerveit. A tárgyi hatály keretét a személyi hatály alá tartozók feladatai alkotják. Ezek igen sokrétűek:³⁶

- a tagállamoknak el kell fogadniuk a hálózati és információs rendszerek biztonsága nemzeti stratégiáját;
- létrejön egy együttműködési csoport a tagállamok közötti stratégiai együttműködés és információcsere támogatása és elősegítése céljából;
- létrejön a számítógép-biztonsági eseményekre reagáló csoportok hálózata (a továbbiakban: CSIRT-ek hálózata);
- biztonsági és bejelentési követelmények kerülnek megállapításra az alapvető szolgáltatásokat nyújtó szereplők és a digitális szolgáltatók számára;
- a tagállamok számára kötelezettségeket állapít meg arra vonatkozóan, hogy a hálózati és információs rendszerek biztonságával kapcsolatos feladatok ellátására jelöljenek ki nemzeti illetékes hatóságokat, egyedüli kapcsolattartó pontokat, valamint CSIRT-eket.

Az irányelv nem érinti azokat az intézkedéseket, amelyeket a tagállamok az alapvető állami funkcióik védelme, és különösen a nemzetbiztonság védelme érdekében hoznak, ideértve az olyan információk védelmét szolgáló intézkedéseket is, amelyek közlését a tagállamok ellentétesnek tartják alapvető biztonsági érdekeikkel.³⁷

b) Alapvető szolgáltatást nyújtó szolgáltató szereplők

A tagállamoknak 2018. november 9-ig kell azonosítaniuk a területükön letelepedett, alapvető szolgáltatásokat nyújtó szereplőket. [5. cikk (1) bekezdés] Ehhez az Irányelv meghatározza az érintett ágazatokat a II. mellékletben (ágazati szempont) és megadja az azonosításhoz szükséges ágazatoktól független szempontokat is: „(...) a) a szervezet a kritikus társadalmi és/vagy gazdasági tevékenységek fenntartásához alapvető szolgáltatást nyújt; b) az adott szolgáltatás nyújtása hálózati és információs rendszerektől függ; és c) az említett szolgáltatást érintő biztonsági esemény jelentős zavart okozna a szolgáltatás nyújtásában (...)”.³⁸ A jelentős zavar megítéléséhez az Irányelv további szempontokat ad: érintett felhasználók száma, gazdaságra/társadalomra gyakorolt hatás, érintett piaci szereplő részesedése, a biztonsági esemény lehetséges földrajzi kiterjedése, a szervezet jelentősége a szolgáltatás elégséges szintje fenntartása szempontjából (...).³⁹

A *biztonsági esemény* minden olyan esemény, amely ténylegesen kedvezőtlen hatást gyakorol a hálózati és információs rendszerek biztonságára.⁴⁰ A tagállamok biztosítják, hogy az alapvető szolgáltatásokat nyújtó szereplők indokolatlan késedelem nélkül bejelentik az illetékes hatóságnak vagy a CSIRT-nek, az általuk nyújtott alapvető szolgáltatások folytonosságára jelentős hatást gyakorló biztonsági eseményeket.⁴¹ Egy biztonsági esemény hatása

36 Uo., 1. cikk (2) bekezdés.

37 Uo., 1. cikk (6) bekezdés.

38 Uo., 5. cikk (2) a) - c).

39 Uo., 6. cikk.

40 Uo., 4. cikk 7. pont.

41 Uo., 14. cikk (3) bekezdés.

jelentőségének meghatározása érdekében, elsősorban az alábbi paramétereket kell figyelembe venni: érintett felhasználók száma, biztonsági esemény időtartama és földrajzi kiterjedése.⁴² A biztonsági események bejelentése kapcsán és azok nyilvánosságra hozása során mérlegelni kell az ezzel járó az előnyöket és hátrányokat (pl. hírnévre, kereskedelmi tevékenységre gyakorolt hatás), különösen is a HIR gyenge pontok nem derülhetnek ki.⁴³

A tagállamok biztosítják, hogy az alapvető szolgáltatásokat nyújtó szereplők megfelelő és arányos műszaki és szervezési intézkedéseket tegyenek a működésük során általuk használt hálózati és információs rendszerek biztonságát fenyegető kockázatok *kezelése* érdekében és gondoskodnak a HIR biztonságát érintő események *megelőzésére* és azok hatásainak csökkentésére szükséges intézkedésekről is annak céljából, hogy biztosítsák az említett szolgáltatások folytonosságát.⁴⁴

c) Digitális szolgáltatók

A digitális szolgáltató csak jogi személy lehet⁴⁵. A digitális szolgáltatás pedig az (EU) 2015/1535 Európai Parlamenti és Tanácsi Irányelv 1. cikke (1) bekezdésének b) pontja szerinti, a III. mellékletben felsorolt típusok valamelyiknek megfelelő szolgáltatás.⁴⁶ E szerint digitális szolgáltatás az „(...) információs társadalom bármely szolgáltatása, azaz bármely, általában térítés ellenében, távolról, elektronikus úton és a szolgáltatást igénybe vevő egyéni kérelmére nyújtott szolgáltatás (...)”.⁴⁷ Az irányelv hatálya azonban csak a III. melléklet szerinti online piactér, keresőprogram és felhőalapú szolgáltatásokat nyújtó digitális szolgáltatókra terjed ki.

A digitális szolgáltatók annak a tagállamnak a joghatósága alá tartoznak, amelyben a központi ügyvezetésük helye található.⁴⁸ Úgy kell tekinteni, hogy egy digitális szolgáltató központi ügyvezetésének helye abban a tagállamban van, amelyben a székhelye található. Azon digitális szolgáltatóknak, amelyek az Unióban nincsenek letelepedve, azonban az Unión belül kínálják a III. mellékletben említett szolgáltatásokat, az Unióban letelepedett képviselőt kell kijelölniük.⁴⁹ Úgy kell tekinteni, hogy a digitális szolgáltató annak a tagállamnak a joghatósága alá tartozik, amelyben a képviselő letelepedett. Az a tény, hogy a digitális szolgáltató képviselőt jelöl ki, nem érinti a magával a digitális szolgáltatóval szembeni keresetindításhoz való jogot.⁵⁰

A tagállamoknak a digitális szolgáltatókat nem kell azonosítaniuk, mivel ezt az irányelvet a hatálya alá tartozó *minden* digitális szolgáltatóra alkalmazni kell.⁵¹ Az irányelv nem gátolja azonban a tagállamokat abban, hogy az uniós jog szerinti kötelezettségeik sérelme nélkül biz-

42 Uo., 14. cikk (4) bekezdés.

43 Uo., 14. cikk (5) bekezdés.

44 Uo., 14. cikk (1) bekezdés.

45 Uo., 4. cikk 6. pont.

46 Uo., 4. cikk 5. pont.

47 Az Európai Parlament és a Tanács (EU) 2015/1535 irányelve (2015. szeptember 9.) a műszaki szabályokkal és az információs társadalom szolgáltatásaira vonatkozó szabályokkal kapcsolatos információszolgáltatási eljárás megállapításáról OJ L 241, 17.9.2015., 1. cikke (1) bekezdésének b) pontja.

48 Uo., 18. cikk (1) bekezdés.

49 Uo., 18. cikk (2) bekezdés.

50 Uo., 18. cikk (3) bekezdés.

51 Uo., 57. preambulumbekkezdés.

tonsági és bejelentési követelményeket állapítsanak meg azon szervekre vonatkozóan, amelyek nem minősülnek az e rendelet hatálya szerinti digitális szolgáltatóknak.⁵²

A tagállamok biztosítják, hogy a digitális szolgáltatók megfelelő és arányos műszaki és szervezési intézkedéseket határoznak és tesznek meg a HIR biztonságát fenyegető kockázatok kezelése érdekében.⁵³ A tagállamok biztosítják, hogy a digitális szolgáltatók intézkedéseket hoznak annak érdekében, hogy megelőzzék és csökkentsék a hálózati és információs rendszereik biztonságát érintő biztonsági események hatásait, annak céljából, hogy biztosított legyen az említett szolgáltatások folytonossága.⁵⁴ Annak elkerülése érdekében, hogy az alapvető szolgáltatásokat nyújtó szereplőkre és a digitális szolgáltatókra aránytalanul nagy pénzügyi és adminisztratív terhek háruljanak, a követelményeknek – a legújabb technikai lehetőségekre figyelemmel – *arányosaknak* kell lenniük az adott hálózati és információs rendszert érintő kockázatokkal. Digitális szolgáltatók esetében az említett követelmények a mikro- és kisvállalkozásokra nem alkalmazandók.⁵⁵

Az intézkedéseket ott kell megtenni, ahol a fenyegetettség fennáll. Nem vonatkozik ezért az irányelv olyan online szolgáltatásokra, amelyek különböző kereskedők által kínált azonos termékek vagy szolgáltatások árát hasonlítják össze, majd a termék megvásárlása céljából a kiválasztott kereskedőhöz irányítják a felhasználót.⁵⁶ Bár a hardvergyártók és a szoftverfejlesztők nem minősülnek alapvető szolgáltatást nyújtó szereplőknek vagy digitális szolgáltatóknak, termékeik fokozzák a hálózati és információs rendszerek biztonságát. Emiatt fontos szerepet játszanak, hiszen lehetővé teszik az alapvető szolgáltatásokat nyújtó szereplők és a digitális szolgáltatók számára, hogy biztonságossá tegyék hálózati és információs rendszereiket. Az említett hardver- és szoftvertermékekre a termékfelelősségre vonatkozó hatályos szabályok vonatkoznak.⁵⁷

A tagállamok biztosítják, hogy a digitális szolgáltatók indokolatlan késedelem nélkül bejelentenek az illetékes hatóságnak vagy a CSIRT-nek minden olyan biztonsági eseményt, amely jelentős hatást gyakorol az általuk kínált szolgáltatás nyújtására.⁵⁸ Annak megítéléséhez, hogy a biztonsági esemény jelentős-e, az alapvető szolgáltatásoknál említett körülményekhez képest meg kell vizsgálni a zavar mértékét és a gazdasági/társadalmi tevékenységre gyakorolt hatást is. Ugyanúgy, mint az alapvető szolgáltatásokat nyújtók esetében, az illetékes hatóságok felé bejelentett biztonsági események nyilvánosságra hozatala tekintetében, két dolgot kell kellően mérlegelni: egyrészt azt, hogy milyen előnyök származnak abból, ha a nyilvánosságot tájékoztatják a fenyegetésekről, másrészt pedig azt, hogy a nyilvánosságra hozatal esetlegesen milyen károkat okozhat a biztonsági eseményeket bejelentő, alapvető szolgáltatásokat nyújtó szereplők és digitális szolgáltatók hírneve és kereskedelmi tevékenysége szempontjából.⁵⁹ A bejelentési kötelezettségek teljesítése során az illetékes hatóságoknak és a CSIRT-eknek külön figyelmet kell fordítaniuk arra, hogy a megfelelő biztonsági korrekciós intézkedések meghozataláig a termékek gyenge pontjai szigorúan titokban maradjanak.

52 Uo., 58. preambulumbekkezdés.

53 Uo., 16. cikk (1) bekezdés.

54 Uo., 16. cikk (2) bekezdés.

55 Uo., 53. preambulumbekkezdés.

56 Uo., 15. preambulumbekkezdés.

57 Uo., 50. preambulumbekkezdés.

58 Uo., 16. cikk (3) bekezdés.

59 Uo., 59. preambulumbekkezdés.

A digitális szolgáltatókra az általuk nyújtott szolgáltatások és az általuk végzett tevékenységek jellege okán kevésbé szigorú és reaktív utólagos felügyeleti tevékenységnek kell vonatkoznia. Az érintett illetékes hatóságnak ezért csak akkor – különösen egy biztonsági esemény bekövetkeztét követően – kell lépéseket tennie, ha minden kétséget kizáróan tudomást szerez arról, például magától a digitális szolgáltatótól, egy másik – akár egy másik tagállami – illetékes hatóságtól, vagy a szolgáltatás igénybevevőjétől, hogy a digitális szolgáltató nem felel meg ezen irányelv követelményeinek. A digitális szolgáltatók felügyeletét ezért nem kell az illetékes hatóság számára általános kötelezettségként előírni.⁶⁰

d) Tagállami feladatok

A hálózati és információs rendszerek magas biztonsági szintjének elérése és fenntartása érdekében „(...) [a] tagállam elfogad egy hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégiát, amelyben meghatározza a stratégiai célokat, valamint a hálózati és információs rendszerek magas szintű biztonságának megteremtéséhez és fenntartásához szükséges megfelelő szakpolitikai és szabályozási intézkedéseket (...)”⁶¹ Az irányelv meghatároz bizonyos kérdésköröket, amelyeket bele kell foglalni ebbe a stratégiába: célok, prioritások megjelölése; a célok teljesítését szolgáló irányítási rendszer kijelölése, a szereplők feladatai és felelőssége; „(...) a felkészültségre, a reagálásra és a helyreállításra vonatkozó intézkedések azonosítása, ideértve a köz- és a magánszféra közötti együttműködést is(...)”; oktatási, tájékoztatási, egyéb kapcsolódó programok megjelölése; kutatási, fejlesztési tervek megjelölése; kockázatkezelési terv készítése; végrehajtásba bevont szereplők jegyének elkészítése.⁶²

„(...) Az illetékes hatóságoknak tagállami szinten kell monitoringozniuk ezen irányelv alkalmazását. Az egyedüli kapcsolattartó pontnak kell ellátnia az összekötő feladatokat a tagállami hatóságok közötti és a többi tagállam érintett hatóságaival folytatott, határokon átnyúló együttműködés, valamint a 11. cikkben említett együttműködési csoporttal és a 12. cikkben említett CSIRT-ek hálózatával folytatott együttműködés biztosítása céljából (...)”⁶³

Minden tagállam – legalább az alapvető szolgáltatásokat nyújtó szervezetek és az irányelv által lefedett digitális szolgáltatásokra vonatkozóan – kijelöl egy vagy több CSIRT-et, amelyek a kockázatoknak és a biztonsági eseményeknek egy jól meghatározott eljárással összhangban történő kezeléséért felelősek.⁶⁴ A CSIRT-ek kötelezettségei többek között: biztosítaniuk kell a hírközlési szolgáltatásaik magas szintű elérhetőségét, továbbá elérhetőségük és másokkal való kapcsolattartásuk céljára, folyamatosan több eszközt kell fenntartaniuk; lehetővé kell tenni, hogy részt vehessenek nemzetközi együttműködési hálózatokban; hivatali helyiségeiket és a támogató információs rendszereket biztonságos helyszíneken kell elhelyezni; üzletmenetük folytonosságát biztosítani kell.⁶⁵ A CSIRT-ek feladatai: a biztonsági események nemzeti szintű monitoringja; a kockázatokkal és biztonsági eseményekkel kapcsolatos korai előrejelzés,

60 Uo., 60. preambulumbekzdés.

61 Uo., II. Fejezet, 7. cikk (1).

62 Uo., II. Fejezet, 7. cikk.

63 Uo., 8. cikk (2) és (4).

64 Uo., 9. cikk (1) bekezdés.

65 Uo., I. Melléklet (1) bekezdés.

riasztás, bejelentéstétel és információterjesztés a releváns érdekelték számára; reagálás a biztonsági eseményekre; a CSIRT-ek hálózatában való részvétel.⁶⁶

A tagállamok biztosítják, hogy vagy az illetékes hatóságok, vagy a CSIRT-ek megkapják az ezen irányelv alapján tett bejelentéseket a biztonsági eseményekről.⁶⁷ A tagállamok biztosítják, hogy az illetékes hatóságok, illetve a CSIRT-ek tájékoztatják az egyedüli kapcsolattartó pontokat az ezen irányelv alapján bejelentett biztonsági eseményekről.

e) Együttműködés

Egy együttműködési csoport kerül létrehozásra a tagállamok közötti stratégiai együttműködés és információcsere támogatása és megkönnyítése, a bizalom megerősítése, valamint a hálózati és információs rendszerek egységesen magas szintű biztonságának Unión belüli megvalósítása érdekében.⁶⁸ Az együttműködési csoport a tagállamok, a Bizottság és az ENISA képviselőiből áll, titkárságát a Bizottság biztosítja. Feladatai közé tartozik többek között: stratégiai iránymutatást nyújt a CSIRT-ek hálózata által végzett tevékenységekhez, biztosítja a bevált gyakorlatok tagállamok közötti cseréjét, megvitatja a tagállamok képességeit és felkészültségét, összegyűjti a kockázatokkal és biztonsági eseményekkel kapcsolatos bevált gyakorlatra vonatkozó információkat, az ENISA segítségével megosztja a bevált gyakorlatot az alapvető szolgáltatásokat nyújtó szereplők tagállami meghatározásával kapcsolatban.⁶⁹

A tagállamok közötti bizalom erősítése, valamint a gyors és hatékony operatív együttműködés előmozdítása érdekében, létrejön a nemzeti CSIRT-ek hálózata.⁷⁰ A CSIRT-ek hálózata a tagállamok CSIRT-jei és a CERT-EU képviselőiből áll. A Bizottság megfigyelőként vesz részt a CSIRT-hálózatban. Az ENISA biztosítja a titkárságot, és aktívan támogatja a CSIRT-ek közötti együttműködést. Feladatai közé tartozik különösen: önkéntesen megosztja és rendelkezésre bocsátja az egyes biztonsági eseményekre vonatkozó nem bizalmas információkat, valamely tagállami CSIRT képviselőjének kérésére megvitatja az érintett tagállam joghatósága alá tartozó területen bekövetkezett biztonsági eseményt, és lehetőség szerint koordinált választ ad a problémára.⁷¹

4.2.2. ENISA

A 2004/97/EK határozattal a tagállamok képviselői úgy határoztak, hogy a Bizottság által előterjesztett javaslat alapján létrehozandó Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) székhelye Görögországban, egy, a görög kormány által kijelölendő városban lesz. Ezt a határozatot követően a görög kormány az ENISA székhelyeként a Kréta szigetén található Iráklíót jelölte ki. A 526/2013/EU rendelet⁷² célja az Ügynökség megerősítése an-

66 Uo., I. Melléklet (2) bekezdés.

67 Uo., 10. cikk (2) bekezdés.

68 Uo., 11. cikk (1) bekezdés.

69 Uo., 11. cikk (3) bekezdés.

70 Uo., 12. cikk (1) bekezdés.

71 Uo., 12. cikk (3) bekezdés.

72 526/2013/EU rendelet az Európai Unió Hálózat- és Információbiztonsági Ügynökségről (ENISA) HL L 165/41. 2013. május 21.

nak érdekében, hogy sikeresen járulhasson hozzá az uniós intézmények és a tagállamok azon erőfeszítéseihez, amelyekkel európai kapacitást kívánnak létrehozni a hálózat- és információbiztonság területén jelentkező kihívások kezelésére.⁷³

Az ENISA tulajdonképpen egy uniós szintű szakértői központ, amely a hálózat- és információbiztonság területén iránymutatással, tanácsadással és segítségnyújtással szolgál, és amelyre az uniós intézmények és a tagállamok támaszkodhatnak. Feladatai közé tartozik különösen is:

- segítséget nyújt és tanácsot ad az uniós hálózat- és információbiztonsági politikához és joghoz kapcsolódó valamennyi kérdésben; előkészítő munkát végez, tanácsot ad és elemzéseket készít az uniós hálózat- és információbiztonsági politika és jog fejlesztésével és naprakésszé tételével kapcsolatban;
- kérésükre támogatja a tagállamokat a hálózat- és információbiztonságot érintő problémák és váratlan események megelőzésének, észlelésének, elemzésének és az ilyen problémák és események kezelése képességének kialakítására és javítására irányuló erőfeszítéseikben, továbbá biztosítja számukra a szükséges ismereteket;
- támogatja a nemzeti/kormányzati és uniós hálózatbiztonsági vészhelyzeteket elhárító csoportok (CERT) képességeinek fejlesztését;
- támogatja az uniós hálózat- és információbiztonsági gyakorlatok szervezését és végzését,
- előmozdítja a bevált gyakorlatok kidolgozását és megosztását.

4.2.3. Elektronikus hírközlő hálózatokra vonatkozó ágazati követelmények

A 2016/1148/EU irányelv értelmében, az elektronikus hírközlési hálózatok is HIR-nek minősülnek [4. cikk 1. pont a)], ugyanakkor a HIR irányelv biztonsági és bejelentési követelményei nem alkalmazandók a nyilvános hírközlő hálózatokat szolgáltatókra és a nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújtó vállalkozásokra. [1. cikk (3) bekezdés] A biztonsági és bejelentési követelményeket az elektronikus hírközlés tekintetében a hatályos elektronikus hírközlési ágazatban a személyes adatok kezeléséről és a magánélet védelméről szóló 2002/58/EK irányelv (Adatvédelmi irányelv)⁷⁴ írja elő, ugyanakkor ezt az irányelvet a Bizottság javaslata hatályon kívül kívánja helyezni és helyébe egy új rendeletet kíván léptetni⁷⁵, amely megteremtené az összhangot az Európai Parlament és a Tanács (EU) 2016/679 rendeletével.⁷⁶ Ennek jegyében a biztonsági és bejelentési követelményeket az elektronikus hírközlés tekintetében is a GDPR tartalmazná, míg az elektronikus hírközlési adatvédelmi rendelet többek között a közlések titkosságára, a felhasználói végberendezéseken lévő adattárolásra, az ott tárolt adatokhoz való hozzáférésre vonatkozna, illetve a jogi személyek adatainak védelme tekintetében kiegészítené a GDPR-t.

73 Uo., 11. preambulumbekkezdés.

74 OJ L 201, 2002. 07. 31.

75 A Bizottság javaslata az elektronikus hírközlés során a magánélet tiszteletben tartásáról és a személyes adatok védelméről, valamint a 2002/58/EK irányelv hatályon kívül helyezéséről (elektronikus hírközlési adatvédelmi rendelet Brüsszel, 2017.1.10. COM (2017) 10 final 2017/0003 (COD).

76 A természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) OJ L 119, 4.5.2016. 1–88.

A 2002/21/EK irányelv alapján a tagállamok biztosítják, hogy a nyilvános hírközlő hálózatokat szolgáltató és a nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújtó vállalkozások *értesítsék* az illetékes nemzeti szabályozó hatóságot a biztonság megsértésének és az integritás hiányának minden olyan esetéről, amely jelentős hatással volt a hálózatok, illetve a szolgáltatások működésére. Az adott nemzeti szabályozó hatóság szükség szerint értesíti a többi tagállam nemzeti szabályozó hatóságát és az ENISA-t. Az adott nemzeti szabályozó hatóság tájékoztathatja a nyilvánosságot, illetve a vállalkozásokat erre kötelezheti, amennyiben úgy ítéli meg, hogy a biztonság megsértésének vagy az integritás hiányának nyilvánosságra hozatalához közérdek fűződik. Az érintett nemzeti szabályozó hatóság a beérkező bejelentésekről és az e bekezdésnek megfelelően tett intézkedésekről, évente összefoglaló jelentést nyújt be a Bizottságnak és az ENISA-nak. Az ENISA egyebek mellett szakértői tevékenységgel és tanácsadással, valamint a legjobb gyakorlati megoldások cseréjének elősegítésével járul hozzá az ilyen tárgyú műszaki és szervezési jellegű biztonsági intézkedések harmonizálásához.

A hatóságok kötelezhetik a vállalkozásokat:

- a) a szolgáltatásaik és a hálózataik biztonsági és/vagy integritási szintjének megállapításához szükséges adatok szolgáltatására, ideértve az írásos biztonsági stratégiájuk átadását is; és
- b) arra, hogy vessék alá magukat egy minősített független szerv vagy egy illetékes nemzeti hatóság által végzett biztonsági ellenőrzésnek, és az ellenőrzés eredményeit bocsássák a nemzeti szabályozó hatóság rendelkezésére. Az ellenőrzés költségei az adott vállalkozást terhelik.

Az elektronikus hírközlő hálózatok szolgáltatása, illetve az elektronikus hírközlési szolgáltatások nyújtása – bizonyos kivételekkel (pl. szám- és rádiófrekvencia használati jogok) – csak általános felhatalmazás tárgyát képezheti. Az érintett vállalkozástól megkövetelhető, hogy bejelentést tegyen a tevékenysége megkezdése előtt, de nem írható elő számára, hogy a szabályozó hatóság kifejezett határozatát előzetesen beszerezze. A bejelentés nem tartalmazhat többet, mint valamely nemzeti szabályozó hatóságnak címzett nyilatkozatot, az elektronikus hírközlési szolgáltatások nyújtásának megkezdésére irányuló szándékot, valamint olyan minimális adatokat, amelyek a nemzeti szabályozó hatóság számára a szolgáltatók nyilvántartása szempontjából szükségesek.⁷⁷ Az általános felhatalmazás alapján a vállalkozások jogosultak elektronikus hírközlő hálózatokat és elektronikus hírközlési szolgáltatásokat nyújtani és arra, hogy a létesítmény telepítéshez szükséges jogokra vonatkozó kérelmük elbírálásra kerüljön.⁷⁸ Ugyanakkor *mindez nem zárja ki, hogy a hálózatok biztonságával, a jogosulatlan hozzáféréssel szembeni követelmények legyenek az általános felhatalmazáshoz feltételként előírva.*

4.2.4. Kritikus infrastruktúrákra vonatkozó szabályozás

2005 decemberében a Bel- és Igazságügyi Tanács felkérte a Bizottságot, hogy terjesszen elő javaslatot a kritikus infrastruktúrák védelmére vonatkozó európai programról (European Programme for Critical Infrastructure Protection – a továbbiakban: az EPCIP), és úgy döntött, hogy a programnak összveszély-megközelítésen kell alapulnia, elsőbbséget adva a terrorizmusból eredő veszélyekkel szembeni küzdelemnek. E megközelítés értelmében, a kritikus infra-

77 Az elektronikus hírközlési hálózatok és szolgáltatások engedélyezéséről szóló 2002/20/EK irányelv HL L 108. 2002.4.24. 3. cikk.

78 Uo., 4. cikk.

struktúrák védelmével kapcsolatban figyelembe kell venni az ember által okozott technológiai veszélyeket és a természeti katasztrófákat is, azonban a terrorveszélynek kell elsőbbséget adni.⁷⁹

A 2008/114/EK irányelv, az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről az első lépést jelenti az európai kritikus infrastruktúrák (European Critical Infrastructure – a továbbiakban: az ECI) azonosítása és kijelölése, valamint védelmük javítása szükségességének értékelése terén alkalmazott fokozatos megközelítésben. Ez az irányelv az energiaágazatra és a közlekedési ágazatra összpontosít. Az ECI-k védelmének elsődleges és végső felelőssége a tagállamokat és az infrastruktúrák tulajdonosait/üzemeltetőit terheli.

a) Fogalom-meghatározás

Az irányelv kritikus infrastruktúrának tekinti a tagállamokban található azon eszközöket, rendszereket vagy ezek részeit, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához, az egészségügyhöz, a biztonsághoz, az emberek gazdasági és szociális jólétéhez, valamint amelyek megzavarása vagy megsemmisítése e feladatok folyamatos ellátásának hiánya miatt, jelentős következményekkel járna valamely tagállamban.⁸⁰ Az 'európai kritikus infrastruktúra' vagy 'ECI' a tagállamokban található olyan kritikus infrastruktúra, amelynek megzavarása vagy megsemmisítése jelentős hatással lenne legalább két tagállamra. A hatás jelentőségét a horizontális kritériumok alapján kell értékelni. Ide tartoznak azok a hatások is, amelyek az egyéb típusú infrastruktúrákkal fennálló, ágazatokon átnyúló kölcsönös függőségből erednek.⁸¹

b) ECI-k azonosítása

A fenti fogalmi elemek mellett, az irányelv horizontális és ágazati kritériumokat is előír, amelyek figyelembe vételével a tagállamok azonosítják az ECI-t. Az említett *horizontális* kritériumok⁸² közé a következők tartoznak:

- veszteségek kritériuma (a halottak és sebesültek feltételezhető száma alapján)
- gazdasági hatás kritériuma (a gazdasági veszteség és/vagy a termékek, illetve szolgáltatások romlásának mértéke alapján, ideértve a várható környezeti hatásokat is)
- társadalmi hatás kritériuma (a közbizalomra tett hatás, a fizikai szenvedés és a mindennapi élet rendjének felborulása alapján értékelve; beleértve az alapvető szolgáltatások veszteségeit is).

A horizontális kritériumok küszöbértékeit az adott infrastruktúra megzavarása, vagy megsemmisítése következményeinek súlyossága alapján kell meghatározni. A horizontális kritériumokra vonatkozó konkrét küszöbértékeket, az adott kritikus infrastruktúrában érintett tagállamok eseti alapon határozzák meg. Az irányelv végrehajtásában *érintett ágazatok* az energiaágazat és a közlekedési ágazat.⁸³

79 2008/114/EK irányelv az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről HL L 345/75 2008. december 8. 2. preambulumbekzdés.

80 Uo., 2. cikk a) pont.

81 Uo., 2. cikk b) pont.

82 Uo., 3. cikk (2) bekezdés.

83 Uo., 3. cikk (3) bekezdés.

Az ECI azonosítását a tagállamok a követő lépések sorozatán keresztül hajtják végre:⁸⁴

1. lépés) Az egy ágazaton belüli kritikus infrastruktúrák első körben történő kiválasztása érdekében, az egyes tagállamok az ágazati kritériumokat alkalmazzák.
2. lépés) Az 1. lépés alapján beazonosított potenciális ECI-kre az egyes tagállamok a kritikus infrastruktúrákra vonatkozó fogalom-meghatározást alkalmazzák. A hatás jelentőségét vagy a kritikus infrastruktúrák azonosítására szolgáló nemzeti módszerek alkalmazásával, vagy a horizontális kritériumok alapján állapítják meg, a megfelelő tagállami szinten. A kritikus szolgáltatásokat nyújtó infrastruktúra esetében figyelembe kell venni a lehetséges alternatívákat, valamint a megzavarás/helyreállítás időtartamát is.
3. lépés) Azon potenciális ECI-kre, amelyek megfeleltek ezen eljárás első két lépésének, az egyes tagállamok az ECI-re vonatkozó fogalom-meghatározás határon átnyúló jelleggel kapcsolatos elemét alkalmazzák. Azon potenciális ECI-kre, amelyek megfelelnek a fogalom-meghatározásnak, az eljárás következő lépését alkalmazzák. A kritikus szolgáltatásokat nyújtó infrastruktúra esetében figyelembe kell venni a lehetséges alternatívákat, valamint a megzavarás/helyreállítás időtartamát is.
4. lépés) Az így megmaradó potenciális ECI-kre az egyes tagállamok a horizontális kritériumokat alkalmazzák. A horizontális kritériumok figyelembe veszik: a hatás súlyosságát; valamint a kritikus szolgáltatásokat nyújtó infrastruktúra esetében a lehetséges alternatívákat, és a megzavarás/helyreállítás időtartamát. Azon potenciális ECI-k, amelyek nem elégitik ki a horizontális kritériumokat, nem tekintendők ECI-nek.

Az ezen eljárásnak megfelelt potenciális ECI-kről csak azon tagállamokat lehet tájékoztatni, amelyeket a potenciális ECI jelentős mértékben érinthet.

c) Az ECI-k kijelölése

Valamennyi tagállam ellátja a többi olyan tagállamot, amelyre egy adott potenciális ECI jelentős hatással lehet, az infrastruktúra beazonosításához szükséges információkkal, valamint tájékoztatja arról, hogy miért jelölte azt ki ECI-nek.⁸⁵ Valamennyi olyan tagállam, amelynek területén potenciális ECI található, két- és/vagy többoldalú megbeszéléseket folytat a többi olyan tagállammal, amelyre a potenciális ECI jelentős hatással lehet.⁸⁶ Ha egy tagállam megalapozottan úgy véli, hogy a potenciális ECI jelentős hatással lehet rá, de az a tagállam, amelynek a területén a potenciális ECI található, nem jelölte meg ilyenként, tájékoztathatja a Bizottságot arról a kívánságáról, hogy vonják be a kérdéssel kapcsolatos két- és/vagy többoldalú megbeszélésekbe. A Bizottság törekszik az érintettek közötti megállapodás előmozdítására. Az a tagállam, amelynek területén a potenciális ECI elhelyezkedik, az infrastruktúrát azt követően minősíti ECI-nek, hogy erről az adott tagállam és azon tagállamok, amelyekre az infrastruktúra jelentős hatást gyakorolhat, megállapodtak.⁸⁷ Szükséges azon tagállam beleegyezése, amelynek területén az ECI-nek kijelölendő infrastruktúra található.

⁸⁴ Uo., III. Melléklet.

⁸⁵ Uo., 4. cikk (1) bekezdés.

⁸⁶ Uo., 4. cikk (2) bekezdés.

⁸⁷ Uo., 4. cikk (3) bekezdés.

d) Intézkedések

Valamennyi kijelölt ECI tekintetében gondoskodni kell arról, hogy létezzen egy üzemeltetői biztonsági terv (Operator Security Plan – a továbbiakban: az OSP), vagy ezzel egyenértékű olyan intézkedések kerüljenek bevezetésre, amelyek magukban foglalják a jelentős eszközök meghatározását, a kockázatértékelést, valamint az ellenintézkedések és eljárások meghatározását, kiválasztását és rangsorolását.⁸⁸

Valamennyi kijelölt ECI tekintetében gondoskodni kell egy biztonsági összekötő tisztviselő kijelöléséről a kritikus infrastruktúrák védelméért felelős, megfelelő nemzeti hatóságokkal való együttműködés és kapcsolattartás megkönnyítése érdekében.⁸⁹

Az ECI-k tulajdonosai/üzemeltetői számára hozzáférést kell biztosítani a kritikus infrastruktúrák védelmével kapcsolatos legjobb gyakorlatokhoz és módszerekhez, elsősorban az érintett tagállami hatóságokon keresztül.⁹⁰ Az ECI-k hatékony védelme nemzeti és közösségi szinten egyaránt megköveteli a kommunikációt, a koordinációt és az együttműködést. Ez leghatékonyabban úgy érhető el, ha valamennyi tagállam az európai kritikus infrastruktúrák védelmével foglalkozó kapcsolattartó pontot nevez ki (European Critical Infrastructure Protection Contact Point – a továbbiakban: az ECIP kapcsolattartó pont), amely az európai kritikus infrastruktúrák védelmével kapcsolatos kérdéseket nemzeti szinten, valamint a többi tagállammal és a Bizottsággal is koordinálja.⁹¹ A valamely tagállam vagy a Bizottság nevében ezen irányelv alapján minősített információkat kezelő személyeknek megfelelő szintű biztonsági átvilágításon kell átesniük.⁹² A tagállamok, a Bizottság és az illetékes felügyeleti szervek biztosítják, hogy a kritikus infrastruktúrák védelmével kapcsolatosan a tagállamokhoz vagy a Bizottsághoz eljuttatott érzékeny információkat kizárólag a kritikus infrastruktúrák védelme céljából használják fel.⁹³

4.3. HIR biztonságát szolgáló adatvédelmi rendelkezések

4.3.1. A hálózati és informatikai biztonság garantálása, mint jogos érdek

Az érintett adatkezelő jogos érdekének minősül a közhatalmi szervek, számítástechnikai vészhelyzetekre reagáló egység (CERT), hálózatbiztonsági incidenskezelő egységek (CSIRT), elektronikus hírközlési hálózatok üzemeltetői és szolgáltatások nyújtói, valamint biztonságtechnológiai szolgáltatók által végrehajtott olyan mértékű személyes adatkezelés, amely a hálózati és informatikai biztonság garantálásához feltétlenül szükséges és arányos, vagyis adott titkossági szinten az érintett hálózat vagy információs rendszer ellenálló képessége az e hálózatokon és rendszereken tárolt vagy továbbított adatok, valamint az e hálózatok és rendszerek

88 Uo., 11. preambulumbekzdés.

89 Uo., 13. preambulumbekzdés.

90 Uo., 16. preambulumbekzdés.

91 Uo., 10. cikk.

92 Uo., 9. cikk (1) bekezdés.

93 Uo.

által nyújtott vagy rajtuk keresztül elérhető, kapcsolódó szolgáltatások hozzáférhetőségét, hi-telességét, integritását és bizalmas jellegét sértő véletlen eseményekkel, illetve jogellenes vagy rosszhiszemű tevékenységekkel szemben.⁹⁴ Ez magában foglalhatja például az elektronikus kommunikációs hálózatokhoz való engedély nélküli hozzáférés és a rosszindulatú program-terjesztés megakadályozását, továbbá a szolgáltatás megtagadásával járó támadások, valamint a számítógépes és elektronikus kommunikációs rendszerekben való károkozás megállítását.

4.3.2. Megfelelő technikai és szervezési intézkedések az adatkezelés biztonsága érdekében

Az Európai Parlament és a Tanács (EU) 2016/679 rendeletének – a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásá-ról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet, a továbbiakban: GDPR)⁹⁵ – 32. cikk (1) bekezdése szerint, az adatkezelő és az adatfeldolgozó a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, ha-tóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelen-tett, változó valószínűségű és súlyosságú kockázat figyelembevételével, megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja, ideértve, többek között, adott esetben:

- a) a személyes adatok álnevesítését és titkosítását;
- b) a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét;
- c) fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatok-hoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani;
- d) az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedé-sek hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljá-rást.

Ugyanezen cikk (2) bekezdése szerint a biztonság megfelelő szintjének meghatározásakor kifejezetten figyelembe kell venni az adatkezelésből eredő olyan kockázatokat, amelyek külö-nösen a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalá-ból, vagy az azokhoz való jogosulatlan hozzáféréstől erednek. A 32. cikk (3) bekezdése értel-mében az adatkezelő, illetve az adatfeldolgozó 40. cikk szerinti jóváhagyott magatartási kó-dexekhez vagy a 42. cikk szerinti jóváhagyott tanúsítási mechanizmushoz való csatlakozását felhasználhatja annak bizonyítása részeként, hogy az e cikk (1) bekezdésében meghatározott követelményeket teljesíti. A 32. cikk (4) bekezdése szerint az adatkezelő és az adatfeldolgozó intézkedéseket hoz annak biztosítására, hogy az adatkezelő vagy az adatfeldolgozó irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező természetes személyek kizárólag az adatkezelő utasításának megfelelően kezelhessék az említett adatokat, kivéve, ha az ettől való eltérésre uniós vagy tagállami jog kötelezi őket.

94 L. GDPR rendelet 49. preambulumbekzdés.

95 OJ L 119, 4.5.2016. 1–88.

4.3.3. Az adatvédelmi incidens bejelentése a felügyeleti hatóságnak

A GDPR 33. cikk (1) bekezdése értelmében, az adatvédelmi incidenst⁹⁶ az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti az illetékes felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is. Ugyanezen cikk (2) bekezdése szerint az adatfeldolgozó az adatvédelmi incidenst, az arról való tudomásszerzését követően, indokolatlan késedelem nélkül bejelenti az adatkezelőnek. A 33. cikk (5) bekezdése alapján az adatkezelő nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket. E nyilvántartás lehetővé teszi, hogy a felügyeleti hatóság ellenőrizze az e cikk követelményeinek való megfelelést.

4.3.4. Az érintett tájékoztatása az adatvédelmi incidensről

A 34. cikk (1) bekezdése szerint, ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül, világosan és közérthetően tájékoztatja az érintettet az adatvédelmi incidensről. A 34. cikk (3) bekezdése alapján az érintettet nem kell az (1) bekezdésben említettek szerint tájékoztatni, ha a következő feltételek bármelyike teljesül:

- a) az adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták;
- b) az adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett, az (1) bekezdésben említett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;
- c) a tájékoztatás aránytalan erőfeszítést tenne szükségessé.

4.3.5. Az elektronikus hírközlési adatvédelmi rendelet-javaslat⁹⁷

A 2002/58/EK irányelvet azért kell felváltani újabb szabályozással, mert megjelentek olyan elektronikus hírközlési szolgáltatások, amelyek fogyasztói szempontból kiváltják ugyan a hagyományos szolgáltatásokat, de nem kell megfelelniük az azokra vonatkozó szabályoknak.⁹⁸ Ezért a Javaslat kiterjedne az internetes hangtovábbítási, üzenetküldési és weblapú e-mail-szolgáltatásokra, WIFI-re és a dolgok internetére.⁹⁹

96 A biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi. GDPR rendelet 4. cikk 12. pont.

97 A Bizottság javaslata az elektronikus hírközlés során a magánélet tiszteletben tartásáról és a személyes adatok védelméről, valamint a 2002/58/EK irányelv hatályon kívül helyezéséről (elektronikus hírközlési adatvédelmi rendelet).

98 Uo., 6. preambulumbekkezdés.

99 Uo., 11. és 12. preambulumbekkezdések.

A Javaslát szerint nem lenne alkalmazható a bűncselekmények megelőzése, kivizsgálása, felderítése, büntetőeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett tevékenységekre, ideértve a közbiztonságot fenyegető veszélyekkel szembeni védelmet és e veszélyek megelőzését.¹⁰⁰

A Javaslát konkretizálja az Európai Unió Alapjogi Chartája 7. cikkének érvényesülését (amely védi a polgárok magán- és családi életének, otthonának és kommunikációjának tiszteletben tartásához fűződő alapvető jogát) az elektronikus hírközlési ágazatban.¹⁰¹ A Javaslát kiegészíti a GDPR-t egyfelől, mert nem csak természetes személyek, hanem a jogi személyek adatainak védelméről is gondoskodik, mert az elektronikus hírközlési adatok jogi személyekkel kapcsolatos adatokat, például üzleti titkokat és egyéb, gazdasági értékkel bíró, bizalmas információkat is tartalmazhatnak.¹⁰² A Javaslát továbbá kiegészíti a GDPR-t abban az értelemben is, hogy a személyes adatnak minősülő elektronikus hírközlési adatok kezelésére vonatkozik.¹⁰³ Az elektronikus hírközlési adatok a Javaslát szerint magukba foglalják az elektronikus hírközlés tartalmát (elektronikus hírközlési szolgáltatások útján küldött vagy fogadott tartalom, például szöveg, beszéd, videók, képek és hang) és elektronikus hírközlési metaadatokat (az elektronikus hírközlés tartalmának továbbítása céljából, elektronikus hírközlő hálózatban kezelt adatok; idetartoznak a kommunikáció feladójának és címzettjének nyomon követésére és azonosítására szolgáló adatok, a kommunikáció dátuma, időpontja, időtartama és típusa).¹⁰⁴

A Javaslát rögzíti, hogy az elektronikus hírközlési adatok titkosak. A végfelhasználókon kívüli személyeknek tilos az elektronikus hírközlési adatokhoz bármilyen módon hozzáférni.¹⁰⁵

A Javaslát megengedi a jogosultak hozzájárulása esetén a metaadatok tárolását, de ezzel összefüggésben adatvédelmi hatásvizsgálat elvégzésének szükségessége merülhet fel a GDPR 35-36. cikkeinek megfelelően, ha az adatkezelés valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve.¹⁰⁶ A hírközlés tartalmának bizalmas jellege miatt vélelem szól amellett, hogy a felhasználó hozzájárulásával végzett e-mail szűrés bizonyos előre meghatározott tartalmak eltávolítása céljából, nagy kockázattal jár a természetes személyek jogaira és szabadságaira nézve.¹⁰⁷

A Javaslát 8. cikke szerint a végberendezések adatkezelési és -tárolási kapacitásainak használata és a végfelhasználók végberendezéseiről való – egyebek mellett a végberendezés szoftvereivel és hardverével kapcsolatos – adatgyűjtés az érintett végfelhasználón kívül mindenki számára tilos, kivéve, ha az alábbi okok valamelyike indokolja:

- a) kizárólag az elektronikus kommunikáció elektronikus hírközlő hálózaton keresztüli továbbításához szükséges; vagy
- b) a végfelhasználó a hozzájárulását adta; vagy
- c) a végfelhasználó által igényelt, információs társadalommal összefüggő szolgáltatás nyújtásához szükséges; vagy

100 Uo., 2. cikk (2) bekezdés d) pont.

101 Uo., Indokolás 1.1. pontja.

102 Uo., 3. preambulumbekkezdés.

103 Uo., 5. preambulumbekkezdés.

104 Uo., 2. cikk (1) bekezdése és 4. cikk (3) bekezdés a)-c) pontok.

105 Uo., 5. cikk.

106 Uo., 19. preambulumbekkezdés.

107 Uo., 17. preambulumbekkezdés.

d) online közönségméréshez szükséges, amennyiben a mérést a végfelhasználó által igényelt, információs társadalommal összefüggő szolgáltatást nyújtó szolgáltató végzi.

A másik eszközhez vagy hálózati berendezéshez való kapcsolódás lehetővé tétele céljából a végberendezés által kibocsátott adatokat tilos gyűjteni, kivéve, ha:

- a) ez kizárólag a kapcsolat létesítése érdekében, az ahhoz szükséges ideig és annak a céljából történik; vagy
- b) egyértelmű és jól látható értesítés jelenik meg, amely legalább az adatgyűjtés módjairól, céljáról, az adatgyűjtésért felelős személyről, valamint a végberendezés végfelhasználója által az adatgyűjtés beszüntetése vagy minimalizálása érdekében tehető intézkedésekről tájékoztat.

Az ilyen adatok gyűjtésének feltétele, hogy a GDPR rendelet 32. cikkében foglaltak szerint, a megfelelő technikai és szervezési intézkedések alkalmazásával garantálják a kockázatok mértékének megfelelő szintű adatbiztonságot.

A Javaslat 17. cikke szerint a hálózatok és az elektronikus hírközlési szolgáltatások biztonságát esetlegesen veszélyeztető konkrét kockázat felmerülése esetén, az elektronikus hírközlési szolgáltatást nyújtó szolgáltatónak értesítenie kell a végfelhasználókat erről a kockázatról, és amennyiben a kockázat a szolgáltató által végrehajtandó intézkedések alkalmazási körén kívül esik, tájékoztatnia kell a végfelhasználókat a jogorvoslati lehetőségekről, a várható költségeket is jelezve. A végfelhasználóknak a különös biztonsági kockázatokról való tájékoztatására vonatkozó követelmény nem mentesíti a szolgáltatót azon kötelezettség alól, hogy saját költségén megfelelő és azonnali intézkedéseket tegyen minden új, előre nem látott biztonsági kockázat elhárítása és a szolgáltatás szokásos biztonsági szintjének helyreállítása végett.¹⁰⁸ Az elektronikus hírközlési szolgáltatást nyújtó szolgáltatóknak tájékoztatniuk kell a végfelhasználókat arról, hogy milyen intézkedéseket hozhatnak kommunikációjuk biztonságának megőrzése érdekében, ilyen például bizonyos szoftverfajták vagy titkosítási technológiák használata.¹⁰⁹ A végfelhasználókat díjmentesen kell tájékoztatni a biztonsági kockázatokról. A biztonságot az (EU) 2016/679 rendelet 32. cikke alapján kell értékelni.

5. Összegzés

Az élet egyre több dimenziójának (politikai, kulturális, gazdasági, személyes) digitális térbe helyeződése (a kibertér kialakulása) tény, amelynek pozitív hatásai csak annyiban tudnak megnyilvánulni, amennyiben az ott tárolt, közvetített adatokkal nem történik visszaélés (pl. lehallgatás, adatlopás, rombolás), illetve azok védve vannak a véltlen károsodástól is.

Másként, az online tér jólétet eredményező továbbfejlődése a felhasználók bizalmától függ. A bizalom fenntartása pedig igényli a biztonságot. A biztonság jellemzően eljárási, módszertani kérdés. Különösen is akkor, ha elfogadjuk, hogy nem létezik tökéletes biztonság az informatikai rendszerek esetében sem. Ekkor felértékelődik a kockázat csökkentése és annak előzetes felmérése. A HIR biztonság-szabályozása lényegében a hálózatok működésének (integritásába, külső behatástól mentességébe) *biztonságába vetett bizalmat veszélyeztető kockázatok mérséklésnek eljárásrendjét jelenti*. A HIR biztonságára három egymást kiegészítő

¹⁰⁸ Uo., 37. preambulumbekzdés.

¹⁰⁹ Uo.

szabályrendszer vonatkozik: adatvédelmi, továbbá a bűncselekményi tilalmak mellett, maguknak a hálózati vagy információs rendszerek ellenállási képességének a fejlesztésére vonatkozó előírások. Ez utóbbi a szűken vett HIR biztonság szabályozás, amelynek célja a véletlen vagy rosszindulatú műveletekkel szembeni védelem.

A HIR ellenálló képességére vonatkozó szabályozás jellemzője, hogy miután a fenyegetések és veszélyek nem küszöbölhetőek ki teljes mértékig, továbbá nem rendelkezünk megfelelő elrettentő mechanizmussal (a szándékolt támadások például gyorsak, nehezen észrevehetőek és az elkövetők felderítése a technikai és globális jellege miatt nehézségekbe ütközik), ezért a szabályozás eszközrendszerében a jelzési mechanizmus, a megelőzés, az együttműködés, a legjobb gyakorlatok cseréje szerepel. Miután a fenyegetések is globálisak, ezért a fellépés is hatékonyabb lehet a nemzetinél magasabb szinten, amely az EU-ban EU szintű szabályozás létrehozását indokolta.

A felhőszolgáltatások egyes jogi kérdései – különös tekintettel az Európai Unió szabályozására*

KLEIN TAMÁS

1. Prolóógus

Amikor napjaink legforróbb technológiai jogi szabályozási kérdései fölött tartunk szemlét, kétségkívül az egyik legizgalmasabb témaként tekinthetünk a felhőszolgáltatások jelentette jogalkotói és jogalkalmazói kihívások sorára. A technicizált, információs társadalmak polgárai nap mint nap használnak olyan eszközöket, részt vesznek olyan (pénzügyi) műveletekben, amelyek során a polgárokhöz köthető adatok egy része, vagy egésze egy távoli, fizikailag nem meghatározott tárhelyen kerül tárolásra. Okos eszközeink használata során rendszerint a 'felhőbe' tároljuk adatainkat, a rendelkezésünkre álló információink egy részét.¹

A jogi szabályozás számára a felhőalapú szolgáltatások és a használatuk során keletkező jogviszonyok, felelősségi viszonyok rendkívül komplex jelenséggé azonosíthatók, hiszen a *prima facie* jól érzékelhető adatvédelmi jogi kihívások mellett, szerzői jogi, elektronikus kereskedelmi jogi, kötelmi jogi kérdések sorát veti fel. A magunk részéről jelen tanulmányban nem térünk ki valamennyi aspektusra, vizsgálódásunk fókuszpontját egyes adatvédelmi jogi, felelősségtani és elektronikus kereskedelmi jogi összefüggésekre szeretnénk irányítani, hiszen választott perspektívánk az infokommunikációs jog és információtechnológia nézőpontjára esett. A felhőszolgáltatások szerzői jogi kérdéseivel nem foglalkozunk, az ilyen összefüggésekről az elmúlt esztendőben kiváló, gondolatébresztő írások születtek.²

A felhőalapú informatikai szolgáltatások (angol nyelvű dokumentumokban: *cloud computing*, magyar nyelvű fordításokban: számítási felhő, e tanulmányban mi felhőszolgáltatásként, vagy felhőalapú szolgáltatásként használjuk) által használt informatikai megoldás ugyan nem tekinthető kifejezetten új technológiának, ám az utóbbi esztendőben a technológiavezérelt infokommunikációs szektorokban rendkívül széles körben váltak alkalmazottá. Napjainkban minden meghatározó internetszolgáltató alkalmaz valamilyen felhőalapú informatikai eljárást/megoldást, és egyöntetűen kiemelt figyelmet fordítanak saját felhőszol-

* A szerző köszönetet mond Szabó Endre Győzőnek, a Nemzeti Adatvédelmi- és Információhatóság elnökhelyettesének a tanulmány megszületéséhez nyújtott szakértő megjegyzéseiért és kritikáiért, valamint Bartha Bencének, a KRE ÁJK joghallgatójának a tanulmány elkészítésében nyújtott közreműködéséért.

1 Az okos eszközök és a felhő alapú informatikai megoldások mindazonáltal egymást feltételező technológiai fejlemények, hiszen míg a nagy teljesítményű okostelefonok és táblagépek elterjedésének egyik fontos előfeltétele volt a hardveren kívüli adattárolás hatékony módjának megteremtése, addig a felhő-informatika gyors fejlődése is serkentően hat a multimédiás eszközök újabb és újabb generációinak intenzíven növekvő tárhely igénye.

2 A szerzői jogi kérdésekről I. GRAD-GYENGE Anikó – FALUDI Gábor: A cloud computing-alapú szolgáltatások szerzői jogi megítéléséről. *Infokommunikáció és Jog*, 2012/3. 105-108. GRAD-GYENGE Anikó: A modern technológiák szerzői jogi és iparjogvédelmi kihívásai - különös tekintettel a fájlcsere, a felhő-programozásra és a 3D nyomtatókra: File-sharing, cloud computing and 3D printing - actual technological challenges in the field of copyright. In: TÓTH András (szerk.): *Technológia jog*. Budapest, KRE ÁJK, 2016. 98-115. BARTKÓ Viktor: A felhőalapú szolgáltatások szerzői jogi megítélése – Magáncélú többszörözés a felhő tárhelyekben I-II. *Polgári Jog*, 2017/5-6.

gáltatásuk fejlesztésére technológiai stratégiáik kialakítása során. A felhőszolgáltatások tömegessé válása – amiként arra már utaltunk – élesen hozta felszínre a vele kapcsolatos jogi problémákat, a jogi szabályozás mikéntjét.

Az új technológiák szabályozási kihívásai kapcsán a szabályozási koncepciók megfogalmazása során, a konkrét jogi szabályozás fókuszában rendszerint annak a kérdésnek a megválaszolása áll, hogy a fejlődés pozitív hatásait a jognak a közérdek mentén (az innovációban rejlő társadalmi és egyéni előnyök biztosítása mellett) be kell-e csatornázni a társadalmi folyamatokba, vagy a nem várt és nem kívánt hatások, a társadalmi és/vagy egyéni károk bekövetkezését kell megakadályozni? A jognak ezért az új technológiák szabályozása során olyan egyensúlyt kell találnia, amely nem fojtja el a technológiai és az annak hatására remélt társadalmi fejlődést, egyúttal pedig biztosítja a kontrollt a sokszor előre nem pontosan azonosítható irányú folyamatok felett. Ez a dilemma a technológiaszabályozás időhorizontjának jelentőségére hívja fel a figyelmet, hiszen a technológia korai szakaszában való leszabályozása a technológia ismeretének hiányában korlátozó lehet, ha viszont megvárjuk, amíg egy adott technológia kibontakozik, elveszítethetjük felette a társadalmi kontrollt. Ezt a jelenséget *Collingridge dilemmaként* is emlegetik.³

Tóth András idézett munkájában emlékeztet arra, hogy szabályozás és a technológia gyakran egymás ellentéteinek tűnnek, hiszen sokak szemében a technológia a haladást, a szabályozás pedig éppen a haladás gátját, a bürokratizmust szimbolizálja. A szabályozásra gyakorta hivatkoznak úgy, mint a korlátok ésszerűtlen, önmagáért való világára, a technológiára pedig, mint a szabadság hírnökére. A technológiai fejlődésben érdekelték gyakran használják vádként azt az érvet, hogy amellett, hogy a társadalom érzéketlen bizonyos technológiai változásokra, a szabályozó indokolatlanul és túlzottan óvatos, amely viszont szükségszerűen akadályozza a technológiai fejlődést. Felmerül, hogy a jognak kell-e legyen egyáltalán szerepe a technológia haladásban?⁴

A felhőalapú szolgáltatások elterjedése mögött csakúgy, mint általánosan a technológiai változások háttérben is, mindig társadalmi folyamatok húzódnak meg. A társadalmi és a technológiai dinamikák pedig folyamatosan megtermékenyítően hatnak egymásra, hiszen amint a társadalmi igény nélkül nem lehet sikeres egy technológiai innováció, úgy a technológiai innováció is változásokat generálva (vissza)hat a társadalmi folyamatokra. Tóth András álláspontját osztva kijelenthető, hogy a technológia olyan iparágakra is innovációt gyakorolhat, amelyek hosszú ideje a stagnálás, vagy a lassú, de a korábbi technológiai alapon megújulni nem képes hanyatlás jeleit mutatják.⁵ Így hatott a felhőalapú szolgáltatások megjelenése is az informatikai iparra, ahol az adattárolási kapacitások műszaki megoldásai, a fizikai valóságukban a felhasználó birtokában lévő tárolókapacitások révén, elérték a korábbi műszaki szinten a határokat.

A jogi szabályozás felelőssége elsősorban az, hogy hidat képezzen a technológiai fejlődés hajtóerői és a társadalom között, biztosítsa az innovációban rejlő legnagyobb közjó kiaknázását, a nem kívánt hátrányok, társadalmi veszélyek kiküszöbölése mellett.

3 Vö. Tóth András: A technológia szabályozásának jogi kihívásai. In: Tóth András (szerk.): *Technológia jog*. Budapest, KRE ÁJK, 2016. 26-37.

4 Uo., 28-29.

5 Uo., 27.

2. A felhőszolgáltatások információtechnológiai alapjai

A felhőalapú informatikai megoldások az adatok távoli számítógépeken/szervereken történő tárolását, feldolgozását és felhasználását jelentik, amelyek egy hálózaton, általában (de nem kizárólagosan) az internet elektronikus hírközlési infrastruktúráján keresztül válnak hozzáférhetővé. A szolgáltatás így nem egy dedikált és a felhasználó számára fizikailag (térben) is azonosítható hardvereszközön érhető el, hanem azokat a szolgáltató közelebbről nem azonosított eszközein elosztva üzemelteti oly módon, hogy a szolgáltatás üzemeltetési részletei a felhasználó előtt rejtve maradnak.

2.1. A felhőszolgáltatások fogalmi meghatározhatósága

A felhőalapú számítástechnikai megoldások univerzális fogalmának a megadása több szempontból is korlátozottan lehetséges. Egyfelől azért, mert az elemzésünk tárgyaként választott technológia folyamatos fejlődésben van, egy fejlődésben lévő paradigma, másfelől pedig azért, mert a globális szolgáltatásra vonatkozóan, egységes nemzetközi terminológia sem került még elfogadásra. Különböző nemzetközi munkacsoportok különböző munkadokumentumai, jelentései foglalkoznak egy, a szolgáltatás valamennyi jellemzőjét leíró fogalom megalkotásával, több-kevesebb sikerrel. Mi a Nemzetközi Távközlési Adatvédelmi Munkacsoportnak a felhőalapú számítástechnika, a magánszféra és az adatok védelmének kérdései című munkadokumentumában is elfogadott,⁶ az amerikai Nemzeti Szabványügyi és Technológiai Intézet (a továbbiakban: NIST) által kidolgozott definíciót vesszük alapul. Ennek alapján:

„A felhőalapú számítástechnika egy olyan modell, amely széleskörű, kényelmes, igény szerint rendelkezésre álló hálózati hozzáférést kínál konfigurálható számítástechnikai erőforrásokhoz (pl. hálózatokhoz, szerverekhez, tárházhoz, alkalmazásokhoz és szolgáltatásokhoz), amelyek gyorsan és minimális kezelési ráfordítással és minimális, a szolgáltatóval folytatott interakcióval igénybe vehetők, és nyilvánosan rendelkezésre állhatnak. Ez a felhőmodell öt lényeges tulajdonságot tartalmaz, három szolgáltatási és négy felhasználási modellt.”⁷

A NIST definíciója a felhőalapú számítástechnika fontos jellemzőit írja le, és – mint az általános fogalmi elemek hordozója – az egyes felhőszolgáltatások széles körű összehasonlításának eszköze kíván lenni. Amint azt a NIST dokumentuma is rögzíti a NIST-definíció kiindulópontot kíván nyújtani a felhőalapú számítástechnikáról folytatott tudományos diskurzu-

6 International Working Group on Data Protection in Telecommunications: Working Paper on Cloud Computing – Privacy and data protection issues – Sopot Memorandum. 2012. (a továbbiakban: Sopot Memorandum), https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=3065.

7 „Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.” I. National Institute of Standards and Technology, Special Publication 800-145, The NIST Definition of cloud computing (a továbbiakban: NIST Special Publication), <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>.

sokhoz és a felhőalapú számítástechnika legjobb használatának kialakításához. A definiált szolgáltatási- és telepítési modellek egyszerű taxonómiai rendszert alkotnak, a fogalom nem szándékozik előírni vagy korlátozni semmilyen konkrét telepítési, szolgáltatásnyújtási vagy üzleti tevékenységet.⁸

Napjainkban magánszemélyek és vállalkozások, sőt még közigazgatási tevékenységet ellátó szervek is használják a számítási felhőszolgáltatásokat, sok esetben anélkül, hogy tudatában lennének az igénybe vett szolgáltatás természetével, az előnyökkel és hátrányokkal. Az információs társadalommal összefüggő, elektronikus hírközlési szolgáltatások jelentős része is felhőalapú technológiára épül, úgy, mint az e-mail szolgáltatások, vagy éppen a közösségi hálók, amelyek használata a társadalomban rendkívül magas arányú.

A felhőszolgáltatásokat a felhasználók különböző célra, tudatossággal, intenzitással és eredményességgel hasznosítják. A magánszemélyek a mindennapi magánérintkezéseik, magánszférájukat érintő kommunikációjuk során a legkülönbözőbb célra használják a felhőket, elektronikus levelezésüket, vagy éppen családi emlékeiket, fotóikat tárolják egy távoli eszközön található tárhelyen. Az információs technológia professzionális felhasználói számára, akik (elsősorban) üzleti célra használják a felhőalapú számítástechnikai megoldásokat, a felhőszolgáltatások nagyfokú rugalmasságot biztosítanak a munkájukhoz szükséges számítási teljesítmény nagyságát illetően. A lokálisan telepíthető tárolókapacitásokhoz képest a felhőben eszközölt tárolás nagyfokú flexibilitása mellett, gazdaságilag is rentábilisabb megoldásnak látszik.

2.2. A felhőalapú szolgáltatások működési elve

A felhőalapú számítástechnika technikai alapja egy jól kifejlesztett hálózati technológia és 'szervervirtualizálás.' Ez a technológia megteremti a lehetőséget az adatok és az adatfeldolgozás dinamikus áttelepítésének a mindenkorai számítóközpont szerverei között mind lokálisan, mind pedig globálisan a tipikusan világszerte működő számítóközpontok szerverei között. A technológia a hagyományos adatfeldolgozási-tárolási technológiákhoz képest, rendkívül könnyen méretezhető anélkül, hogy az korlátozó szűk keresztmetszeteket hozna létre. Az internetes hálózat közbejöttével a szolgáltató biztosítja, hogy a végfelhasználó a számítóközpont telephelyétől függetlenül hozzáférjen az adatokhoz.⁹

A felhőalapú szolgáltatások felhasználói egy, erre a célra kifejlesztett szoftver segítségével számítógépüket a számítási felhő platformjához csatlakoztatják. A számítási felhő feldolgozókapacitásáról egy, szerverek és adattároló rendszerek százait magába tömörítő, hatalmas adatközpont gondoskodik. Ezek az informatikai rendszerek gyakorlatilag képesek kezelni valamennyi, az ügyfelek által potenciálisan használható szoftvert.

A szolgáltatások sok esetben ingyenesek (például a webmail ajánlatok), de az ügyfelek többsége a nagyobb kapacitásokat rugalmas, használatarányos díjszabás keretében, vagy egy-egy havi díj megfizetése mellett veheti igénybe.¹⁰

8 Vö. NIST Special Publication i.m. (7. lj.) Purpose and Scope.

9 Vö. Sopot Memorandum i. m. (6. lj.) 31. pont.

10 A számítási felhőben rejlő potenciál felszabadítása Európában – mi is jelent ez pontosan és milyen módon érint bennünket? http://europa.eu/rapid/press-release_MEMO-12-713_hu.htm.

De az ingyenesség még akkor is, ha a szolgáltatás igénybevétele tényleges előfizetési díj fizetéssel nem jár, többnyire csupán látszólagos. A legtöbb ingyenes szolgáltatás esetén ugyanis a felhasználónak el kell fogadnia, hogy egyfelől a szolgáltató a felhasználói felületén reklámokat helyez el (tulajdonképpen a szolgáltatónak ez a tevékenység eredményezi a gazdasági hasznot), másfelől pedig csupán egy limitált mennyiségű adat tárolására alkalmas méretű tárhelyet biztosít. Az előfizetési díj ellenében igénybe vett szolgáltatások ezzel szemben a díjjal arányos méretű tárolókapacitást és reklámmentes felületet biztosítanak. Mindazonáltal azt már itt hangsúlyozni szükséges, hogy az ingyenesen, illetőleg díj ellenében igénybe vett szolgáltatások között kizárólag a felhasználói felület kereskedelmi kommunikációs közegként való használatában és a tárolókapacitás méretében lehet különbség, a később részletesen bemutatott adatvédelmi követelmények, vagy éppen a felelősségi szint nem tehető függővé a szolgáltatás ingyenes vagy visszerthes voltától.

A felhőszolgáltatások működési struktúrájából következik a NIST által kidolgozott fogalomban hivatkozott, öt lényeges tulajdonság.

- 1) Igény szerinti önkiszolgálás (*On-demand self-service*): A felhasználó (pillanatnyi) tárolási szükséglete szerint igényelhet tárolási kapacitást. Az így igényelt és rendelkezésre bocsátott tárhelyhez bármikor hozzáférhet, a szolgáltató bármilyen közrehatása nélkül.
- 2) Széleskörű hálózati hozzáférés (*Broad network access*): A tárolási kapacitások hálózaton keresztül érhetők el, és szabványos informatikai eszközök széles körével hozzáférhetők.
- 3) Erőforrások összevonása (*Resource pooling*): A felhőszolgáltató erőforrásait koncentrálja, annak érdekében, hogy több felhasználó részére, a felhasználói igények messzemenő figyelembevételével diverzifikálja.
- 4) Teljes flexibilitás (*Rapid elasticity*): A koncentrált erőforrások felhasználók részére történő diverzifikálását a rendkívüli rugalmasság, igényekhez való alkalmazkodás jellemzi, vagyis, hogy azok kiosztása, megosztása az egyes felhasználók között, mindig azok igényeihez igazodik, és újra-újra felosztásra kerül.
- 5) Mért szolgáltatás (*Measured service*): A felhőszolgáltatások automatikusan ellenőrzik és optimalizálják az erőforrásaik felhasználását. Mivel az erőforrás felhasználása matematikailag mérhető, így folyamatosan biztosítható a szolgáltatás zavarmentes szervezése, és átláthatósága, mind a szolgáltató, mind pedig a felhasználó vonatkozásában.¹¹

2.3. A 'felhő földrajz' – az adattárolás helye

A virtuális adattárolás helye, a felhő a földgolyón valahol, egy közelebből meg nem határozott adatközpont erőforrásainak használatával működik, vagyis a szolgáltatást nem egy (lokálisan) dedikált hardvereszközön üzemeltetik, hanem a felhőszolgáltató rendelkezésére álló, akár különböző földrajzi helyeken telepített eszközein diverzifikálva működtetik. Az adatkezelés tehát sokkal dinamikusabban történik, mint korábban. Az adatfeldolgozás helye, aktuális helyszíne, számos külső tényezőtől függ. Az egyes adattárolási kapacitások telepítésének szempontjai között szerepel példának okáért a villamosenergia ára, az időjárási viszonyok megfelelősége, a különböző időzónák előnyei. Az adattárolás pillanatnyi, aktuális helye, a több helyszínrre telepített szerverek közötti diverzifikáció, többnyire olyan körülményekre, esetenként nem várt

11 Vö. NIST Special Publication i.m. (7. l.) Characteristics, 2.

eseményekre is visszavezethető, mint egy szerver váratlan leállása, meghibásodása, csúcsterhelés esetén egy adott szerver kapacitásának telítődése (túlsordulása). Ilyen esetekben az adatokat szükség szerint egy másik, rendelkezésre álló adatközpontba kell továbbítani.

Az informatikai tárolókapacitás földrajzi elhelyezkedése, a szerverek állami szuverenitás által meghatározott helye jogi relevanciával rendelkezik, hiszen főszabályként annak az országnak a joga irányadó a felhőszolgáltató működésére, amelynek a területén ténylegesen található. A jogi védelem azonban az egyes országok (adatvédelmi vagy éppen szerzői jogi) jogszabályaiban és joggyakorlatában jelentékeny különbséget mutathat, ezért a felhőben tárolt tartalmak tényleges földrajzilag azonosítható tárolási helye nagyban meghatározhatja a szolgáltatás igénybevevőjének jogi helyzetét. Előfordulhat például, hogy a felhasználó személyes adatai egy megfelelő jogvédelmet nem biztosító állam területén telepített szerverre kerülnek, ahol az enyhébb védelmi szintet, a garanciák hiányát kihasználva azokkal visszaélhetnek.

A különböző védelmi szintből fakadó, visszaélésszerű ország választás megelőzése érdekében szükséges megoldás lehet egy minimális védelmi szint meghatározása, vagy annak a kimondása, hogy nem továbbíthatók adatok olyan országba, ahol nem biztosított a jogvédelem azonos szintje. Ez utóbbi megoldást követi például az Európai Unió adatbiztonsági irányelve, amely a személyes adatok megfelelő szintű védelme érdekében előírja, hogy adatokat vagy az Európai Gazdasági Térségen (EGK) belül, vagy egy olyan területen kell tárolni, ahol az EGK adatvédelmi jogszabályaival egyenértékű jogszabályokat alkalmaznak. Erről az adatvédelmi jogi fejezetben részletesen szólunk.

A szolgáltató letelepedésének és az adattárolás tényleges megvalósulásának helye tehát azért bír kiemelt jelentőséggel, mert ez határozza meg a konkrét jogviszony tekintetében azokra az alapvető, jogilag releváns kérdésekre adható konkrét jogi válaszokat, amelyeket a felhőalapú szolgáltatások alkalmazása általában felvet. A felhőszolgáltatások igénybevétele során elsősorban adatvédelmi, adatbiztonsági, szerzői jogi, valamint az elektronikus kereskedelmi jogi kérdéseket szükséges vizsgálni.

2.4. A felhőszolgáltatások legfontosabb előnyei a felhasználók számára

- 1) A felhőszolgáltatások egyik leginkább érzékelhető előnye, hogy a felhasználók számára megszűnik a kapacitásszűkösség korábbi évtizedekben megtapasztalt problémája, tekintve, hogy az adattárolásuk nem az általuk megvásárolt és működtetett szervereken és adattároló berendezéseken történik. A felhasználó a felhőszolgáltatás útján megvalósított adattárolás során kizárólag tárhelyet (tárhelyszolgáltatást) vásárol. Ez jelentékeny erőforrás megtakarítással jár, hiszen ugyan a felhőszolgáltatás igénybevételéért egy adattárolási volumen felett szerződésben kikötött díjat kell fizetni, de meg lehet spórolni a saját eszközök beszerzésével, fenntartásával, karbantartásával együtt járó költségeket (eszközvásárlás, épület, informatikai személyzetet alkalmazása stb.). A tárolókapacitás fenntartását, üzemeltetését a felhasználó helyett a szolgáltató vállalja magára.
- 2) A felhasználók számára a felhő továbbá csaknem teljes rugalmasságot biztosít az igénybe vett tárhely és eszközök tekintetében.

A felhőtárhely tehát a felhasználó számára nagyon könnyen létrehozható, ezzel szemben a szolgáltató szempontjából rendkívül komplex tevékenységet feltételez, amely magában foglalja a folyamatos, és változó intenzitású kapacitásépítést, kapacitásmenedzsmentet és általános irá-

nyítási tevékenységet követel meg. Mindez pedig kimagaslóan erőforrás-igényes tevékenységgé teszi a felhőszolgáltatást. Ez a primer forrásigény (hatalmas belépési költség) nagyban emlékeztet a hálózatos iparágak közgazdasági törvényszerűségére, azzal azonban, hogy a szolgáltatás fenntartása némiképp magasabb konstans költségekkel kalkulálható, mint a hagyományos hálózatos szektorokban. Ez a közgazdasági determináció hatással van az iparág egészére.

A felhőalapú számítástechnika minden internet felhasználó számára komoly előnyökkel jár, és számos területen forradalmi változásokat hozhat.

A felmérések eredményei szerint a számítási felhőt használó vállalkozások 80%-ánál tapasztalható az IT-költségek mintegy 10–20%-os csökkenése, míg 20%-uk esetében annak alkalmazása 30%-os és afeletti megtakarítást eredményezett.

Sok fogyasztó már rendszeres felhasználója a számítási felhő alapszintű szolgáltatásainak (többek között az internetalapú e-mail fiókok használata okán). Költségmentesen vagy minimális összegű ellenszolgáltatás fejében igénybe vehető óriási tárhely, kényelmesen és bárhol elérhető hozzáférés, kevesebb kiadás – hogy csak néhányat említsünk a számítási felhő kínálta előnyök közül. Magasabb integrációs szintű, hatékony és kisebb költségráfordítás mellett biztosítható szolgáltatások lehetővé tétele révén, a számítási felhő alkalmazása a közzsféra számára is igen hasznosnak bizonyulhat.

A felhőalapú szolgáltatások serkentően hathatnak a tudományos haladásra, elsősorban a kutatásokra, hiszen az egyes kutatóhelyek, tanszékek, kutatóintézetek a belső, célorientált számítógépes infrastruktúrájukban rejlő potenciált ki tudják egészíteni, bizonyos vonatkozásokban tehermentesíteni (az olyan műveletek esetében, amelyeknél nem szükséges a tudományos kutatási célra kifejlesztett speciális informatikai elemzés) is tudják a felhőalapú szolgáltatást nyújtó szolgáltatókéval, ennek köszönhetően pedig hatalmas mennyiségű adatot képesek tárolni, minek következtében azok feldolgozása is lényegesen gyorsabb válhat. Az IT-termékekre és szolgáltatásokra vonatkozó legújabb ötleteket sokkal egyszerűbben és olcsóbban lehetne kipróbálni, ez pedig ösztönzőleg hatna az innovációra is.

2.5. A felhőszolgáltatások és az IKT-szektor fejlődési lehetősége

Különböző európai kutatások készültek az elmúlt években a felhőszolgáltatások gazdasági hatásaival kapcsolatban,¹² amelyek közös tézise szerint, amennyiben a belső piacon elhárulnának a napjainkban fennálló, a szolgáltatás elterjedését gátló akadályok (ezek egy része szabályozás útján lenne kiküszöbölhető), az iparág szükségszerűen nyereséges lehetne.

Az európai vállalati szektor fejlődési és a felhőszolgáltatásokban rejlő potenciált összeolvasó elemzések szerint, az EU-s vállalatok több mint 98%-a kezdené meg vagy bővítené az olyan szolgáltatásait, alkalmazásait, amelyek felhőalapú informatikai megoldásokon alapulnak. A felhőszolgáltatások intenzív használata új felhasználókat vonzana, a szolgáltatást

12 Pl. A számítási felhőben rejlő potenciál felszabadítása Európában, A Bizottság Közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának, Brüsszel, 2012.9.27. COM (2012) 529 final,

www.eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52012DC0529&from=HU vagy az IDC jövőkutatása A számítási felhő iránti európai igénnyel kapcsolatos mennyiségi becslések Európában és az esetlegesen felszámolandó akadályok (Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Take-up), www.cordis.europa.eu/fp7/ict/ssai/docs/study45-d2-interim-report.pdf.

napjainkban még nem használó, de azt el nem utasító uniós vállalkozások 96%-a kezdene ilyen irányú beruházásokat.

Megnőne az IT-ismeretek iránti igény, nem kizárólag olyan alapvető területeken, mint például az adatközpontok irányítása, hanem a digitális marketing, a webes alkalmazástervezés, a közösségi hálók, a pénzügyi szolgáltatások és stabilitás tekintetében is.

2.6. A felhőszolgáltatási modellek tipológiája

2.6.1. Szolgáltatási modellek

A felhőalapú szolgáltatások fő szolgáltatásnyújtási modelljei:

Annak megfelelően, hogy milyen felhasználói igények jelentkeznek, felhőszolgáltatással kapcsolatban több felhőalapú számítástechnikai megoldás is elérhető. Ezek a különböző felhasználói igényeket kielégítő informatikai konstrukciók három szolgáltatási modellben csoportosíthatóak.

- 1) A szoftver szolgáltatás (*Software as a Service*) olyan felhőszolgáltatás, ahol a szoftver maga a szolgáltatás. Az ilyen felhőalkalmazásokat többnyire egy *http protokollon* keresztül, egy böngészőprogram segítségével lehet használni, a felhasználói programon a felhasználó csupán minimális változtatást tud/képes eszközölni. A szolgáltató az interneten keresztül különféle alkalmazási szolgáltatásokat nyújt, és a végfelhasználók rendelkezésére bocsátja azokat. E szolgáltatások gyakran a felhasználók helyi rendszerére telepítendő hagyományos alkalmazások helyettesítésére szolgálnak; ennek megfelelően a felhasználók feltehetően végső soron kiszervezik az adataikat az egyedi szolgáltató számára. Erre a típusú felhőszolgáltatásra példaként említhetők a *Google Docs*, és az *Oracle Netsuite* szolgáltatása.
- 2) A platform szolgáltatás (*Platform as a Service*) az alkalmazás üzemeltetéséhez szükséges környezetet biztosítja, terheléelosztással és feladatátvétellel, kezelő felülettel, valamint ezek rendszeres biztonsági frissítésével. Itt a platform (operációs rendszer), mint környezet is része a szolgáltatásnak. A szolgáltató biztosítja a platformot és az eszközöket, a felhasználónak pedig a szoftver szolgáltatáshoz képest szabadabb keze van, kiválaszthatja és ellenőrizheti az alkalmazásokat és a tárhelyet is. A szolgáltató az alkalmazások továbbfejlesztésére és üzemeltetésére vonatkozó megoldásokat kínál. E szolgáltatásokat általában azoknak a piaci szereplőknek nyújtják, akik olyan saját alkalmazáson alapuló megoldások fejlesztésére és üzemeltetésére használják a szolgáltatott felhőt, amelyek célja a vállalaton belüli igények kielégítése és/vagy harmadik felek számára történő szolgáltatásnyújtás. A *PaaS* szolgáltató által biztosított szolgáltatások szintén szükségtelenné teszik, hogy a felhasználó a további és/vagy különleges vállalaton belüli hardvert vagy szoftvert vegyen igénybe. A platform alapú szolgáltatások elvén működik a *Google App Engine*, vagy éppen az *OpenShift*.
- 3) Infrastruktúra szolgáltatás (*Infrastructure as a Service*): Bizonyos esetekben a felhő infrastruktúra rendelkezésre bocsátása a szolgáltatás. Az infrastruktúra üzemeltetője virtuális hardvert (szervert, blokk-tárhelyet, hálózati kapcsolatot, számítási kapacitást) szolgáltat,

ennek keretében működteti és ellenőrzi a felhő infrastruktúráját, míg a fogyasztó választja ki a platformot, a hálózati elemeket, de ez a joga a tárolás és az alkalmazások tekintetében is fennáll. A szolgáltató haszonbérbe adja a technológiai infrastruktúrát, vagyis a virtuális távoli kiszolgálóegységeket, amelyeket a végfelhasználó bizonyos mechanizmusoknak és szabályoknak megfelelően úgy vehet igénybe, hogy egyszerűen, hatékonyan és hasznosan helyettesítheti a vállalat telephelyein meglévő vállalati IT-rendszereket, és/vagy a bérelt infrastruktúrának a vállalati rendszerek melletti használatát.¹³ A szolgáltatások infrastruktúra szolgáltatáson alapuló modelljére lehet jó példa az *Amazon EC2* és a *Google Compute Engine* felhőszolgáltatás.¹⁴

2.6.2. Hozzáférhetőség szempontú csoportosítás

A hozzáférhetőség alapján megkülönböztetünk publikus, privát, hibrid, közösségi felhőt.

- 1) A publikus/bárki által igénybe vehető/osztott felhő esetén egy szolgáltató a saját eszközlományával (tárhely, hálózat segítségével) szolgálja ki a felhasználók szerverigényeit, tehát a szolgáltatási infrastruktúra a szolgáltató tulajdonában áll. Publikus felhők esetén különös jelentősége van a különböző ügyfelek izolálásának. A felhőtárhely tartalma heterogén és egy piaci elvű szolgáltatást nyújtó szolgáltató rendelkezik felette. Az osztott felhő esetén a szolgáltató az egyes felhasználók, hozzáférésre jogosultak számára egy dedikált hozzáférést (*locker*) biztosít. A szolgáltatások internethálózaton keresztül hozzáférhetők, aminek következtében az adatfeldolgozási műveletek és/vagy a felhasználói adatok átkerülnek a szolgáltató rendszereibe. Ebből fakadóan a szolgáltató központi szerepet játszik a rendszereire bízott adatok hatékony védelme tekintetében. Az ilyen adatkezeléssel járó felhőszolgáltatás során a szolgáltató felelőssége sem megkerülhető. A felhasználó az adatok mellett az azok feletti ellenőrzés legnagyobb részét is köteles átadni.¹⁵
- 2) Privát felhő esetében saját vagy bérelt erőforrások felhasználásával, azok informatikai alapjain lehet saját felhőt is építeni. A saját felhő egy olyan IT-infrastruktúra, amelyet kizárólag egy konkrét, arra jogosult személy, vagy szervezet használ, és aki ahhoz egyedileg fér hozzá. A saját felhő a jogosult valamilyen, tipikusan üzleti tevékenységének az informatikai támogatására szolgál. Ez megoldást jelent a publikus felhők problémáira, viszont az üzemeltetésről a privát felhő tulajdonosának kell gondoskodnia. Ez a modell a hagyományos adatközpontok működéséhez hasonlítható, *azzal a különbséggel, hogy az egyes technológiai eljárásokat úgy hajtják végre, hogy optimálisan kihasználják a rendelkezésre álló erőforrásokat, és az idővel lépésenként eszközölt kis beruházások révén, megerősíték azokat.*¹⁶ Példák privát felhő szoftverekre: *VMware vSphere*, *oVirt*, *CloudStack*, *OpenNebula*.

13 L. A személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló az Európai Parlament és a Tanács 95/46/EK irányelve 29-es cikke alapján létrehozott adatvédelmi munkacsoport 05/2012. számú véleménye a számítási felhőről (a továbbiakban: 29-es munkacsoport véleménye), www.eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52012DC0529&from=HU.

14 Vö. NIST Special Publication i.m. (7. l.) Service Models, 2-3.

15 29-es munkacsoport véleménye i.m. (14. l.).

16 Uo.

- 3) Hibrid felhő a privát és publikus felhők sajátságos kombinációja. Ez lehetővé teszi átmeneti teljesítmény igény esetén a számítási felhő kiegészítését publikus, a szolgáltató által kínált megoldással.
- 4) Közösségi felhőt a hasonló jogi szabályozás alá eső szervezetek hoznak létre, több szervezet, vagy személy osztozik a felhőn, és közösségi célok érdekében használják, közös alapelvek mentén.¹⁷

2.7. A felhőalapú technológia jogilag releváns sajátosságai:

- 1) A hardver (számítógépek, tárolókapacitások) nem a tárhelyet interneten keresztül elérő felhasználók, hanem a felhő szolgáltatójának tulajdona.
- 2) A hardvereszközök használata dinamikusan optimalizált hálózati környezetben történik, ezáltal a felhasználónak elvben és szigorúan technikai értelemben, nem szükségszerű az adatok és adatkezelés, adatfelhasználás pontos (földrajzi) helyével, illetve a felhasználót egy adott pillanatban ténylegesen kiszolgáló hardvert beazonosító információkkal foglalkoznia (mindazonáltal, ahogy arra a későbbiekben részletesen kitérünk, ennek a jogi szabályozás, a személyes adatok védelmét biztosító intézményi garanciák kapcsán kiemelt jelentősége lesz).
- 3) A felhőalapú szolgáltatást nyújtó szolgáltatók a rendelkezésre álló tárolási kapacitások használatának optimalizálása érdekében, gyakran helyezik át a felhasználói terheléseket, mozgatják az egyes, tárolt adatállományokat.
- 4) Az adatokat egy távoli hardver tárolja, dolgozza fel és teszi elérhetővé egy informatikai felületen, például egy alkalmazáson keresztül, amelynek következtében a vállalatok a felhőalapú számítási kapacitásaikat a webes levelező fiókokhoz hasonlóan használhatják.
- 5) A szervezetek és magánszemélyek tértől és időtől függetlenül, ott és akkor férhetnek hozzá tartalmaikhoz, bármilyen alkalmas (személyi számítógép, okoseszközök) eszközön futtathatják az adateléréshez szükséges szoftvereiket, ahol és amikor arra igényük van.
- 6) A felhőarchitektúra rétegekből áll: hardverből, köztes rétegből (*middleware*) vagy platformból, valamint alkalmazás szoftverekből. A szabványosítás különösen a köztes rétegnél fontos, mert ez teszi lehetővé a fejlesztők számára a lehetséges ügyfelek széles körének elérését, illetve kínál választási lehetőséget a felhasználók számára.
- 7) A felhasználók általában a használat arányában fizetnek a szolgáltatásért, ezáltal elkerülve az összetett saját számítási környezetek felállításához és működtetéséhez szükséges, nagy összegű kezdeti és fix költségeket.
- 8) A tárolókapacitás mennyiségi paraméterei rendkívül rugalmasan alakíthatók igazodva a mindenkori, aktuálisan felmerülő tárolási-kapacitási igényekhez. A felhasználók ugyanakkor nagyon egyszerűen (pl. néhány kattintással, másodpercek alatt további tárolókapacitást vehetnek igénybe) módosíthatják az általuk használt hardvereszközök mennyiségét.

17 Vö. NIST Special Publication i.m. (7. lj.) Deployment Models, 3.

2.8. A felhőszolgáltatás társadalmi és gazdasági haszna:

Az új technológiák akkor képesek tartósan a piaci versenyben és a társadalmi gyakorlatban fennmaradni, ha azoknak van gazdasági, s jó esetben társadalmi haszna is. A felhőszolgáltatás kétségkívül olyan informatikai szolgáltatás, amely rendelkezik mind a gazdaság, mind pedig a társadalom számára kedvező fejlődési potenciállal.

A felhőalapú számítástechnika gazdasági hajtóereje kétségkívül a méretgazdaságossága.

„Az adatfeldolgozás- és tárolás nagy adatközpontokba való koncentrálása javítja a drága erőforrások felhasználását, pl. az emberi tudását, a tárgyi tőkéjét (hardver, szoftver, épületek), a kommunikáció sávszélességét és az energiáját. Ezen túlmenően a felhőalapú szolgáltatások nyújtói nagyságuk és tömegük következtében, amikor erőforrásokat vásárolnak, különösen erős tárgyalási pozícióban vannak. A felhőszolgáltatók ezért csökkenthetik darabonkénti költségeiket, és kedvezőbb egységárakat kínálhatnak ügyfeleiknek. A méretgazdaságosság elérésének feltétele, hogy sok ügyfél legyen az «áruházban». Egy kielégítő tömeg elérése érdekében, a felhőalapú szolgáltatásokat világszerte az interneten kínálják.”¹⁸

A felhasználói oldalról szemlélve, a haszon ugyancsak a méretgazdaságosságra vezethető vissza. A magánszemélyek mellett, a gazdasági fejlődésben jelentékeny szerepet játszó kis- és közepes vállalkozások számára ugyanis lehetővé válik a megfizethető árú és méretezhető számítástechnikai forrásokhoz való hozzáférés. Amint azt már fentebb meghatároztuk, a 'számítási felhőadatok' interneten keresztül elért, távoli számítógépeken történő tárolását, feldolgozását és felhasználását biztosítja felhasználói számára. Ez azt jelenti, hogy a felhasználók kérésre szinte korlátlan számítási teljesítményhez juthatnak, igényeik kielégítéséhez nincs szükség jelentős befektetésekre, és adataikat bármilyen internet-hozzáféréssel rendelkező helyről elérhetik. A számítási felhő jelentősen csökkenti a felhasználók informatikai kiadásait és az így fennmaradó erőforrásokból számos új szolgáltatás fejlesztését teszi lehetővé. A felhő használatával még a legkisebb cégek is egyre nagyobb piacokat érhetnek el, a kormányok pedig még megcsorítások idején is vonzóbbá és hatékonyabbá tehetik szolgáltatásaikat.

Az Európai Bizottság meglátása szerint, tekintve, hogy a felhőalapú technológia még fejlődési potenciáljának elején jár, „[E]urópa számára lehetővé teszi, hogy a további fejlesztések éllavasává váljon és a széles körben elterjedt felhőhasználat, valamint a felhőalapú szolgáltatások révén a keresleti és a kínálati oldalon egyaránt előnyre tegyen szert.” Az előzetes prognózisok szerint 2020-ban a számítási felhő alkalmazása Unió-szerte további 45 milliárd EUR közvetlen befektetést jelenthet, 2020-ig 957 milliárd EUR¹⁹ összesített általános hatást gyakorolhat a GDP-re és 3,8 millió munkahelyet teremthet.

A felhőszolgáltatás használatának – a hagyományos fizikai adathordozókkal ellentétben – olyan specifikumai vannak, amelyek egyszersmind előnyt és hátrányt jelentenek. Ebben a

18 Sopot Memorandum i. m. (6. lj.) 32. pont.

19 IDC (2012) IDC (2012): „Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Take-up” (A számítási felhő iránti európai igénnyel kapcsolatos mennyiségi becslések és az esetlegesen felszámolandó akadályok); további részletekért pedig lásd az e közleményt kísérő bizottsági szolgálati munkadokumentum 3.1. szakaszát. A számítási felhő munkahelyteremtésben betöltött szerepének fontosságát az „Út a munkahelyteremtő fellendülés felé” című közlemény (COM(2012) 173 végleges) mellékletének „Kulcsfontosságú intézkedések az ikt-ágazat foglalkoztatási helyzete tekintetében” című szakasza is felismeri.

helyzetben a jogi szabályozásnak olyan normákat kell alkotni, amelyek lehetővé teszik, hogy a gazdasági-társadalmi előnyöket a hátrányos következmények kiküszöbölése mellett tudja biztosítani. Ebből adódóan a felhasználó más típusú veszélyekkel találja magát szembe a felhőalapú adattárolást biztosító szolgáltatások igénybevételekor, mint a más jellegű, akár elektronikus úton megvalósuló adattárolás során. A felhőszolgáltatások igénybevétele esetén a felhasználó nem a saját (többnyire fizikailag is rendelkezésére álló) eszközén (tárhelyén) tárolja az adatait, hanem egy másik személy, többnyire egy szolgáltató által üzemeltetett eszközön, amelyre az adatot elektronikus hírközlő hálózaton keresztül helyezi el. A felhasználónak úgy tűnhet, hogy nem kell tartania a tároló eszköz meghibásodásától vagy összetörésétől, elvesz(t)ésétől. Ezzel szemben azonban valójában tartania kell attól, hogy az üzemeltetett eszköz meghibásodik, a szolgáltató érdekkörén kívül. Ilyen esetekben szintén előfordulhat adatvesztés. Ugyanakkor ebben az esetben (is) szükség van egy 'közvetítő vagy lehívó' eszközre, amellyel kapcsolatban szintén felmerülhetnek ezek a kérdések.

A felhasználó számára ismeretlen helyen vannak az adatai, olyan szervereken, amelyeket nem tud felügyelni. Így az az adathordozó kikerül az ő fizikai védelme alól. A tárolt adatok maximálisan elhelyezhető mennyiségét a felhasználó által megvásárolt vagy ellentételezett adattár nagysága határozza meg. Ez a tárolási mód potenciálisan lényegesen nagyobb mozgásteret, szabadságot enged az adatok tárolása és hozzáférhetősége tekintetében, mint a fizikai eszközök tárolókapacitásai. A felhasználó a tárolt adatokat internethozzáféréssel és egy arra alkalmas eszközzel tudja lehívni, (elvileg) tértől és időtől függetlenül. Sok szolgáltató a maga felhőjét kiegészítő szolgáltatásként használja/nyújtja. Jó példával szolgálnak erre a nagy vállalatok és szolgáltatásaik (Google–Google Drive, Microsoft–One Drive, Yahoo–Yahoo mail, Dropbox, Apple– iCloud).

2.9. EU perspektíva – A számítási felhőben rejlő potenciál felszabadítása Európában

A felhőszolgáltatások térhódításával – amint arra korábban már utaltunk – szükségszerűen szabályozási szükséghelyzet keletkezett. Az Európai Bizottság, mint a közösségi jogalkotás motorja, 2012-ben kiadott egy közleményt,²⁰ amelyben az egységes digitális piac előmozdítása érdekében, illetve a felhasználói bizalom növelése céljából, szabályozási lépéseket javasolt. A Bizottság célja ezért – áll a közleményben – a számítási felhő valamennyi gazdasági ágazatban való gyorsabb alkalmazásának lehetővé tétele és megkönnyítése, miáltal csökkenhetnek az ikt-költségek, és – új digitális üzleti gyakorlatokkal kiegészítve – nőhet a termelékenység, a növekedés és a munkahelyek száma. Az egyik fontos kérdéskör, amelyet a Bizottság közleménye azonosított, az a 'szerződésekkel kapcsolatos problémák' halmaza volt. Ebben a körben több olyan releváns kérdést is felvet az érintett a közlemény, amelyek kapcsolódnak a felhőszolgáltatásokhoz, úgy, mint „[a]z adatok hozzáférhetőségével, hordozhatóságával, változáskezelésével és tulajdonjogával kapcsolatos aggályokkal (...) a szolgáltatás–kiesések – leállítás, adatvesztés – miatti felelősség miként ellentételezhető, (...) ki a felhőalapú alkalmazásokkal létrehozott adatok tulajdonosa, illetve hogyan történik az esetleges vitás kérdések rendezése.”

20 Számítási felhőben rejlő potenciál felszabadítása Európában, COM(2012) 529 final, Brüsszel, 2012.9.27.

A Bizottság idézett aggodalmai is jól mutatják, hogy a felhőszolgáltatások igénybevételére a szolgáltató és a felhasználó közötti sok mozzanatú jogviszonyt létrehozó szerződés (a továbbiakban: 'felhőszerződés') számos megválaszolandó kérdést vet fel és veszélyt rejt magában. A továbbiakban ezzel a felhőszerződés révén létrejövő jogviszonnyal kapcsolatban vizsgálunk meg néhány kérdést.

3. A felhőalapú szolgáltatások adatvédelmi jogi összefüggései

A gyors ütemű technológiai változás és a globalizáció mind kvantitatív, mind kvalitatív értelemben átalakította az állami, vállalati szektorban, de a magánérinkezésekben is folyamatosan növekvő mennyiségű személyes adat gyűjtésének, hozzáférhetőségének, felhasználásának és továbbításának módját. A becslések szerint 250 millió európai internet felhasználó minden napi életének, az online személyiség megélésének, kibontakoztatásának, az online társadalmi kapcsolattartás szerves részévé váltak a közösségi hálózatokon (médiában) megvalósuló új információ-megosztási módok, és az adatok, köztük nagyszámú személyes adat távoli helyen történő tárolása. Ugyanakkor vállalkozások számára is értékessé váltak a személyes adatok. A vállalkozások potenciális fogyasztóiról, fogyasztói szokásokról, piaci magatartásokról szóló (személyes) adatok piaci értékkel bírnak, az ügyfelek adatainak gyűjtése, összesítése és elemzése gyakorta gazdasági tevékenységük, üzleti stratégiájuk fontos részét képezi, így ezekért az adatokért, illetve ezen adatokból kikövetkeztethető információkért az érdekelt piaci szereplők jelentékeny pénzügyi eszközöket is hajlandók feláldozni. A potenciális ügyfelek adatainak gyűjtése, összesítése és elemzése tehát mára egyértelműen piacilag értelmezhető, értékkel bíró tevékenységgé vált (vö. *datafication*, *commodification* jelenségével).

Az érintettek természetesen ebben az új, digitális információs közegben is gyakorolják információs önrendelkezési jogukat, jogosultak arra, hogy tényleges ellenőrzést gyakorolhassanak személyes adataik felett, saját személyes adataik sorsáról minden döntést meghozzanak. Az érintettek információs önrendelkezési joga mind a személyes adatát kezelő adatkezelővel, mind pedig az adatkezelővel szerződésben álló adatfeldolgozóval szemben érvényesül. Amint a későbbiekben részletesen bemutatjuk, a legegyszerűbb felhőjogviszonyok kétpólusúak, az érintett és egy adatkezelő részvételével, az összetettebb jogviszonyok azonban tipikusan háromoldalúak, a két előbb jelzett alany mellett, egy adatfeldolgozó is kötelezettje a személyes adatok védelmével összefüggő jogi kapcsolatnak.

A felhőalapú informatikai rendszerek segítségével történő adatkezelés jogi értelemben legegyszerűbb formájában kétoldalú, de a komplexebb adatkezelések során (pl. vállalati adatkezelések esetén) legalább háromoldalú jogviszonyokat eredményeznek.

3.1. A felhőszolgáltatások általános adatvédelmi kockázatai

A személyes adatok felhőszolgáltatás útján történő feldolgozása – a hagyományos manuális, vagy informatikai mechanizmusokhoz képest egyaránt – a technológia jellegéből fakadó sajátos kockázatokat hordoz. A kockázatok közül, általánosan és némiképp szimplifikálva két jól azonosítható veszélyforrás fenyegeti a személyes adatok oltalmát: az adatok felett érvényesülő kontroll, valamint az adatfeldolgozási műveletekkel kapcsolatos transzparencia hiánya.

3.1.1. Az információbiztonság áttörése – az ellenőrzés hiánya

A két tipizált kockázati forrás közül az egyik az információbiztonsági általános követelményének áttörése, vagyis a teljes körűen érvényesülő ellenőrzés hiánya, hiszen a felhőszolgáltatás igénybevétele után – a felhőben történő adattárolás érdekében – személyes adatokat bocsátott a szolgáltató rendelkezésére, az adatkezelés során a továbbiakban elveszíti a kizárólagos ellenőrzési jogát az adatok fölött. Az ellenőrzés érintett általi kizárólagosságának hiánya, illetve az ellenőrzés bizonyos esetekben való lehetetlensége azonban komoly alkotmányos visszassághoz vezet, tekintettel arra, hogy az ellenőrzés (potenciálisan, még inkább konkrét) lehetőségének a hiányában az érintett elesik alanyi joga, aktív önrendelkezési joga gyakorlásától, többé már nem lesz ura saját adatainak. Nem várt esetben előfordulhat a személyes adatok bizalmas voltának, integritásának, rendelkezésre állásának sérelme anélkül, hogy arról az érintettel szemben felelősséggel tartozó adatkezelőnek, és/vagy magának a személyes adat jogosultjának tudomása lenne.

3.1.2. Adathordozhatóság kétsége

Az adatok folyamatos, és feltétlen rendelkezésre állása bizonyos körülmények között kétséggé, vagy nehézkessé válhat. Ennek oka többek között a szolgáltatók közötti átjárhatóság esetlegességére vezethető vissza. Az átjárhatóság hiánya (*vendor lock in*) elsősorban abból következik, hogy egyes felhőszolgáltatók saját, más szolgáltatókétól különböző technológiát, szoftvert alkalmaznak, s így a felhasználó számára az adatok szolgáltatók (felhőalapú rendszerek) közötti átvitele nehézségbe ütközhet, vagy ellehetetlenülhet.

A szolgáltatás biztonságos, zavarmentes működtetésének esetlegessége, a tárolt tartalmak szerver- vagy hálózati hibákból fakadó elérési zavarai szintén a rendelkezésre állás bizonytalanságához vezethetnek, amely a szolgáltatásba vetett felhasználói bizalom megerősödése ellen hathat.²¹

3.1.3. Adatok sértetlensége

A sérülésmentesség/sértetlenség hiánya az erőforrások megosztása miatt következhet be. A felhőt, mint tárhelyet, informatikai értelemben megosztott rendszerek és infrastruktúrák alkotják. A szolgáltatók az érintettek széles köréből származó személyes adatokat dolgoznak fel, és előfordulhat, hogy az adatfeldolgozás során ellentétes érdekek és/vagy eltérő célok jelenhetnek meg.

²¹ Az adatok folyamatos rendelkezésre állását sok esetben szerver- vagy hálózati hibák is befolyásolhatják, s bár ezek az esetlegességek a szolgáltatás biztonságos igénybe vétele vonatkozásában számba veendő kockázatot jelentenek, nem kifejezetten jogi, sokkal inkább informatikai szempontból vizsgálándók. Természetesen az ilyen hibákból fakadó (vagyonosi és nem vagyonosi) károk, mint következmények felvethetik a szolgáltató kontraktuális felelősségének a kérdését. Ezzel azonban itt nem foglalkozunk.

3.1.4. Az adatvédelmi szint univerzalitásának hiánya

Amint arra már utaltunk, a felhőszolgáltatások határokon átívelő, globális szolgáltatásokként írhatók le. A szolgáltatók gyakorta több országban párhuzamosan hoznak létre adatközpontokat, így a szolgáltatás tényleges helye és ezáltal a rá vonatkozó nemzeti jog számos tényező együtthatására tekintettel: pl. csúcsterhelés esetén valamely adatközpont kapacitásának hiánya miatt) időről-időre változhat. Ez a szolgáltatási modell azonban azzal a kockázattal jár, hogy az adatok továbbítása olyan államba történik, amelynek jogrendszere nem biztosítja a személyes adatok megfelelő védelmét.

Az Európai Unió is különös hangsúlyt fektet a felhőszolgáltatások adatbiztonsági relációjára, tekintve, hogy a magas szintű adatvédelmi szabályok érvényesülése sok tekintetben, így a gazdasági fejlődés által motivált belső piac szempontjából is döntő jelentőséggel bír. Az adatvédelem magas szintje hozzájárulhat az információs társadalommal összefüggő, így online elérhető szolgáltatások iránti bizalom erősödéséhez, és az így létrejött felhasználói bizalom kiaknázhatóvá teheti a digitális gazdaságban rejlő lehetőségeket. Az adatvédelem, mint a gazdasági növekedést serkenteni képes bizalmi tényező kiemelt figyelmet kap az Európai Unió jogalkotásában, hiszen az hozzájárulhat az uniós iparágak versenyképességéhez, ami a globális versenyben elemi érdeke a belső piacot működtető közösségnek. Ezért külön pontban foglalkozunk az adatvédelmi kockázatok EU-s dimenzióival.²²

4. Az Európai Unió adatvédelmi jogi szabályozási kerete és a felhőszolgáltatás kihívása

4.1. Az Európai Unió szabályozásának jogi forrásai és a jogalap

A természetes személyek személyes adatainak kezelésével összefüggő védelem az Európai Unióban rendkívül magas jogvédelmet élvez, tekintettel arra, hogy azt az alapvető jogi dokumentumok (elsődleges jogforrások) alapvető jogként ismerik el. Az Európai Unió Alapjogi Chartája 8. cikkének (1) bekezdése és az Európai Unió működéséről szóló szerződés (EUMSZ) 16. cikkének (1) bekezdése egyaránt rögzíti, hogy mindenkinek joga van a rá vonatkozó személyes adatok védelméhez.

Az Alapjogi Charta az adatkezelés generál klauzulájaként rögzíti, hogy „[a személyes] adatokat csak tisztességesen és jóhiszeműen, meghatározott célokra, az érintett személy hozzájárulása alapján vagy valamilyen más, a törvényben rögzített jogos okból lehet kezelni”, továbbá röviden rámutat az információs önrendelkezési jog két szelvényére: „[m]indenkinek joga van ahhoz, hogy a róla gyűjtött adatokat megismerje, és joga van azokat kijavíttatni.”²³

A jogalap kérdéséről az EUMSZ 16. cikk. (2) bekezdése rendelkezik, megteremtve az uniós jogalkotási hatáskört a személyes adatok védelmére: „A természetes személyeknek az uniós intézmények, szervek és hivatalok által, illetve az uniós jog alkalmazási körébe tartozó tevékenységeik során a személyes adataiknak a tagállamok által végzett feldolgozása tekintetében

²² L. 4. 5. pontot.

²³ Az Európai Unió Alapjogi Chartája 8. cikk (2) bek. [2012/C 326/02, 26.10.2012].

történő védelmére, valamint az ilyen adatok szabad áramlására vonatkozó szabályokat rendes jogalkotási eljárás keretében az Európai Parlament és a Tanács állapítja meg.”²⁴

A felhőszolgáltatások adatvédelmi jogi aspektusaira a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK irányelv²⁵ (a továbbiakban: Irányelv) biztosítja a jogi hátteret. Az Irányelv rendelkezéseit kell alkalmazni minden olyan esetben, amikor felhőszolgáltatás keretében személyes adat kezelésére kerül sor. Az Irányelv 2018. május 25-én hatályát veszti. Ekkor válik ugyanis alkalmazandóvá az Európai Parlament és Tanács által elfogadott általános adatvédelmi rendelet²⁶ (a továbbiakban: GDPR), amely közvetlen hatályú és alkalmazható kógens normáival váltja fel a korábbi harmonizációs célú jogforrást.²⁷ Jelen tanulmányban arra tekintettel elemezzük a még hatályban lévő Irányelv vonatkozó rendelkezéseit, hogy röviden kitekintünk a GDPR alkalmazandóvá válásával bekövetkező változásokra is.²⁸

4.2. Az alkalmazott nemzeti jog meghatározása

Az Irányelv, mint jogharmonizációs jogforrás nem állapít meg közvetlenül alkalmazandó szabályokat, azok célkitűzéseit a tagállamok kötelesek átültetni a nemzeti jogukba. Így egy meghatározott adatkezelés során az alkalmazott konkrét szabályok attól függenek, hogy melyik tagállam nemzeti jogában meghatározott normákat kell alkalmazni. Az alkalmazott nemzeti jogra irányadó szabályokat az Irányelv 4. cikke állapítja meg, amely kimondja, hogy minden tagállam az Irányelvnek megfelelően elfogadott, harmonizált nemzeti rendelkezéseket alkalmazza. Az Irányelv vonatkozó cikkének személyi hatálya egyaránt kiterjed az egy vagy több tagállamban letelepedett, illetve a nem az Európai Unió tagállamának területén letelepedett, de a személyes adatok feldolgozása során valamely tagállam területén működtetett eszközt alkalmazó adatkezelőre.

Az Irányelv 29. cikke alapján működő adatvédelmi munkacsoport²⁹ (a továbbiakban: 29-es adatvédelmi munkacsoport) véleménye – hivatkozva az Irányelvre – egyértelművé teszi,

24 Az Európai Unióról szóló szerződés és az Európai Unió működéséről szóló szerződés egységes szerkezetbe foglalt változata, 2012/C 326/01, C 326, 26/10/2012 o. 0001 – 0390.

25 Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról. (a továbbiakban: Irányelv), www.eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:31995L0046&from=HU.

26 2016/679 EU rendelet Az Európai Parlament és Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet).

27 A GDPR elemzését I. SZABÓ Endre Győző: Az Európai Unió általános adatvédelmi rendeletének egyes kérdéseiről I. *Pázmány Law Working Papers*, Pázmány Péter Katolikus Egyetem, 2016/26, www.d18wh0wf8v71m4.cloudfront.net/docs/wp/2016/2016-26_Szabo.pdf; SZABÓ Endre Győző: Az Európai Unió általános adatvédelmi rendeletének egyes kérdéseiről II. *Pázmány Law Working Papers*, Pázmány Péter Katolikus Egyetem, 2016/27, www.plwp.eu/docs/wp/2016/2016-27_Szabo.pdf; SZABÓ Endre Győző: Az Európai Unió általános adatvédelmi rendeletének egyes kérdéseiről III. *Pázmány Law Working Papers*, Pázmány Péter Katolikus Egyetem, 2016/28, www.plwp.eu/docs/wp/2016/2016-28_Szabo.pdf

28 A terminológia a magyar jogi szaknyelvben szokatlan, de a GDPR szövege expressis verbis fogalmaz úgy, hogy a GDPR már hatályos, de alkalmazandóvá csak 2018. május 25-től válik.

29 Az Irányelv 29. cikke elrendeli a személyes adat-feldolgozás vonatkozásában az egyének védelmével foglalkozó tanácsadói státuszban működő és eljárásában függetlenül munkacsoport felállítását. A munkacsoport az egyes tagállamok által kijelölt felügyelő hatóság vagy hatóságok képviselőjéből, a közösségi intézmények és szervek nevében létrehozott hatóság vagy hatóságok képviselőjéből, továbbá a Bizottság egy képviselőjéből áll.

hogy az alkalmazandó jogot nem a felhőszolgáltató letelepedési/működési helye, hanem a felhőszolgáltatást igénybe vevő, felhasználó/adatkezelő letelepedési helye alapozza meg.³⁰

Amennyiben az adatkezelő több tagállamban is letelepedett, és ezekben a tagállamokban adatokat dolgoz fel, minden esetben annak a tagállamnak a joga az alkalmazandó jog, amelyben a konkrét adatfeldolgozás történik, és a letelepedés valamennyi helyén meg kell, hogy feleljen az alkalmazandó nemzeti jog által megállapított adatvédelmi szabályoknak.

Az Irányelv végül szabályozza azt az esetet is, amikor az adatkezelő nem telepedett le a Közösség területén, és a személyes adatok feldolgozása céljából gépi vagy más olyan eszközt alkalmaz, amely a fenti tagállam területén található (kivéve, ha ezt az eszközt kizárólag a Közösség területén átmenő adatforgalom céljára használják). Ebben az esetben, amikor a felhőszolgáltatás igénybevevője az EGT-n kívül telepedett le, de az EGT-n belül letelepedett felhőszolgáltatót bíz meg az adatfeldolgozással, úgy a szolgáltató az igénybevevőjére is kiterjeszti az EU-s adatvédelmi alapelveken nyugvó, tagállami jogszabályok hatályát.

4.3. Nemzetközi adattovábbítások

Az Irányelv 25. és 26. cikke csak abban az esetben teszi lehetővé automatikusan a személyes adatok szabad áramlását az EGT területén kívüli országokba, ha amellet, hogy az adatkezelés kellő jogalappal rendelkezik és egyébként is minden tekintetben jogszerű, az adat továbbítására megjelölt célország jogrendszere a megfelelő adatvédelmi szintet biztosítja.³¹ A védelmi szint megfelelőségét „[az] adattovábbítási művelet vagy adattovábbítási műveletsorozat feltételeinek figyelembevételével kell értékelni.” E körben különös figyelemmel kell lenni „[az] adatok jellegére, a tervezett adatfeldolgozási művelet vagy műveletek céljára és időtartamára, a kiindulási és a célországra, az adott harmadik országban hatályos, általános és ágazati jogrendre, valamint az adott országban érvényesülő szakmai szabályokra és biztonsági intézkedésekre”.³² Egyéb esetben az adatkezelőnek, társ-adatkezelőinek és/vagy adatfeldolgozóinak különleges biztosítékokat kell nyújtaniuk a személyes adatok védelmét biztosító szabályok sértetlensége érdekében. Az Irányelvben rögzített, szigorú adattovábbítási szabályokat különösen annak fényében kell értékelni, hogy az EU messzemenőkéig érvényesíti a személyes adatok védelmét, és vannak olyan EGT-n kívüli harmadik országok (még oly demokratikus ország is, mint példának okáért az Egyesült Államok), amelyek alkotmányos tradícióik, jogfejlődésük, vagy éppen a közelmúltjukban rejlő fejlemények miatt, az adatvédelemnek egy, az európainál enyhébb modelljét valósítják meg. Annak érdekében, hogy az EU-s állampolgárok személyes adatai az EU által megkövetelt védelmi szintnek megfelelő oltalmat élvezzék az EGT-n kívüli országokban is, szükséges annak biztosítása, hogy az Irányelvben rögzített alapelvek és intézményes garanciák érvényesüljenek.

Az Irányelv 26. cikk (1) bekezdése a megfelelő adatvédelmi szint biztosítását előíró rendelkezés alól meghatározott esetekben felmentést ad, amennyiben:

30 29-es munkacsoport véleménye i.m. (14. lj.).

31 Irányelv i.m. (27. lj.) 25. cikk (1) bek.

32 Uo., (2) bek.

- a) az érintett egyértelműen hozzájárulását adta személyes adatának tervezett továbbításához, vagy
- b) a továbbítás az érintett és az adatkezelő közötti szerződés teljesítéséhez, vagy az érintett kérelmére hozott, szerződést megelőző intézkedések végrehajtásához szükséges; vagy
- c) a továbbítás az adatkezelő és valamely harmadik fél közötti, az érintett érdekét szolgáló szerződés megkötéséhez vagy teljesítéséhez szükséges; vagy
- d) a továbbítás fontos közérdekből vagy jogi követelések létrejötte, érvényesítése vagy védelme miatt szükséges, illetve azt jogszabály írja elő; vagy
- e) a továbbítás az érintett létfontosságú érdekeinek védelme miatt szükséges; vagy
- f) a továbbítást olyan nyilvántartásból végzik, amely a törvények vagy rendeletek értelmében a nyilvánosság tájékoztatását szolgálja, és amely általában a nyilvánosság, vagy bármely jogos érdekét igazoló személy számára betekintés céljából rendelkezésre áll, amennyiben a jogszabályok által a betekintésre megállapított feltételek az adott esetben teljesülnek.³³

A fenti esetek közül, az érintett által adott hozzájárulás lehet a leggyakoribb indok, a személyes adat megfelelő védelmi szintet nem biztosító állam joghatósága alatt álló szolgáltató felhőalapú rendszerébe való adattovábbításra. Ilyenkor ugyanis az érintett dönt személyes adatai sorsáról, arról, hogy azokat egy, az uniós jogvédelemnél alacsonyabb szintű oltalmat biztosító ország szabályozásának védelme alá helyezi, s kiteszi magát annak, hogy az adatokhoz illetéktelenek hozzáférhetnek, azokat megismerhetik, illetve visszaélhetnek velük. Az érintett döntésének szabadságához azonban hozzá kell tenni, hogy a felhőszolgáltatók piaci ereje miatt, a szolgáltatás igénybevétele kapcsán egy érdekérvényesítési aszimmetria tapasztalható, amint azt a 29-es adatvédelmi munkacsoport is észlelte, s amire a felhőjogviszonyra vonatkozó pontban mi is ki fogunk térni. Ebből fakadóan a döntési szabadság részben korlátozott – vagy, ha tetszik látszólagos –, és csak arra terjed ki, hogy az érintett eldöntse hozzájárul-e adatainak felhőbe való továbbításához, és vállalja-e az azzal járó kockázatot.

Az Irányelv továbbá még abban az esetben is lehetővé teszi az EGT-n kívülre történő adattovábbítást – vagyis a tagállamok engedélyezhetik a személyes adatok harmadik országba irányuló továbbítását vagy továbbítás-sorozatát –, amennyiben a harmadik ország ugyan nem biztosít megfelelő szintű védelmet, de az adatkezelő megfelelő garanciákat teremt az egyének magánéletének, alapvető jogainak és szabadságainak védelme, továbbá a kapcsolódó jogok gyakorlása tekintetében. A garanciák körében az Irányelv kiemeli a felhőszolgáltatásra irányuló szerződésben megfelelő, az Irányelv követelményeit kielégítő általános szerződési feltételek biztosítását.³⁴ Az ilyen tagállamok által biztosított egyedi döntésről (engedély) a tagállam köteles értesíteni a Bizottságot és a tagállamokat,³⁵ akiknek jogukban áll tiltakozni, s ezzel összefüggésben a Bizottság intézkedéseket foganatosíthat. Amennyiben a Bizottság úgy dönt, hogy az egyes általános szerződési feltételek biztosítják a megfelelő védelmi szintet, úgy a tagállamok kötelesek megtenni a bizottsági döntés teljesítéséhez szükséges intézkedéseket.³⁶

33 Uo., 26. cikk (1).

34 Uo., 26. cikk (2) bek.

35 Uo., 26. cikk (3) bek.

36 Uo., 26. cikk (4) bek.

4.4. A biztonságos adatkikötő (Safe Harbor)³⁷ és a megfelelő védelmi szint elve

A megfelelőségi vizsgálat nem fedi le a felhő alapú szolgáltatásokkal összefüggő valamennyi adattovábbítást, mivel az földrajzi szempontból korlátozott. A 29-es adatvédelmi munkacsoport álláspontja szerint, a biztonságos adatkikötőre vonatkozó megfelelőségi nyilatkozat önmagában nem tekinthető elegendőnek, amennyiben nem jár együtt az adatvédelmi elvek határozott érvényesítésével a felhőalapú számítástechnikai környezetben.

Emellett az Irányelv 17. cikke előírja, hogy az adatkezelőnek a feldolgozás céljából szerződést kell kötnie az adatfeldolgozóval. Az adatfeldolgozásra vonatkozó szerződés vagy más jogi aktus az adatfeldolgozót az adatkezelővel szemben köti, és minimálisan kimondja, hogy az adatfeldolgozó kizárólag az adatkezelő utasítása alapján járhat el, továbbá az adatfeldolgozót terhelő ezen kötelezettséget annak a tagállamnak a jogszabályai szerint kell meghatározni, amelyben a feldolgozó letelepedett, és azok a feldolgozóra is vonatkoznak.³⁸

Az adatkezelő kötelezettsége továbbá, hogy – amennyiben az adatfeldolgozás az ő nevében történik – olyan adatfeldolgozót válasszon, aki a technikai biztonsági intézkedések és az elvégzendő adatfeldolgozásra vonatkozó szervezési intézkedések tekintetében megfelelő garanciákat nyújt, továbbá köteles biztosítani az említett intézkedések teljesítését.³⁹

Ezt az EU-USA biztonságos adatkikötő keretrendszerének dokumentációjában szereplő 10. gyakran ismételt kérdésre adott válasz is megerősíti. A különböző nemzeti jogszabályok és adatvédelmi hatóságok további követelményeket támaszthatnak.

4.4.1. A Safe Harbor egyezmény

Az Európai Unióból az Egyesült Államokba történő adattovábbítás azért keltett különösen komoly aggodalmat, mivel a két adatvédelmi rendszer védelmi szintje között jelentékeny különbség van, amely az utóbbiban lényegesen alacsonyabb, továbbá az USA Alkotmányának sajátosságai miatt, az nem védi a nem USA állampolgárokat.

Az Európai Bizottság 2000. július 26-án fogadta el az Egyesült Államokra vonatkozóan azt a megfelelőségi határozatot,⁴⁰ (520/2000/EK határozat (a továbbiakban: biztonságos adatkikötőről szóló határozat), amelyben elismeri az Egyesült Államok Kereskedelmi Minisztériuma által kiadott, biztonságos adatkikötőre (*Safe Harbor*) vonatkozó alapelveket és az ezzel kapcsolatos gyakran felvetődő kérdéseket, mivel azok – áll a határozatban – megfelelő védelmet biztosítanak az EU-ból továbbított személyes adatok számára. A *Safe Harbor* megállapodás következtében a Bizottság olyan esetekben is lehetővé tette a személyes adatok továbbítását a tagállamokból az Irányelvben megfogalmazott alapelveket elfogadó amerikai vállalatok számára, amelyek az Európai Unió és az Egyesült Államok adatvédelmi szabályo-

37 A magyar nyelvű fordítások közül (védett, megbízható stb. adatkikötő) a biztonságos (adat)kikötő kifejezést használjuk, tekintettel arra, hogy a magyar nyelvű dokumentumokban ez a szóhasználat terjedt el.

38 Irányelv i. m. (27. lj.) 17. cikk (3) bek.

39 Uo., (2) bek.

40 A Bizottság közleménye az Európai Parlamentnek és Tanácsnak a védett adatkikötő működése az uniós polgárok és az EU-ban letelepedett vállalatok szempontjából, COM(2013) 847 final, [www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com\(2013\)0847/_com_com\(2013\)0847_hu.pdf](http://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com(2013)0847/_com_com(2013)0847_hu.pdf)

zásának különbözősége, és az USA védelmi szint alacsonyabb volta miatt, a megállapodás nélkül nem felelnének meg a megfelelő szintű adatvédelemre vonatkozó uniós elvárásnak.

A *Safe Harbor* jogi rezsim működése a csatlakozó vállalatok önkéntes kötelezettségvállalására, önkorlátozására és öntanúsítására épült azzal, hogy a megállapodás betartása az alávető tengerentúli vállalatok számára kötelező volt. A biztonságos adatkikötő kritériumok magukba foglalták a csatlakozó vállalatok adatvédelmi politikájának átláthatóságát, és az adatvédelmi elveknek abba való beépítését is.

A 29-es adatvédelmi munkacsoport véleménye szerint az adatokat *exportáló* vállalatnak bizonyítékot kell szereznie arra vonatkozóan, hogy a biztonságos adatkikötőre vonatkozó megfelelőségi nyilatkozatok valóban léteznek, és olyan *bizonyítékot* kell igényelnie, amely tanúsítja az abban foglalt elvek tényleges betartását. Ez kiváltképpen fontos az adatfeldolgozás révén érintett adatalanyok által szolgáltatott információk vonatkozásában. A munkacsoport úgy véli továbbá, hogy a felhőalapú szolgáltatás igénybe vevőjének ellenőriznie kell, hogy a szolgáltató által összeállított, általános szerződési feltételek összhangban állnak-e a *szerződéses* adatfeldolgozással kapcsolatos nemzeti követelményekkel. A nemzeti jogszabályok előírhatják, hogy a szerződésben kell meghatározni a további feldolgozást, amely felöleli a helyszíneket és az alvállalkozókra vonatkozó egyéb adatokat, valamint az adatok nyomon követhetőségét. A felhőszolgáltatók általában nem nyújtanak ilyen információkat az igénybe vevőknek. Ilyen esetekben az adatexportőr alkalmazza az egyéb rendelkezésre álló jogi eszközöket, így az általános szerződési feltételeket, vagy a kötelező erejű vállalati szabályokat.

Az adatvédelmi munkacsoport véleményében úgy ítélte meg, hogy a biztonságos adatkikötő elvei önmagukban nem garantálhatják az adatexportőr számára az annak biztosításához szükséges eszközöket, hogy az egyesült államokbeli szolgáltatók megfelelő biztonsági intézkedéseket alkalmazzanak, amint azt az Irányelven alapuló nemzeti jogszabályok előírhatják számukra.

A biztonságos adatkikötő rendszerének EU részéről való felülvizsgálatának szükségessége 2013-ban vetődött fel, bizonyos új összefüggésekre tekintettel. A Bizottság 2013. november 27-én fogadott el egy közleményt a biztonságos adatkikötő működése, az uniós polgárok és az EU-ban letelepedett vállalatok szempontjából. Ebben többek között az alábbiakra hívta fel a figyelmet:⁴¹

- a) az adatáramlás exponenciális növekedése, amely korábban csupán kíséreljensége volt a digitális gazdaság gyors növekedésének, mára azonban annak központi elemévé vált, továbbá az adatgyűjtés, -feldolgozás és -használat terén, rendkívül jelentős fejlődés következett be,
- b) az adatáramlások kiemelkedő fontossága, különösen a transzatlanti gazdaság számára,
- c) a biztonságos adatkikötőre vonatkozó szabályozáshoz csatlakozó amerikai vállalatok számának gyors emelkedése, amely 2004 óta nyolcszorosára (a 2004. évi 400-ról a 2013-ban 3246-ra) nőtt,
- d) az Egyesült Államok hírszerzési programjairól a közelmúltban napvilágra jutott információk, amelyek újból megkérdőjelezzik azon védelem szintjét, amelyet a biztonságos adatkikötőre vonatkozó szabályozás garantálni látszott.

A fent említett négy megállapítás során kétséggel a negyedik, az USA hírszerzési tevékenységével összefüggő adatvédelmi bizonytalanság gyengítette leginkább a biztonságos adatkikötő rendszerének fenntarthatóságát.

41 Uo.

4.4.2. *Patriot Act*⁴²

A Bizottság 2013-as közleményében hivatkozott amerikai hírszerzési tevékenységre leginkább az Edward Snowden által kibombantott megfigyelési botrány hívta fel a figyelmet, de annak jogi alapját egy egy évtizeddel korábban elfogadott jogforrás képezte.

Az USA Kongresszusa 2001-ben fogadta el a *Patriot Act*-et, amely egyértelmű reflexió volt a szeptember 11-i terrortámadásra, és amely széles körű jogosítványokat biztosított a szövetségi kormányzat számára. Adatvédelmi szempontból a leglényegesebb rendelkezés kétségtől az volt, hogy a végrehajtó hatalom az USA joghatósága alá tartozó vállalatok által kezelt adatokat, bírói végzés nélkül is lefoglalhatta. E rendelkezés lényegében védtelenné, kiszolgáltatottá tette az EU polgárok USA-ba továbbított személyes adatait az amerikai kormányzattól...

A *Safe Harbor* kritériumokat teljesítő amerikai vállalatok tehát ugyan elviekben biztosították a megfelelő adatvédelmi szintet, ám annak tényleges biztosítása a *Patriot Act* által konstituált kormányzati hatáskörre tekintettel lehetetlen volt, egy vállalat ugyanis hiába vette alá magát a szigorú adatvédelmi elvárásoknak, a bírói végzés nélküli kormányzati hatáskör miatt az adatok bizalmasságát (oltalmát) végső soron nem tudták biztosítani.

2015 októberéig a *Safe Harbor* megállapodás alapján, az amerikai vállalkozások továbbíthatták az európai polgárok személyes adatait az Egyesült Államokba. Az amerikai Központi Hírszerző Ügynökségnél (NSA) dolgozó, Edward Snowden nevéhez fűződő adatszivárgási botrány után, azonban egyre többen kérdőjelezték meg a keretegyezmény alkalmasságát. Az egykori műveleti tisztviselő révén nyilvánosságra került sok egyéb mellett az is, hogy az amerikai hírszerzés tömegesen vizsgálja a nem amerikai, így az európai polgárok személyes adatait is. Ez ellen lépett fel egy osztrák jogász Maximillian Schrems, akinek a beadványa nyomán, az Európai Unió Bírósága az ír legfelsőbb bíróság előzetes döntéshozatal iránti kérelmére meghozott, 2015. október 6-i ítéletével⁴³ megszüntette a *Safe Harbor* rendszerét.

4.4.3. *Privacy Shield*

A *Safe Harbor* megszűnése után szükséges volt egy új adattovábbítási mechanizmust bevezetni. A 29-es adatvédelmi munkacsoport az Európai Unió Bíróságának döntését követően, 2016. február 2-3-i plenáris ülésén megvitatta, hogy az ítélete mennyiben befolyásolja a nemzetközi adattovábbításokat. A Munkacsoport a vizsgálatát az európai emberi jogi esetjog alapulvételével végezte el, amely négy alapvető garanciát követel meg a nemzetbiztonsági célú adatkezelések területén:

- 1) Az adatkezelésnek világos, pontos és mindenki számára hozzáférhető szabályokon kell alapulnia: ez egyben azt is jelenti, hogy bárkinek, akit az adatkezelésről kielégítően tájékoztattak, képesnek kell előre látnia, hogy mi történik majd személyes adataival, ha azokat külföldre továbbítják;

42 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf.

43 Maximillian Schrems v. Data Protection Commission ügy [c-362/14.],

www.curia.europa.eu/juris/document/document.jsf?docid=169195&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=HU&cid=1178236.

- 2) A szükségesség és arányosság követelményeinek az adatkezelés törvényes céljára tekintettel érvényesülniük kell: a személyek jogaiba való beavatkozásnak egyensúlyban kell állnia az adatgyűjtés és -kezelés törvényes céljával (általában a nemzet biztonságával);
- 3) Egy hatékony és pártatlan független felügyeleti eljárást kell biztosítani: ezt végezheti bíróság, vagy más független szerv, mindenestre rendelkeznie kell azzal a minimális jogkörrel, amely a szükséges ellenőrzések lefolytatását lehetővé teszi;
- 4) Az egyének hatékony védelmét biztosítani kell: mindenkinek biztosítania kell azon jogát, hogy megvédhesse jogait egy független szerv előtt.

A Munkacsoport a továbbiakban hangsúlyozta, hogy a fenti négy garanciának minden esetben konjunktívan érvényesülnie kell mindazon esetekben, amikor személyes adatot továbbítanak az Európai Unióból az Egyesült Államokba, vagy más harmadik országba, vagy azokat az Európai Unió tagállamai kezelik.

A Munkacsoport bár elismerte az Egyesült Államoknak azokat az erőfeszítéseit, amelyeket 2014-2015-ben tett a nem amerikai állampolgárok alapjogai védelmének javítására, mégis fenntartotta korábbi aggályait abban a vonatkozásban, hogy az Egyesült Államok jogszabályai tartalmazzák-e mind a négy garanciát, különösen az adatkezelés célja és az adatalányok számára nyitva álló jogorvoslati lehetőségek vonatkozásában.⁴⁴

Az új szisztéma *Privacy Shield* beszédes címmel került elfogadásra. A Bizottság álláspontja szerint a *Privacy Shield* megvédi az uniós polgárok alapjogait és jogi biztonságot nyújt a cégek számára és megfelel az Európai Unió Bírósága által megszabott feltételeknek. A korábbiakhoz képest három pontban foglaljuk össze azokat a legfontosabb változásokat, amelyeket a *Privacy Shield* eredményeként értékelhetünk:

- 1) Az Egyesült Államok jogilag kötelező erejű dokumentumban vállalta, hogy az amerikai hatóságok csak korlátozások mellett férhetnek hozzá az uniós állampolgárok USA-ban tárolt adataihoz. Ehhez az amerikai fél írott biztosítékot ad, amelynek betartását az uniós fél ellenőrizheti.
- 2) A mechanizmus része egy évenként megvalósuló átvilágítás, amelyet az Európai Bizottság és az USA Kereskedelmi Minisztériuma közösen folytat le, annak érdekében, hogy kivizsgálják teljesülnek-e az Egyezményben foglalt vállalások. A felügyeleti munkában továbbá hatáskört kapnak a tagállami adatvédelmi hatóságok is.
- 3) Az uniós állampolgárok közvetlenül az amerikai jogrendszerben kapnak jogvédelmet. Az EU-s polgárok jogvédelemért a nemzeti adatvédelmi hatósághoz fordulhatnak, melyek az amerikai Szövetségi Kereskedelmi Bizottsággal (*FTC*) együttműködve – szigorú határidők által kötött eljárásban – vizsgálják ki, hogy megvalósult-e a panaszolt jogsértés. Amennyiben az *FTC* és a nemzeti adatvédelmi hatóság között lefolytatott egyeztetési eljárás nem jár eredménnyel, úgy az érintett a döntőbírószághoz fordulhat. Az USA fórumrendszerében a panaszokat nem a hírszerző hatóságok, hanem egy új ombudsman-típusú szerv kezeli, amelyik (elvben) függetlenséget élvez.

⁴⁴ A 29-es cikk szerinti Munkacsoport nyilatkozata a Schrems-ügy következményeiről, www.naih.hu/files/2016-02-08-nyilatkozat_forditas_SCHREMS.pdf.

A Bizottság határozata az EU–USA adatvédelmi pajzs által biztosított védelem megfelelőségéről 2016. július 12-én megszületett.⁴⁵

„[A]z EU–USA adatvédelmi pajzs olyan öntanúsítási rendszeren nyugszik, amelynek keretében az egyesült államokbeli szervezetek kötelezettséget vállalnak egy sor adatvédelmi elv – az EU–USA adatvédelmi pajzs keretelvei, köztük a kiegészítő elvek betartására. Ezeket az elveket az Egyesült Államok Kereskedelmi Minisztériuma bocsátotta ki, és megtalálhatók a határozat II. mellékletében. A pajzs egyaránt vonatkozik az adatkezelőkre és az adatfeldolgozókra (megbízottakra), azzal a sajátossággal, hogy az adatfeldolgozók szerződéses kötelezettsége, hogy kizárólag az uniós adatkezelő utasításai alapján járhatnak el, és segítséget kell nyújtaniuk az utóbbinak ahhoz, hogy választ adjon az elvek alapján a jogait gyakorló egyéneknek.”⁴⁶

Az adatvédelmi pajzs értelmében az öntanúsítás keretében a szervezeteknek vállalniuk kell a Bizottság végrehajtási határozatában felsorolt elveket.⁴⁷

4.5. Az adatvédelem és adatbiztonság technikai és szervezési intézkedései a felhőalapú szolgáltatásokban

Az Irányelv 17. cikk. (2) bekezdése szerint tehát az adatkezelőként eljáró, a felhőjogviszonyban igénybe vevőként, felhasználóként pozícionált fél teljes felelősséggel tartozik a felhőszolgáltató megválasztásáért. Ebből fakadóan, a felelősségük fennáll a személyes adatok védelme érdekében szükséges technikai és szervezési megoldások betartatásáért is.

A 29-es Bizottság véleményében kifejtett álláspontjában adatbiztonsági szempontból, kiáltépp az alábbi követelmények biztosítása érdemel kiemelt figyelmet:

- 5) Rendelkezésre állás követelménye: a személyes adatokhoz való gyors és megbízható hozzáférés biztosítását jelenti. Tekintettel arra, hogy a felhőalapú adattárolás és -elérés hálózati infrastruktúrán (internet, intranet, egyéb hálózat) keresztül történik, előfordulhat a hírközlési hálózaton olyan zavar (hálózati kapcsolat megszakadása, szerverteljesítmény radikális csökkenése, vagy megszűnése), amely az adatokhoz való hozzáférést gátolja. Hasonlóan a hozzáférést akadályozhatják meg a felhő informatikai rendszerében a feldolgozási, vagy az adattárolási infrastruktúrában bekövetkező hibák (pl. hardver meghibásodás). Előbbi sok esetben rosszindulatú (hacker) támadás következménye, de mind a két, a rendelkezésre állást átmenetileg, vagy tartósan ellehetetlenítő hiba véletlen, műszaki okból is bekövetkezhet.

Az igénybe vevőnek, mint adatkezelőnek a felelőssége, hogy ellenőrizze, a szolgáltató megtett-e minden olyan ésszerű intézkedést, amely a szolgáltatás megszakadásának kockázatát képes kiküszöbölni. Ilyen intézkedés lehet például a tartalék hálózati

45 A Bizottság (EU) 2016/1250 végrehajtási határozata a 95/46/EK európai parlamenti és tanácsi irányelv alapján az EU–USA adatvédelmi pajzs által biztosított védelem megfelelőségéről (a továbbiakban: Adatvédelmi pajzs határozat), www.eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016D1250&from=EN.

46 Uo., 14. bek.

47 Uo., 2.1. pont.

kapcsolatok kiépítése, másodlagos adattárolási kapacitások fenntartása, személyes adatok biztonsági másolatának biztosítása.⁴⁸

- 6) Sértetlenség: a személyes adatok azon tulajdonsága, amely biztosítja, hogy az adatkezelés, adatfeldolgozás során épségük nem kerül veszélybe, az adatok (illetéktelen) módosítása nem valósulhat meg, vagyis az adatfeldolgozás során a személyes adatok változatlanok maradjanak. A sértetlenség, de még inkább az illetéktelen adatmódosítás kiderítésének biztosítására leginkább kriptografikai hitelesítési eljárásokat lehet alkalmazni, amelyek kódokkal, vagy elektronikus aláírással történnek. De ugyanilyen fontos követelmény a behatolási szándékot érzékelő, és a tényleges behatolás következtében megvalósuló adatmódosítást, adattörlést megelőző műszaki megoldások alkalmazása.⁴⁹
- 7) A személyes adatok bizalmas természetének figyelembe vétele: Egy felhőalapú szolgáltatás használata esetén a titkosítás – ha helyesen alkalmazzák – jelentős mértékben hozzájárulhat a személyes adatok bizalmas kezeléséhez, noha nem teszi visszafordíthatatlanná anonimmá a személyes adatokat. A személyes adatok titkosítását minden olyan esetben alkalmazni kell 'továbbítás közben', amikor 'nyugalomban lévő' adatok is rendelkezésre állnak. Egyes esetekben (pl.: *IaaS* tárolási szolgáltatás) előfordulhat, hogy a felhőszolgáltatás igénybe vevője nem él a szolgáltató által kínált titkosítási megoldással, hanem úgy dönt, hogy a felhőbe történő megküldés előtt, maga titkosítja a személyes adatokat. A nyugalomban lévő adatok titkosítása során különös figyelmet kell fordítani a kriptográfiai kulcs kezelésére, mivel az adatbiztonság végső soron a titkosítási kulcsok bizalmas kezelésétől függ majd. Titkosítani kell továbbá a felhőszolgáltató és az igénybe vevő, valamint az adatközpontok közötti kommunikációt is. A felhő platformjának távolról történő igénybevétele kizárólag biztonságos kommunikációs csatornán keresztül valósulhat meg. Ha az igénybe vevő azt tervezi, hogy nem pusztán tárolja, hanem fel is dolgozza a felhőben tárolt személyes adatokat (pl.: adatok keresése az adatbázisokban), szem előtt kell tartania, hogy az adatok feldolgozása folyamán nem tartható fenn a titkosítás.⁵⁰
- 8) Transzparencia biztosítása: A technikai és szervezési intézkedéseknek az adatkezelés jogszerűsége felülvizsgálatának biztosítása érdekében, támogatniuk kell az eljárások átláthatóságát.⁵¹
- 9) Elkülönítés követelménye (a cél korlátozása): A számítási felhő infrastruktúráján és erőforrásain – így a tárhely, a memória és a hálózatok – tipikusan sok igénybe vevő (felhasználó) osztozik. Ez újabb kockázatokat generál az adatok nyilvánosságra hozatala és jogellenes célokra történő feldolgozása tekintetében. Az 'elkülönítés', mint adatvédelmi cél a jogellenes nyilvánosságra hozatal és adatfelhasználás kiküszöbölésére szolgál, és hozzájárul annak garantálásához, hogy az adatokat ne használják fel az eredeti célkitűzésen túl (célhoz kötött adatkezelés)⁵², továbbá megőrizték azok titkosságát és sértetlenségét.⁵³

48 29-es munkacsoport véleménye i.m. (14. lj.) 16.

49 Uo., 17.

50 Uo.

51 Uo., 18.

52 Vö. 95/46/EK irányelv 6. cikke (1) bekezdésének b) pontja: a személyes adatok gyűjtése csak meghatározott, egyértelmű és törvényes célból történhet, és további feldolgozása nem végezhető e célokkal összeférhetetlen módon. A személyes adatok további feldolgozása történelmi, statisztikai vagy tudományos célokra nem tekinthető összeférhetetlennek, amennyiben a tagállamok biztosítják a megfelelő garanciákat.

53 29-es munkacsoport véleménye i.m. (14. lj.).

- 10) Beavatkozás lehetősége: Az Irányelv biztosítja az érintett számára a hozzáférés, a helyesbítés, a törlés, a zárolás és a tiltakozás jogát.⁵⁴ Az igénybe vevőnek ellenőriznie kell, hogy a felhőszolgáltató nem állít-e technikai és szervezési akadályokat az érintett e jogosultságaiból származó igények teljesítése elé.⁵⁵
- 11) Hordozhatóság biztosítása: Amint arra már fentebb utaltunk, a legtöbb felhőszolgáltató nem alkalmaz olyan szabványos adatformátumokat és olyan szolgáltatási interfészeket, amelyek elősegítik a különböző felhőszolgáltatók közötti átjárhatóságot és hordozhatóságot. Ha a felhőszolgáltatás igénybe vevője úgy dönt, hogy az egyik számítási felhőszolgáltatótól egy másikra tér át, az átjárhatóság hiánya megghiúsíthatja, vagy legalábbis megnehezítheti az igénybe vevő birtokában lévő (személyes) adatok átvitelét az új szolgáltatóhoz (a szolgáltatótól való függőség, az úgynevezett '*vendor lock-in*') Ugyanez igaz azokra a szolgáltatásokra is, amelyet az igénybe vevő az eredeti szolgáltató által biztosított platformon (*PaaS*) alakított ki. A felhőszolgáltatás igénybe vevőjének a szolgáltatás megrendelése előtt ellenőrizni kell, hogy a szolgáltató garantálja-e az adatok és a szolgáltatások hordozhatóságát, és ha igen, akkor milyen módon teszi ezt.⁵⁶
- 12) Elszámoltathatóság: Az elszámoltathatóság informatikai értelemben úgy határozható meg, mint annak a megállapítására való képesség, hogy egy entitás mit, és miként tett egy adott múltbeli időpontban. Az adatvédelem terén ezt a fogalmat gyakran tágabb értelemben, annak a leírására használják, hogy a felek igazolni tudják, hogy megfelelő lépéseket tettek az adatvédelmi elvek érvényesítésének biztosítására. Az IT-elszámoltathatóság különösen fontos a személyes adatok megsértéseinek kivizsgálása terén, hiszen a felhőjogviszonyokban az igénybe vevők, a szolgáltatók (és az alvállalkozó) egyaránt bizonyos mértékben operatív felelősséget viselhetnek. Kiemelkedő jelentőségű ebben a tekintetben, hogy a számítási felhő platformja képes legyen megbízható monitorozási és átfogó naplózási mechanizmusokat biztosítani. Ezenfelül a felhőszolgáltatóknak igazoló dokumentumokat kell szolgáltatniuk azokról a megfelelő és hatékony intézkedésekről, amelyek biztosítják az előbbi szakaszokban körvonalazott adatvédelmi elvek érvényesülését. Példát jelentenek az ilyen intézkedésekre az adatfeldolgozási műveletek azonosítására szolgáló eljárások, a hozzáférés iránti kérelmek megválaszolására szolgáló eljárások, az erőforrások elosztása – ideértve az adatvédelmi előírásoknak való megfelelés megszervezéséért felelős adatvédelmi tisztviselő kijelölését –, vagy a független tanúsítási eljárások. Emellett az adatkezelőknek gondoskodniuk kell arról, hogy az illetékes felügyeleti hatóság kérése esetén, készen álljanak a szükséges intézkedések meghozatalának igazolására.⁵⁷

A fentiekből egyértelműen kitűnik, hogy a felhőalapú szolgáltatás több specifikus adatbiztonsági kockázatot vet fel, így többek között az irányítás/ellenőrzés elvesztését, a nem biztonságos, vagy nem teljeskörű adattörlést, a nem elegendő ellenőrzési nyomvonalat, vagy az elszigetelés megghiúsulását. A korábban részletesen bemutatott – az EU-ban a felhőszolgáltatások

54 Irányelv i.m. (27. lj.) 12. és 14. cikk.

55 29-es munkacsoport véleménye i.m. (14. lj.).

56 Uo., 19.

57 Uo.

A 29-es munkacsoport részletes észrevételeket tett az elszámoltathatóság kérdéséről az elszámoltathatóság elvéről szóló 3/2010. sz. véleményében, ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_hu.pdf.

szabályozására elsőként kidolgozott, harmadik országokba történő adattovábbítás szabályait meghatározó – biztonságos adatkikötő (*Safe Harbor*) mechanizmusban érvényesülő előírások nem kezelik megfelelően ezeket a kockázatokat.

Ezért szükségesnek látszik további adatbiztonsági biztosítékok kiépítése, például olyan harmadik felek szakértelmének és erőforrásainak felhasználásával, akik különféle ellenőrzési, szabványosítási és tanúsítási rendszerek révén meg tudják vizsgálni a felhőszolgáltató megfelelőségét. Az Irányelv 26. cikkében előírt eltérések lehetővé teszik az adatexportőrök számára, hogy további garanciák nyújtása nélkül továbbítsanak adatokat az EU-n kívülre. Ezek az eltérések azonban kizárólag akkor alkalmazhatók, amennyiben az adattovábbítások nem ismétlődőek, tömegesek vagy strukturáltak. Ennek az értelmezésnek az alapján a felhőszolgáltatással kapcsolatosan szinte lehetetlen eltéréseket alkalmazni.

Az Európai Bizottság által elfogadott azon általános szerződési feltételek, amelyek célja két adatkezelő, illetve egy adatkezelő és egy adatfeldolgozó közötti nemzetközi adattovábbítások szabályozása, kétoldalú megközelítésen alapulnak. Amennyiben a számítási felhő-szolgáltatót adatfeldolgozónak tekintjük, a 2010/87/EU bizottsági határozat szerinti mintafeltételek olyan eszközöket jelentenek, amelyeket az adatfeldolgozó és az adatkezelő felhasználhat a felhőalapú számítástechnikai környezet megalapozására, hogy megfelelő biztosítékokat nyújtson a nemzetközi adattovábbítások összefüggésében. A számítási felhő-szolgáltató az általános szerződési feltételek mellett, a gyakorlati tapasztalataira épülő fogyasztói előírásokat is kínálhat, amennyiben azok közvetve vagy közvetlenül nem ellentétesek a Bizottság által jóváhagyott általános szerződési feltételekkel, vagy nem sértik az érintettek alapvető jogait és szabadságait. A vállalatok nem módosíthatják vagy változtathatják meg az általános szerződési feltételeket anélkül, hogy megszűnne a feltételek általános jellege. Ha az adatfeldolgozóként eljáró szolgáltató letelepedett az EU területén, még bonyolultabb helyzet állhat elő, mivel a mintafeltételek általában véve kizárólag az uniós adatkezelőtől a harmadik országbeli adatfeldolgozóhoz történő adattovábbításra vonatkoznak. Ami a harmadik országbeli adatfeldolgozó és az alvállalkozók közötti szerződéses viszonyt illeti, olyan írásbeli megállapodást kell kötni, amely azonos kötelezettségeket határoz meg az alvállalkozó számára a mintafeltételekben szereplő, az adatfeldolgozót terhelő kötelezettségekkel.

A *kötelező erejű vállalati szabályok* a vállalatcsoporton belüli adattovábbítást végző vállalatok magatartási kódexei. A számítási felhő vonatkozásában is létre fog jönni hasonló kódex azokra az esetekre, amikor a szolgáltató adatfeldolgozó, ugyanis a 29. cikk szerinti adatvédelmi munkacsoport jelenleg is az adatfeldolgozókra vonatkozó, kötelező erejű vállalati szabályokon dolgozik, amelyek lehetővé teszik majd az adatkezelők javára történő vállalatcsoporton belüli adattovábbítást anélkül, hogy minden igénybe vevő esetében kötelezővé tennék az adatfeldolgozó és az alvállalkozók közötti szerződések aláírását. Az adatfeldolgozókra vonatkozó ilyen kötelező erejű vállalati szabályok lehetővé teszik, hogy a szolgáltatás igénybe vevője az adatkezelőre bízva a személyes adatait, miközben biztosítékot kap arra nézve, hogy a szolgáltató érdekkörén belül továbbított adatok megfelelő szintű védelemben részesülnek.

4.6. A felhőjogviszony alanyai

A felhőszolgáltatás segítségével végzett adatkezelés, adatfeldolgozás folyamatában több szereplő azonosítható, akiknek jól leírható feladatai, jogai és kötelezettségei vannak. A felhőszer-

zódések egyes szereplőinek feladat- és felelősségi körét a 29-es adatvédelmi munkacsoport is behatóan vizsgálta.

A jogviszonyban a 29-es adatvédelmi munkacsoport által idealizált modellben szerepel a személyes adat érintettje (az a jogalany, akire a személyes adat vonatkozik, akinek az adatát felhőalapú adatkezelés, adattárolás útján kezelik), az adatkezelő (aki valamely jogalapra tekintettel a személyes adatot kezeli) és a felhőszolgáltató (aki a jogviszonyban adatfeldolgozóként jelenik meg). Ebben az összefüggésben szükséges idézni a 29-es munkacsoport adatkezelő és adatfeldolgozó fogalmait tisztázó egy korábbi véleményét, amelyben világossá tette, hogy „[a]z adatkezelő fogalma és annak az adatfeldolgozó fogalmához való viszonya döntő szerepet játszik az Irányelv alkalmazásában, mivel ezek a fogalmak határozzák meg, hogy ki felelős az adatvédelmi szabályok betartásáért, és hogy az érintettek a gyakorlatban hogyan érvényesíthetik a jogaikat. Az adatkezelő fogalma az alkalmazandó nemzeti jog meghatározása (...)”⁵⁸szempontjából is jelentőséggel bír. „[A]z adatkezelő fogalmának első és legfontosabb szerepe annak meghatározása, hogy ki felelős az adatvédelmi szabályok betartásáért, és hogy az érintettek a gyakorlatban hogyan tudják érvényesíteni a jogaikat. Más szóval: a felelősség elosztása.”⁵⁹ Ennek a két kritériumnak a figyelembe vétele elengedhetetlen fontosságú a felhőalapú adatkezelések esetén is.

Az adatkezelő és adatfeldolgozó pozícióját azért kell pontosan meghatározni, hogy egyértelműen meg lehessen határozni a felek adatvédelmi kötelezettségeit, és ezen kötelezettségekükből fakadó felelősségüket. A személyes adatok oltalmának jelentékeny veszélyét okozza egy olyan szabályozási környezet, ahol az érintett alanyi jogát intézményesen védő jogi kötelezettek nem egyértelműen meghatározottak, amiből fakadóan a jogsértésért való felelősség megállapíthatósága kérdésessé válhat. Az Irányelv rendelkezéseiből következik, hogy a felhőszolgáltató mint adatfeldolgozó, felelősséggel tartozik az adatfeldolgozás biztonságáért, azért, hogy az adatfeldolgozás során az adatok integritása ne sérüljön, az adatokhoz illetéktelenek ne férjenek hozzá, azokat ne ismerhessék meg. De amiként már fentebb hivatkoztuk, abban a tekintetben az adatkezelőt terheli a felelősség, hogy olyan adatfeldolgozót bízson meg, amelyik biztosítja ezeket a követelményeket.

Bizonyos esetekben közös adatkezelés valósul meg, hiszen nem kizárt az a lehetőség, hogy a felhőszolgáltató és a szolgáltatást igénybe vevő együttesen közös adatkezelőként jelennek meg a jogviszonyban, példának okáért akkor, amikor a felhőszolgáltató saját célból is végez adatkezelést.

Az Irányelv nem tiltja, hogy a felhőszolgáltató az adatfeldolgozást, vagy annak egy részét (általánosan, vagy egyes műveletek vonatkozásában) kiszervezze, az általa (hatékonyan, rentábilisan) elvégezni nem tudott adatfeldolgozási műveletek elvégzésével alvállalkozót bízson meg. A felhőszolgáltatók a rendkívül nagy adatbázisok és kiterjedt hálózatok önkezü működtetésének terheit csökkentendő, gyakorta szervezik ki az adatfeldolgozási tevékenységüket alvállalkozóknak. Erre az Irányelv ugyan lehetőséget ad, de ennek tényéről és a közreműködő adatfeldolgozók személyéről, köteles tájékoztatni a szolgáltatást igénybe vevő adatkezelőt. A felhőszolgáltató által igénybe vett adatfeldolgozók működésük során kötelesek betartani az adatvédelmi előírásokat és követni az adatkezelő (felhőszolgáltatás igénybe vevőjének) rendelkezéseit.

58 A 29-es adatvédelmi munkacsoport 1/2010. számú véleménye az „adatkezelő” és az „adatfeldolgozó” fogalmáról. ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_hu.pdf.

59 Uo.

Az Irányelv fogalmi rendszerében a felhőszolgáltatást igénybe vevő *adatkezelőnek*, míg a felhőszolgáltató *adatfeldolgozónak* minősül. Az adatkezelő „[a]z a természetes vagy jogi személy, hatóság, intézmény vagy bármely más szerv, amely önállóan vagy másokkal együtt meghatározza a személyes adatok feldolgozásának céljait és módját.”⁶⁰ Aki meghatározza a személyes adatok feldolgozásának célját és módját, mint adatkezelő, felelősséggel tartozik az adatvédelmi jogszabályok betartásáért és mindazoknak a kötelezettségeknek a teljesítéséért, amelyeket az Irányelv, mint az adatkezelőt terhelő kötelezettségként állapít meg. Az adatkezelő szabad döntése, hogy miként intézkedik a személyes adatok feldolgozásáról, miként határozza meg az adatfeldolgozás célját és módját. Ebből fakadóan dönthet úgy, hogy az adatfeldolgozáshoz igénybe vesz felhőszolgáltatót és arról is, hogy az általa meghatározott adatkezelési célok eléréséhez szükséges intézkedések megválasztására a felhőszolgáltatót bízta meg. A felelőssége azonban arra is kiterjed, ha úgy dönt, hogy az adatfeldolgozás egyes mozzanatait vagy egészét felhőalapú szolgáltatás igénybevételével kívánja biztosítani, hogy olyan szolgáltató informatikai megoldását válassza, amely képes biztosítani a megfelelő adatvédelmi szintet.

A felhőszolgáltató az igénybe vevő adatkezelő megbízása alapján bocsátja rendelkezésre a platformot és biztosítja az adatfeldolgozás módját, s mint ilyen, az Irányelv szerint *adatfeldolgozónak* minősül, aki „[s]zemélyes adatokat dolgoz fel az adatkezelő nevében.”⁶¹

Az Irányelv 55. preambulumban bekezdés egyértelművé teszi, hogy amennyiben az adatkezelő nem tartja tiszteletben az érintettek jogait, a nemzeti jogalkotásnak kell gondoskodnia a jogorvoslatról tekintettel arra, hogy a törvénytelen adatfeldolgozás miatt kárt szenvedett személy kártérítését az adatkezelőnek kell állnia. Az adatkezelő akkor mentesül a felelősség alól, ha bizonyítja, hogy a kárért nem ő felelős, különösen, ha megállapítja, hogy az érintett hibás, vagy *vis maior* esete áll fenn, mivel szankciókat kell kiróni minden olyan személyre – függetlenül attól, hogy a magán- vagy a közjog hatálya alá tartozik –, aki nem tesz eleget az Irányelv alapján meghozott nemzeti intézkedéseknek.

A 29-es adatvédelmi munkacsoport 2012. július 1-én elfogadott véleménye részletesen elemzi a felhőszolgáltatások egyes jogi összefüggéseit. A munkacsoport azon túl, hogy átfogó képet kíván nyújtani a felhőszolgáltatások adatvédelmi kérdéseiről, ajánlásokat is megfogalmaz.

A munkacsoport azt az általános, tömegesen előforduló és a fentiekben általunk is elemzett esetet helyezi vizsgálata fókuszába, amelyben az igénybe vevő az EGT-n belüli adatkezelőként, a felhőszolgáltató pedig EGT-n kívüli adatfeldolgozóként jár el, tehát az adattovábbítás, a személyes adatok feldolgozása az Európai Unió határain kívülre, harmadik országba történik. Erre az esetre – az adatkezelőre tekintettel – kiterjed az Irányelv hatálya.⁶²

Az adatkezelés célját mindig az adatkezelő köteles meghatározni és arról az érintettet értesíteni. Az adatkezelő dönt továbbá arról is, hogy az adatkezelési tevékenységet maga végzi, vagy más szervezetnek kiszervezi, és hogy a kiszervezett adatfeldolgozási tevékenységet milyen eszközök, módszerek alkalmazásával kell az adatfeldolgozónak elvégeznie. Arról tehát,

60 29-es munkacsoport véleménye i.m. (14. lj.) 2. cikk d.) pont.

61 Uo., e.) pont. Az Irányelv 2. cikk. b.) pontja az alábbiak szerint határozza meg az adatfeldolgozói tevékenységet: „a személyes adatokon automatikus vagy nem automatikus módon végzett bármely művelet vagy műveletek összessége, azaz gyűjtés, rögzítés, rendszerezés, tárolás, átalakítás vagy megváltoztatás, visszakeresés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel révén, összehangolás vagy összekapcsolás, zárolás, törlés, illetve megsemmisítés.”

62 Amennyiben a felhőszolgáltatás keretében elektronikus hírközlési szolgáltatást nyújtanak, az elektronikus hírközlési adatvédelmi irányelv rendelkezéseit is alkalmazni kell.

hogy a személyes adatok feldolgozása felhőalapú informatikai megoldással valósuljon meg, szintén csak az adatkezelő, a felhőszolgáltatás igénybe vevője jogosult dönteni.

4.7. Felelősség a felhőjogviszonyban

A számítási felhőben számos különböző szereplő vesz részt. Vizsgálandó az egyes szereplők szerepe annak megállapításához, hogy a jelenlegi adatvédelmi jogszabályok tekintetében milyen konkrét kötelezettségek vonatkoznak rájuk, hiszen, ahogy a 29. cikk szerinti adatvédelmi munkacsoport az 'adatkezelő' és az 'adatfeldolgozó' fogalmáról szóló 1/2010. számú véleményében rámutatott, „[a]z adatkezelő fogalmának első és legfontosabb szerepe annak meghatározása, hogy ki felelős az adatvédelmi szabályok betartásáért, és hogy az érintettek a gyakorlatban hogyan tudják érvényesíteni a jogaikat.”

A felhőalapú informatikai szolgáltatás igénybe vevője – amint arra már korábban utaltunk – a személyes adatok vonatkozásában *adatkezelőként* jár el, hiszen meghatározza az adatfeldolgozás végső célját, módját és dönt e feldolgozás kihelyezéséről, valamint a feldolgozási tevékenységek összességének, vagy egy részének külső szervezetre történő átruházásáról. Végső soron az igénybe vevő dönt az adatfeldolgozási műveletek egy részének, vagy egészének konkrét célok érdekében számítási felhő-szolgáltatásokhoz rendeléséről.

4.7.1. Felhőszolgáltatást igénybe vevő adatkezelő felelőssége

Az *adatkezelő* „[a]z a természetes vagy jogi személy, hatóság, intézmény vagy bármely más szerv, amely önállóan vagy másokkal együtt meghatározza a személyes adatok feldolgozásának céljait és módját”. A számítási felhő-szolgáltatás igénybe vevője (adatkezelői mivoltából fakadóan) köteles elfogadni az adatvédelmi jogszabályok betartásáért viselt felelősséget, továbbá felelős az Irányelvben tárgyalt valamennyi jogi kötelezettségért, amelyek őt egyaránt kötelezik. A számítási felhő-szolgáltatás igénybe vevője megbízhatja a számítási felhő-szolgáltatót az adatkezelő céljainak eléréséhez használt módszerek, valamint technikai és szervezési intézkedések megválasztásával. Az adatkezelőnek olyan számítási felhő-szolgáltatót kell választania, aki garantálja az adatvédelmi jogszabályok betartását, és különös hangsúlyt kell helyezni az alkalmazandó szerződések jellemzőire mind a technikai és szervezési intézkedések, a határokon átvívelő adatáramlás, mind pedig olyan további mechanizmusok körében, amelyek alkalmasnak bizonyulhatnak a kellő gondosság és az elszámoltathatóság elősegítésére.

4.7.2. A felhőszolgáltató felelőssége

A *számítási felhő-szolgáltató* számítási felhő-szolgáltatásokat nyújtó szervezet. Amennyiben – a szolgáltatás igénylőjének nevében eljárva – a számítási felhő-szolgáltató biztosítja az adatfeldolgozás módját és a platformját, úgy kell tekinteni, hogy a szolgáltató az adatfeldolgozó, vagyis az Irányelv szerint „[a]z a természetes vagy jogi személy, hatóság, intézmény vagy bármely más szerv, amely személyes adatokat dolgoz fel az adatkezelő nevében”. A számítási felhő-szolgáltató szerepe a vállalkozó és az ügyfél kapcsolatának felel meg. A számítási felhő-

szolgáltatók (mint adatfeldolgozók) feladata a bizalmas kezelés biztosítása, hiszen a 95/46/EK megállapítja, hogy: „[B]ármely, az adatkezelő vagy az adatfeldolgozó meghatalmazásával eljáró személy, beleértve magát az adatfeldolgozót is, aki a személyes adatokhoz hozzáféréssel rendelkezik, kizárólag az adatkezelő utasítása alapján dolgozhatja fel ezeket az adatokat, kivéve, ha erre őt jogszabály kötelezi.” Az adatfeldolgozóknak figyelembe kell venniük a kérdéses számítási felhő típusát (nyilvános, magán, közösségi vagy vegyes / infrastruktúra-, szoftver- vagy platform-szolgáltatás (*IaaS*, *SaaS* vagy *PaaS*), valamint az ügyfél által megrendelt szolgáltatás típusát.

Felelnek továbbá az adatkezelő és az adatfeldolgozó országában alkalmazott uniós jogszabályoknak megfelelő biztonsági intézkedések elfogadásáért is. Az adatfeldolgozónak emellett támogatnia és segítenie kell az adatkezelőt az érintettek és az általuk gyakorolt jogok tiszteletben tartása során.

Előfordulhatnak olyan helyzetek, amikor a számítási felhő-szolgáltató a konkrét körülményektől függően, közös adatkezelőnek vagy saját jogú adatkezelőnek is tekinthető, ilyen helyzet például, amennyiben a szolgáltató a saját céljaira dolgozza fel az adatokat. *Természetes személyek* (felhasználók) a számítási felhő környezetet az Irányelv hatálya alól mentesülve kizárólag személyes vagy háztartási tevékenységek végzése céljából használhatják. Ilyen esetekben alaposan vizsgálendő az úgynevezett háztartási kivétel alkalmazhatósága, amely mentesíti a felhasználókat az adatkezelői minőségtől. Ha a tevékenység ezen kívül esik, akkor a természetes személy is adatkezelőnek tekintendő, az ezzel járó felelősség pedig őt terheli.

4.7.3. *Alvállalkozóért viselt felelősség és az alvállalkozó felelőssége*

A felhőszolgáltatások üzemeltetői az esetek többségében számos, adatfeldolgozóként eljáró szerződő partner bevonásával járnak el. A felhőszolgáltatók ugyanis elsősorban a magas hozzáadott értékkel bíró infrastruktúrát működtetik, de számukra nem minden esetben térül meg az egyes tárhelyeket fenntartani. A tényleges tárolási kapacitások egy részét ezért olyan szerverszolgáltatóknál bérelik, akik főtevékenységként tárhelyek üzemeltetésével foglalkoznak.

Miután az adatfeldolgozók az adattárolásra alvállalkozókkal szerződést kötnek, az utóbbiak hozzáférnek azokhoz a személyes adatokhoz, amelyeket a felhőszolgáltatást igénybe vevő adatkezelők bocsátottak rendelkezésre. A kérdés tehát az, hogy ebben a konstellációban ki és milyen felelősséggel tartozik a jogszerű adatkezelésért? Hogyan vállalhat felelősséget az adatkezelő olyan adatfeldolgozó tevékenységéért, akit nem ő választott ki, és az adatfeldolgozó felhőszolgáltatónak milyen kötelezettségei vannak az adatkezelővel szemben, és mit követelhet meg az alvállalkozójától?

Az adatfeldolgozó tevékenységét olyan szerződésnek vagy más jogi aktusnak kell szabályoznia, amely az adatfeldolgozót az adatkezelővel szemben köti, és amely az adatfeldolgozó vonatkozásában egyéb előírások mellett különösen megköveteli, hogy az adatfeldolgozó másik adatfeldolgozót kizárólag az adatkezelő előzetes engedélyével vegyen igénybe. Ha az adatfeldolgozók alvállalkozásba adják a szolgáltatásokat, kötelesek ezt az információt az igénybe vevő rendelkezésére bocsátani, megjelölve az alvállalkozásba adott szolgáltatás típusát, a meglévő vagy potenciális alvállalkozók jellemzőit és azon további garanciákat, amelyeket az Irányelv betartására vonatkozóan ezek a szervezetek nyújtanak a felhőszolgáltatónak. Ehhez

mértén az alvállalkozókra is alkalmazandó valamennyi vonatkozó kötelezettség a számítási felhő-szolgáltató és az alvállalkozó közötti olyan szerződések révén, amelyek a számítási felhő-szolgáltatás igénybe vevője és a szolgáltató közötti szerződés rendelkezéseit tükrözik.

A 29-es adatvédelmi munkacsoport már többször idézett véleményében megerősítette, hogy az adatfeldolgozó kizárólag az adatkezelő hozzájárulása alapján adhatja alvállalkozásba a személyes adatokkal kapcsolatos tevékenységének egészét, vagy meghatározott mozzanatait. Az adatkezelői hozzájárulás megadásának általános formája, hogy arra a szolgáltatás megkezdését megelőzően, a felhőszolgáltatásban kerül sor. Az adatfeldolgozó köteles tájékoztatni az adatkezelőt az alvállalkozói kört érintő bármely változásról, összetételük megváltoztatásával kapcsolatos bármely tervezett változtatásról, az adatkezelő pedig fenntartja annak lehetőségét, hogy bármikor kifogásolja ezeket a változtatásokat vagy felmondja a szerződést. A felhőszolgáltató köteles valamennyi megbízott alvállalkozót megnevezni. Emellett a számítási felhő-szolgáltató és az alvállalkozó által aláírt szerződésnek tükröznie kell a számítási felhő-szolgáltatás igénybe vevője és a szolgáltató közötti szerződés rendelkezéseit. Az adatkezelőnek képesnek kell lennie arra, hogy az alvállalkozók által okozott szerződésszegések esetén, az egyes szerződéses jogorvoslati lehetőségeket igénybe vegye.

A személyes adatoknak harmadik országbeli adatfeldolgozók részére történő továbbítására vonatkozó, általános szerződési feltételekről szóló 2010. február 5-i bizottsági határozat, elsőként vezetett be egy olyan lehetséges biztosítási modellt, amely alkalmazható az adatfeldolgozók feladatainak és kötelezettségeinek tisztázására az adatfeldolgozás alvállalkozásba adása esetén. E modellben az alvállalkozásba adás kizárólag az adatkezelő előzetes írásbeli hozzájárulása esetén engedélyezett, amennyiben az írásbeli megállapodás az adatfeldolgozó tekintetében meghatározottakkal azonos kötelezettségeket állapít meg az alvállalkozó számára. Amennyiben a további feldolgozó nem tesz eleget az ilyen írásos megállapodásból fakadó adatvédelmi kötelezettségeinek, az adatfeldolgozó továbbra is teljes felelősséggel tartozik az adatkezelő felé a további feldolgozó, e megállapodásból fakadó kötelezettségeinek teljesítéséért. A további feldolgozáshoz szükséges garanciák biztosítása céljából, ilyen rendelkezést alkalmazhatnának az adatkezelő és a számítási felhő-szolgáltató közötti szerződési feltételek között, amennyiben az utóbbi, alvállalkozás révén kívánja nyújtani a szolgáltatásokat.

5. A felhőszolgáltatás, mint tárhelyszolgáltatás

A felhőszolgáltató funkcionálisan egy hálózaton keresztül, lehívással elérhető, adatok tárolására alkalmas, tárolási kapacitáshoz való hozzáférést (végső soron tárhelyet) bocsát a felhasználó rendelkezésére, a szolgáltatás annak igénybe vevője által küldött információ tárolásából áll.⁶³

Ez a tevékenység olyan, az információs társadalommal összefüggő szolgáltatás keretében nyújtott közvetítőszolgáltatás, amely a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem, egyes jogi vonatkozásairól az Európai Parlament és Tanács által elfogadott 2000/31/EK irányelve (a továbbiakban:

63 Vö. Európai Parlament és a Tanács 2000/31/EK irányelve, amely a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem, egyes jogi vonatkozásairól szól („Elektronikus kereskedelemről szóló irányelv”) 14. cikk. (1) bek.

Ekerirányelv) hatálya alá tartozik, és amely „[a] belső piac megfelelő működéséhez kíván hozzájárulni az információs társadalommal összefüggő szolgáltatások tagállamok közötti szabad mozgásának biztosítása által.”⁶⁴

A felhőszolgáltatásnak ebből a szempontból van egy az adatvédelmi szabályozástól különböző, ám jogi szempontból szükségszerűen vizsgálandó aspektusa, éspedig, hogy a felhőszolgáltató, mint az információs társadalommal összefüggő szolgáltatás nyújtója tartozik-e, és ha igen, milyen felelősséggel tartozik az igénybe vevő által a tárolási kapacitásán (szolgáltatása keretében biztosított tárhelyen) elhelyezett, és mások számára elérhetővé tett (jogellenes) tartalomért. Ezek a kérdések természetüknél fogva a publikus, közösségi és a hibrid típusú felhők esetében merülnek fel, hiszen a felelősség szempontjából jelentősége van annak, hogy mások számára hozzáférhető legyen a jogellenes tartalom. A nagy felhőszolgáltatóknak szinte kivétel nélkül vannak olyan közösségi felhő szolgáltatásai, amelyekben a közösség (egy csoport) tagjai tartalmakat tölthetnek fel a közösen látott és használt térbe (megosztás), és e tartalmakat a közösség erre feljogosított tagja, tagjai, vagy akár valamilyen tagja jogosult szerkeszteni (pl: *Google Drive*, *Dropbox*). Amennyiben a felhasználó ún. megosztott mappát hoz létre, megteremtí a lehetőségét, hogy azok a személyek, akikkel azt megosztotta, a mappa tartalmában bekövetkező változásokat folyamatosan nyomon követhessék. Ez a jogellenes tartalmak esetében azt jelenti, hogy az mások számára hozzáférhetővé, ezáltal érzékelhetővé válik.⁶⁵

Az Ekerirányelv a tagállamok kötelezettségévé teszi az olyan jogi szabályozás megalkotását, amely lehetővé teszi, hogy a tárhelyszolgáltatók vonatkozásában meghatározott feltételek teljesülése esetén, a szolgáltatót ne terhelje felelősség a szolgáltatás igénybe vevőjének kérésére tárolt információért. Az Ekerirányelv két diszjunktív feltétel teljesülése esetén mentesíti a felelősség alól a szolgáltatót:

- a) a szolgáltatónak nincs tényleges tudomása jogellenes tevékenységről vagy információról, és – ami a kárigényeket illeti – nincs tudomása olyan tényekről vagy körülményekről, amelyek nyilvánvalóan jogellenes tevékenységre vagy információra utalnának; vagy
- b) a szolgáltató, amint ilyenről tudomást szerzett, haladéktalanul intézkedik az információ eltávolításáról, vagy az ahhoz való hozzáférés megszüntetéséről.

A tárolt információk, adatokért/tartalomért való felelősség kérdése különösen akkor vetődhet fel, amikor az igénybe vevő adatkezelő a felhőszolgáltató adatfeldolgozási tevékenységét felhasználva tölt fel és tesz közzé (másokkal megoszt) egy nyilvános, vagy közösségi felhőben jogellenes tartalmakat. Az Ekerirányelv iránymutatását követve az Ekertv. is rögzíti, hogy meghatározott feltételek esetén „[a] közvetítő szolgáltató a más által rendelkezésére bocsátott, a közvetítő szolgáltató által nyújtott, információs társadalommal összefüggő szolgáltatással továbbított, tárolt vagy hozzáférhető tett információért (...) nem felel”. A közvetítő szolgáltató nem köteles ellenőrizni az általa csak továbbított, tárolt, hozzáférhetővé tett információt, továbbá nem köteles olyan tényeket vagy körülményeket keresni, amelyek jogellenes tevékenység folytatására utalnak” (előzetes ellenőrzés hiánya).

Amennyiben tehát nem végez tartalomszerkesztési tevékenységet, csupán a mások által szerkesztett tartalmak közzétételére biztosít zártkörű, vagy nyílt fórumot (tárhelyet), úgy a

⁶⁴ Uo., 1. cikk (1) bek.

⁶⁵ Néhány esetben elegendő a tartalom közzététele, más esetekben szükséges lehet a mások általi tényleges érzékelés is.

tartalom jogellenessége esetén, az azzal való tényleges kapcsolata hiányában szerkesztői típusú felelősséggel nem, egy szűk körű, objektív alapú helytállási kötelezettséggel (a tartalom eltávolításának kötelezettségével) azonban rendelkezhet.

A felhőszolgáltató általános nyomon követési és ellenőrzési kötelezettségének hiánya akkor válik igazán fontossá, amikor egy, a tárhelyszolgáltatását igénybe vevő felhasználó (adatkezelő) jogellenes tartalmat tesz közzé, vagy jogellenes módon kezel személyes adatokat, példának okáért nem rendelkezik az érintett hozzájárulásával. De nem csupán adatvédelmi jogi példa hozható fel, említhetnők azt az esetet is, amikor egy közösségi, vagy nyilvános tárhely esetében az igénybe vevő személyiségi jogot sértő tartalmat tesz közzé, vagy szerzői jogot sértő tartalmat oszt meg a felhőben. Ezekben az esetekben a felhőszolgáltató nem szükségszerűen van a jogellenesség tudatában, hiszen nem köteles azt vizsgálni, így a felelőssége megállapíthatóságának körében erre tekintettel kell lenni.

A felhőszolgáltatónak a fentiek összegzéseként tehát rögzíthető, hogy nincs általános nyomonkövetési kötelezettsége, nem köteles monitorozni a tárhelyén elhelyezett tartalmak jogszerűségét, azonban a jogellenességről való tudomásszerzést követően, köteles haladéktalanul eltávolítani a kérdéses tartalmat. A felhőszolgáltatót tehát, mint klasszikus tárhelyszolgáltatót terheli az értesítési és eltávolítási eljárásban a közvetítőszolgáltatóra előírt kötelezettség. Amennyiben az értesítést követően nem tesz eleget eltávolítási kötelezettségének, úgy nem mentesül a felelősségre vonhatóság alól. Ez valójában nem felelősség, hanem kimentést nem engedő helytállási kötelezettség, de csak abban az esetben áll fenn, amennyiben az előzetes értesítést követően nem tesz eleget e felhőszolgáltató eltávolítási kötelezettségének.

A felhő technológia hatékonysága azonban többek között éppen abban manifesztálódik, hogy a felhőtárhelyen elhelyezett, sokszor ugyanazon tartalmakat (pl. sokak által ugyanazon szolgáltató tárhelyén feltöltött azonos zeneszámokat) a felhőszolgáltató nem többszörözi, a publikus vagy szolgáltató által biztosított tartalomból kizárólag egy-egy másolati példányban tárolja, és a felhasználók igénye szerint ezt az egy példányt bocsátja újra és újra rendelkezésre. Ez a tárolási technika azonban a felhőben tárolt tartalmak differenciálását és elemzését követeli meg. A szolgáltató hatékonyságának növelése céljából nyilvánvalóan behatóan vizsgálja a tárhelyen elhelyezett tartalmakat, és azok redundanciája esetén, a duplumokat (és minden további másolatot) törli, s csupán egy fájlt tart rendelkezésre, hogy azt a felhasználó bárhol és bármikor elérhesse.⁶⁶

Az ilyen jellegű felhőszolgáltatások, tehát amikor a szolgáltató az egyes tartalmak egyezőségét vizsgálja, és azok között szelektál, már nyilvánvalóan nem sorolhatók be az egyszerű tárhelyszolgáltatások közé, de nem is érik el a tartalomszerkesztői tevékenység intenzitását.⁶⁷

6. Epilógus

A felhőalapú informatikai adattárolásra szolgáló megoldások az elmúlt évtized egyik legnagyobb informatikai újításai voltak. A felhő-technológia azonban még kétségkívül nem érte el

66 Vö. GRAD-GYENGE Anikó – FALUDI Gábor: A cloud computing-alapú szolgáltatások szerzői jogi megítéléséről. *Infokommunikációs és Jog*, 2012/3. 107.

67 Uo.

fejlődésének csúcspontját, dinamikus fejlődése töretlennek látszik. Ez a töretlen és sok tekintetben egyre gyorsuló fejlődés a jogi szabályozás elé újabb és újabb feladatokat állít.

Számos jogág összehangolt, megfontolt és sok esetben innovatív megoldásai szükségesek a felhőszolgáltatások megnyugtató működésének biztosításához – lokálisan, de főleg globálisan. A szolgáltatás globális jellege ugyanis megköveteli a minél szélesebb nemzetközi együttműködést. Magunk is bemutattunk ígéretes eredményeket, mind regionális szinten (EU), mind pedig nagy jogrendszerek közötti együttműködést példázó egyezményeken keresztül. Számunkra Európában egy jól működő, az Európai Unió által megteremtett intézményi garanciarendszer jelenthet megnyugtató megoldást, azzal, hogy elengedhetetlen a globális szolgáltatóknak rendszerint otthont adó Egyesült Államokkal való hatékony, transzparens, jogi garanciákkal megtámogatott és kikényszeríthető együttműködési mechanizmus fenntartása. Erre jó reményt nyújt a *Privacy Shield* rendszere.⁶⁸

A technológia jogi válaszokat generáló fejlődése – amiként pár sorral feljebb már írtuk – nem állt meg, a jogtudománynak és a jogalkotásnak még bőséggel maradt feladata a felhőszolgáltatásokkal kapcsolatban.

68 A kézirat lezárását követően jelent meg a *Privacy Shield* működésének első éves felülvizsgálatról szóló dokumentum, ezért annak feldolgozására már nem kerülhetett sor, l. Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU–U.S. Privacy Shield {SWD(2017) 344. Brussels, 18.10.2017. COM(2017) 611 final. final}.

A cybercrime, mint infokommunikációs jogi probléma

KLEIN TAMÁS – SZABÓ ALIZ*

1. Néhány előkérdés

Az információs társadalom egyik legnyilvánvalóbb jelensége (folyamatainak serkentője és egyúttal következménye is) az internetes kommunikációs tér megjelenése, szélesedése. Az online kommunikáció mellett, hogy a nyilvánosság szerkezetének jelentékeny átalakulását idézte elő, új kommunikációs terek, platformok kialakulásához vezetett, számos jogilag releváns, a jogalkotók és jogalkalmazók által megválaszolandó kérdést is generált.

Az online nyilvánosság kialakulásával együtt járó társadalmi jelenségek a jogtudomány számára is sok szempontú vizsgálódásra adnak lehetőséget. Az internetes nyilvánosság egyik jelentős aspektusát képezik azok az online magatartások, amelyek valamilyen szempontból jogellenesek. A jogellenes online tevékenységek közül is egy jól karakterizálható, ugyanakkor meglehetősen heterogén jellegű csoportot képeznek azok a cselekmények, amelyek a jogi felelősség és különösen a felelősségre vonás szempontjából kizárólag az *ultima ratio*val – büntetőjogi eszközökkel, a jogrendszer szankciós zárkövének segítségével – lehet hatékonyan küzdeni. Ezeket az online jogellenes magatartások közül társadalmi, vagy egyéni következményeik miatt büntetőjogi szankcióval fenyegetett (és többnyire nemzetközi dokumentumokban azonosított) cselekményeket, a jogirodalom összefoglaló néven *cybercrime* cselekményeknek nevezi. Ezeket a cselekményeket a nemzetközi büntetőjogszabályok legújabb módosításai során a nemzetközi jogalkotók pönalizálták és irántuk intenzív érdeklődéssel fordultak a bűnügyi tudományok, köztük a büntetőjog-tudomány is.

A *cybercrime* ugyanakkor lényegesen sokrétűbb, mint kizárólag a büntetőjogi vizsgálódásra leszűkíthető tárgy. Vitathatatlanul van jelentősége a büntetőjogi dogmatikának, a büntetőjog-tudomány dogmatikája által kiértékelt felelősségtannak, de álláspontunk szerint más szempontú elemzésnek is helye van. Ilyen lehet a *cyberbűnözés* információtechnológiai elemzése, amelyhez ez a tanulmány pár alapvető szempontot kíván adni. Előre bocsátjuk, hogy tanulmányunk módszertana kifejezetten kerüli a büntetőjogi elemzést, a büntetőjogi dogmatikai kérdéseket, helyette hangsúlyozottan az infokommunikációs jog perspektívájából jelentékeny összefüggésre kívánjuk felhívni a figyelmet – a teljesség igénye nélkül. Mindazonáltal vannak olyan büntetőjogi kérdések, amelyek a vizsgálati tárgy okán nem kerülhetők meg, azokra röviden kitérünk.

Az online nyilvánosságban megvalósuló cselekmények különböző jogágak szabályozása alá tartoznak, ebből fakadóan a felelősség kérdése is változatos szempontrendszerben vizsgálható, hiszen a cybertérben megvalósuló jogellenes cselekmények nem kizárólag büntetőjogi dogmatika által leírható bűncselekményt valósítanak meg.¹

* A társszerző Szabó Aliz joghallgató, Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar Infokommunikációs Jogi Tanszéke.

1 Vö. DOMOKOS Andrea: Internetes bűnözés. In: TÓTH András (szerk.): *Technológia jog – Új globális technológiák jogi kihívásai*. Budapest, KRE ÁJK, 2016. 251 – 260.

Az ilyen büntetőjogilag releváns bűncselekmények csoportosítását több szerző is elvégezte,² e bevezetésben a Szabó Imre általi felosztást szeretnénk kiemelni.³ Szabó Imre szerint a számítógép három lényegi összetevője a szoftver, a hardver és az egészet működtető ember, a 'menver' (*manware*)⁴. A számítógép lehet a bűncselekmény tárgya (ha valamely hagyományos büntetőjogi tényállás megvalósításához használják) és eszköze (pl. számítógépalkatrész-gyárakban elkövetett lopások elkövetési tárgya) is. Szabó Imre két kategóriába sorolja a *cybercrime* cselekményeket: az egyik kategóriát a számítógéppel kapcsolatos bűncselekmények, a másikat az interneten elkövethető bűncselekmények adják.

A büntetendő számítógépes cselekmények körébe tartozik az információlopás⁵, a számítógépes szabotázs⁶, az adatok tisztességtelen megváltoztatása vagy manipulálása⁷, a jogosulatlan használat⁸, valamint a jogosulatlan hozzáférés^{9,10}. Az internetes bűncselekményeket Szabó Imre további két kategóriába sorolja, az első kategóriát az internet mint hálózat ellen megvalósuló bűncselekmények adják, a másodikat pedig az interneten előforduló jogtalan cselekmények¹¹. Az internet, mint hálózat ellen megvalósuló bűncselekmények a következők: kommunikációs csatornák kikémlelése, számítógépbe és számítástechnikai rendszerekbe történő jogosulatlan belépés, hálózati működés szabotálása, adatok szándékos megváltoztatása és megsemmisítése, számítógépes hálózatokban történő jogosulatlan szándékos bennmaradás. Az interneten előforduló jogtalan cselekmények körébe az internetes csalás, kábítószerek és állami ellenőrzés alá vont szerek internetes kereskedelme, fegyverek internetes kereskedelme, internetes szerencsejáték, alkohol internetes kereskedelme, online gyermekpornográfia, szoftveralkalmazkodás, illetve a szerzői és szomszédos jogok megsértése tartozik.¹²

Nemzetközi kitekintésben igen tanulságos lehet pár olyan minta, amelyet az Egyesült Államok már működtet saját jogrendszerében.¹³ Az informatikai bűncselekmények őshazája az Egyesült Államok, amely az elsők között ismerte fel azt, hogy az információtechnológiai

2 L. 2.2. A számítógépes bűncselekmények csoportosítása.

3 Vö. DERES Petronella: Internetes bűnözés. In: TÓTH András (szerk.): *Technológia jog – Új globális technológiák jogi kihívásai*. Budapest, KRE ÁJK, 2016. 143 – 249.

4 SZABÓ Imre: Internetes bűncselekmények, különös tekintettel az internetes csalásra. www.ajk.elte.hu/file/SzaboImre-InternetesBuncselekmények.pdf.

5 A számítógépes adatok, programok bevitele, módosítása, törlése vagy elmentése, jogtalan vagyoni eszközök vagy más értékek megszerzése céljából.

6 A számítógépes adatok, programok bevitelét, módosítását, törlését vagy elmentését, vagy a számítógépbe történő bármely más beavatkozást jelent abból a célból, hogy a számítógépes vagy telekommunikációs rendszerek funkcióit megakadályozzák.

7 A számítógépes adatok, programok bevitelét, módosítását, törlését vagy elmentését jelenti hamisítás céljából.

8 A védett számítógépes programok tulajdonosai exkluzív jogainak megsértését jelenti a program jogosulatlan hasznosítása vagy forgalomba hozatala révén.

9 A számítógépes vagy telekommunikációs rendszerbe az arra jogosult engedélye nélkül, vagy a biztonsági intézkedések megsértésével, vagy más tisztességtelen vagy bűnös szándékkal történő belépést vagy annak lehallgatását jelenti.

10 OECD Computer-Related Criminality: Analysis of Legal Police. Paris, 1986.

11 SZABÓ i. m. (4. lj.) 14.

12 Uo.

13 A magyar irodalomban erről lásd Sorbán Kinga munkáit: SORBÁN Kinga: Az informatikai bűncselekmények elleni fellépés az Egyesült Királyságban, In: KERESZTES Gábor (szerk.): *Tavaszi Szél 2015 / Spring Wind 2015 Konferenciakötet: I. kötet*. Budapest, Doktoranduszok Országos Szövetsége, 2015. 339-355. SORBÁN Kinga: Informatikai bűncselekmények és nyomozásuk az Egyesült Királyságban. *Belügyi Szemle*, 2010/9. 48-68. SORBÁN Kinga: Az informatikai bűncselekmények elleni fellépés nemzetközi dimenziói. *Themis*, 2015. június 343-375. SORBÁN Kinga: Az informatikai bűncselekmények elleni fellépés az Egyesült Államokban. I *Themis*, 2016. június. 150-170.

eszközök fejlődése és a széles rétegek számára való elérhetősége a számtalan lehetőség mellett veszélyforrásokat is rejt magában.¹⁴ Mivel

„[a]z Egyesült Államokban szövetségi rendszer működik, ezért az informatikai bűncselekmények szabályozása is kétszintű: a szövetségi informatikai büntetőjog egységes, mindent magába foglaló rendszer, annak területi hatálya az Amerikai Egyesült Államok teljes területére kiterjed, az állami informatikai büntetőjog azonban mindenhol eltérő, mind az 50 szövetségi állam (valamint a kolumbiai körzet) informatikai büntetőjoga csak az adott állam területén érvényes.”¹⁵

A szövetségi szintű fellépésre koncentrálva, említést kell tennünk a Nemzeti Kiberbiztonsági és Kommunikációs Integrációs Központ (*National Cybersecurity and Communications Integration Center*), a Titkosszolgálaton belül működő Elektronikus Bűncselekmények Elleni Munkacsoportok (*Electronic Crimes Task Force*), valamint a Szövetségi Nyomozóirodán belül működő kiberbűnözési egységek (*Cyber Task Force*) munkájáról. A rendvédelmi feladatok az Egyesült Államokban tagállami és szövetségi szint között oszlanak meg¹⁶. Tagállami szinten beszélhetünk továbbá a helyi (önkormányzati vagy városi rendőrség), a megyei (seriff) valamint az állami szint között¹⁷. A kiberbűncselekmények felderítése és nyomozása szempontjából kiemelkedő jelentőséggel bírnak a már említett szövetségi rendvédelmi szervek, úgymint a Nemzeti Kiberbiztonsági és Kommunikációs Integrációs Központ¹⁸, amelynek fő célja a kártékony kibertevékenységek helyzetére vonatkozó információk megosztásának elősegítése (ennek érdekében napi 24 órában üzemelő eseménykezelő és tudatosság növelő központként funkcionálnak); a Titkosszolgálat által működtetett 39 Elektronikus Bűncselekmények Munkacsoport (*ECTF*), melyek célja az elektronikus bűncselekmények megelőzése, felderítése és nyomozása, beleértve a kritikus infrastruktúrák és fizetési rendszerek elleni terrorista támadásokat; s nem utolsósorban a Szövetségi Nyomozóirodán belül működő kiberbűnözési egységek (*Cyber Task Force*)¹⁹. Utóbbiak a Szövetségi Nyomozó Iroda 56 területi irodája mellett működnek, céljuk, hogy összehangolják a kiberbiztonság területén a helyi és a szövetségi szintű fellépést.

Reagálnak az egyes incidensekre és sértett-alapú nyomozásokat folytatnak, ezen felül feltérképezik és kezelik a fenyegetéseket, sérülékenységeket, valamint kapcsolatot tartanak a fontosabb vállalatokkal, közintézményekkel és egyéb szereplőkkel²⁰. Megállapíthatjuk, hogy az Egyesült Államokban mind az informatikai bűncselekmények szabályozása, mind pedig az informatikai bűncselekmények megelőzése és a velük szemben való fellépés jóval részletesebben szabályozott, mint hazánkban, melyet az Egyesült Államokban kialakult többszintű szabályozás, valamint a tényállások nagy száma és összetettsége is indokolhat²¹.

14 SORBÁN Kinga: Az informatikai bűncselekmények elleni fellépés az Egyesült Államokban. I *Themis*, 2016. június. 150. www.ajk.elte.hu/file/THEMIS_2016_jun.pdf.

15 Eoghan CASEY: *Digital Evidence and Computer Crime*. Third Edition. Academic Press, 2011.85.

16 SORBÁN i.m. (14. lj.) 166.

17 Uo.

18 A Központ 4 nagyobb szervezeti egységre tagozódik, a Műveleti és Integrációs Egységre, a Titkosszolgálatra, a Bevándorlási és Vámhatóság Belbiztonsági Nyomozó hivatalára, valamint a Szövetségi Nyomozóirodára.

19 SORBÁN i.m. (14. lj.) 166.

20 Uo., 167.

21 Uo., 169.

A gyors technikai fejlődés, az informatika kiteljesedése és a hálózatok elterjedése következtében, a számítástechnika árnyoldalának tartott számítógépes bűnözés²² mára világméretűvé nőtte ki magát. A modern technika vívmányainak használatával, számos bűncselekmény informatikai úton is megvalósíthatóvá vált. Napjainkban bárki játszi könnyedséggel lehet elkövető és áldozat egyszerre, akár legjobb tudomása nélkül is, ezért elengedhetetlen a megfelelő védelmi stratégia felállítása. Ennek megalapozásához viszont először magát a jelenséget kell körbejárni, annak fényében, hogy a védekezés mind emberileg, mind szakmailag nemzeti és nemzetközi együttműködést kíván. A számítógépes bűnözés történeti fejlődésének prezentálása után, a Számítástechnikai Bűnözésről Szóló Egyezmény²³ (a továbbiakban: Cybercrime-Egyezmény) szemléltetésével és újragondolásával, a kibertámadások elleni szervezettebb prevenció szükségességére világítunk rá. A *cybercrime*-szabályozás lehetséges irányvonalainak bemutatására törekszünk a kiberbiztonsági stratégiák és az uniós jogforrások részletezésével, ennek okán kutatómunkánk során mind a hatályos Büntető Törvénykönyv rendelkezéseire, mind a *cybercrime*-ot specifikusan szabályozó jogszabályokra nagy hangsúlyt fektettünk.

Arra szeretnénk rámutatni, hogy milyen pozitív eredményekkel járhat, ha e két szélsőséges szemlélet egyes elemeit összefésüljük. A számítógépes bűnözési formák ismertetésekor az azok elleni védekezési formákat is részletezzük annak érdekében, hogy életszerű segítséget nyújtsunk egy lehetséges deviáns magatartás leküzdésében mind a felnőtt korosztály, mind a fiatalkorúak számára. Kiemelten vizsgáljuk az adathalászatot, melyre egy új szabályozási koncepciót is felépítünk. A 2018-tól hatályba lépő uniós adatvédelmi szabályozást, a GDPR²⁴-t is elemezzük, majd reflektálunk a rendeletre. Végül, a deviáns cselekmények hétköznapi értelmezésének elősegítésére áttekintettük Cameron S. D. Brown információs biztonsági szakértő 2015-ben befejezett, *Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice*²⁵ címmel megjelent tanulmányát, nem csupán annak kiemelkedő aktualitása miatt, hanem mert véleményünk szerint kifejezetten új, laikusok számára is jól érthető oldaláról vizsgálja ezt az egészen mai, rendkívül aktuális és kardinális problémát.

2. A cybercrime fogalmi kérdései

A definíció meghatározása előtt szükséges tisztázni, hogy a *cybercrime* még nem rendelkezik egységes, a szakirodalom által elfogadott definícióval. Ennek fő indoka az, hogy a jelenség rendkívül sokszínű és változékony, így könnyen lehet, hogy egy választott címszó nem fedné le annak teljes és valós tartalmát. Fontosnak tartjuk megjegyezni, hogy az elmúlt évtizedekben számos definiálási kísérlet zajlott, így most az általunk legkiemelkedőbbnek vélt két fogalom-meghatározást említjük meg. Az Európa Tanács 1989-ben elkészítette 9. számú ajánlását a számítógéppel kapcsolatos bűncselekményekről, melyben az Európa Tanács által felállított szakértői testület kerüli a számítógépes bűncselekmény fogalomszintű meghatározását, helyette az eddig ismert, online környezetben megvalósítható deliktumokat vezeti listákra. A

22 L. 2. A *cybercrime* fogalmi kérdései.

23 Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezménye. (a továbbiakban: Cybercrime-Egyezmény).

24 General Data Protection Regulation.

25 L. 10. Mary esete a kiberbűnözéssel.

tanácsi javaslat egy minimum és egy fakultatív listát is tartalmaz. A minimum lista szereplői a számítógépes csalás, a számítógépes hamisítás, a számítógépes adatokban és programokban történő károkozás, a számítógépes szabotázs, a jogellenes behatolás, a jogellenes titokszerzés, a védett számítógépes programok jogellenes másolása és a félvezető topográfiák jogellenes másolása. A fakultatív lista négy eleme a számítógépes adatok és programok megváltoztatása, a számítógépes kémkedés, a számítógép jogellenes használata és a védett programok jogellenes használata. Ettől eltérően, Kunos Imre 1999-es, a Belügyi Szemlében megjelent tanulmányában²⁶ a számítógépes bűnözést azon bűncselekmények összességéként definiálja,²⁷ melyek esetén információtechnológiai eszközöket, rendszereket használnak a bűncselekmények elkövetésének eszközeként. Ez utóbbi fogalom ma is irányadó lehet azzal a kiegészítéssel, hogy a számítógép ma már nem csupán eszköz, hanem az internet segítségével az elkövetés helye is lehet. A *cybercrime* megjelenése az információtovábbítási eszközöknek köszönhető, így annak definíciója is e körben értelmezhető csupán.

2.1. A jelenség első kutatói

Hazánkban először Polt Péter hívta fel a figyelmet a virtuális kriminalitás létezésére és fontosságára 1983-as, *A számítógépes bűnözés* címmel a Belügyi Szemlében megjelent értekezésével²⁸, az Országos Kriminológiai és Kriminalisztikai Intézet (OKRI) munkatársaként. Az 1980-as évek végén fogott a *cybercrime* tanulmányozásához Pusztai László²⁹ jogtudós is, aki számos tanulmánnyal gyarapította tudásunkat a kiberbűnözésről, melyek közül az első igazán átfogó műve *A számítógép és bűnözés* címmel³⁰ jelent meg 1989-ben. Kutatásai során rendszerbe foglalta a korabeli számítástechnikai bűncselekményeket, számba vette a számítógépes bűnözés közös jellemzőit és rávilágított a jövőbeli tendenciákra is. További tudományos munkásságáról gazdag bibliográfiája árulkodik.

2.2. A számítógépes bűncselekmények csoportosítása

Pusztai László *a Számítógép és bűnözésben* négy alaptípusát különböztette meg az internetes bűncselekményeknek: a számítógépes visszaélést, az adatkikémlelést, a számítógépes szabotázst és a gépidőlopást. Tíz évvel később, a számítógépes bűncselekmények kodifikációjáról szóló tanulmányában³¹ Nagy Zoltán András hasonló kategóriákat határozott meg. Eric Himpton Horder, Jr. amerikai ügyvéd szerint három csoportba sorolhatók a számítógépes bűncselekmények: az első csoportba a számítógép, mint szoftver és hardver együttese ellen irányuló bűncselekmények tartoznak, a második csoportot azok a bűncselekmények adják,

26 KUNOS Imre: A számítógépes bűnözés. A modern információtechnológia felhasználása a bűnözésben. *Belügyi Szemle*, 1999, 47. évf. 11. szám. 28–42.

27 Uo., 28.

28 POLT Péter: A számítógépes bűnözés. *Belügyi Szemle*, 1983, 21. évf. 6. szám, 60–64.

29 Az OKRI igazgatója, valamint az Országos Bűnmegelőzési Tanács első elnöke volt.

30 PUSZTAI László: Számítógép és bűnözés. In: Gödöny József (szerk.): *Kriminológiai és kriminalisztikai tanulmányok*. 1989, 26. kötet, 85–146.

31 NAGY Zoltán András: *Bűncselekmények számítógépes környezetben*. Budapest, Ad Librum, 2009. 5–6.

melyeknél a számítógép médiumként az elkövetés eszközeként szolgál (számítógépes csalás, szerzői vagy szomszédos jogi jogsértések, illegális termékek vagy szolgáltatások online értékesítése, online zaklatás), a harmadikat pedig azok a tényállások teszik ki, amelyeknél a számítógép, mint tároló eszköz jelenik meg, amelyen lévő adatok bizonyítékként szolgálhatnak valamilyen más deliktumhoz. Szabó Imre két kategóriába sorolja a bűncselekményeket³²: az egyik kategóriát az internet, mint hálózat ellen megvalósuló bűncselekmények adják, a másikat pedig az interneten megvalósuló jogtalan cselekmények. Lényegesnek tartja az utóbbi csoport további kettéosztását, mivel az interneten hozzáférhetőek olyan adatbázisok, melyek esetleges elkövetési magatartások bizonyítékai lehetnek, s ezek kizárólag a személyiségi jogok korlátozásával lennének hozzáférhetőek. A technológia személyiségi jogi és szerzői jogi jogsértések elkövetését is lehetővé teszi, de ezek nem kerülnek kifejtésre a dolgozatban. Marjie T. Britz³³ a 2013-ban, *Computer Forensics and Cyber Crime: An Introduction* címmel megjelent könyvében az informatikai bűncselekményekkel kapcsolatban négy fogalmat azonosít; Szabó Imréhez hasonlóan megkülönbözteti a számítógépes, illetve a számítógéppel kapcsolatos bűncselekmény kategóriáját, illetve új fogalmakként említi a digitális bűncselekményt és a kiberbűncselekményt is. A digitális bűncselekmény-fogalmat minden olyan cselekményre használja, mely magában foglalja az elektronikusan tárolt adathoz való jogosulatlan hozzáférést, terjesztést, annak manipulálását, megsemmisítését vagy megmásítását.

A kiberbűncselekmények Marjie szerint olyan számítógépes rendszerekkel vagy internetre csatlakoztatott számítógépekkel való visszaéléseket ölelnek fel, melyek közvetlenül vagy járulékosan veszteségeket okoznak. Úgy gondoljuk, hogy a digitális bűncselekmények és a kiberbűncselekmények új fogalmakként való bevezetése lényegesen fontos mind a hazai, mind a nemzetközi jogban, a technológiai változások előidézték ezek szükségességét. Mivel azonban sok az átfedés e két kategória között (hogy egy példát említsünk: az adathalászat e csoportosítás szerint több fogalomkörbe is sorolható lenne), így szükségesnek tartjuk a két kategóriát egymással párhuzamba állítva vizsgálni, s ehhez mérten az így kialakuló vizsgálati eredményekre alapozva a fogalmakat pontosítani.

3. A számítógépes bűnözés történeti fejlődése

A számítógép egészen annak 1880-as feltalálása óta szolgál eszközként a virtuális bűnözéshez, így fontosnak tartjuk e kettő megszületésének történeti jelentőségű fordulópontjait egymással párhuzamba állítva taglalni. Az első modern komputer alapelveit Charles Babbage tudós dolgozta ki az angol kormány megbízásából, egyes források szerint Sir Humphrey Davyhez írt levelében.³⁴ Valamivel később, 1886-ban Herman Hollerith német származású amerikai feltaláló megépítette az első lyukkártya-feldolgozó gépet, melyet elektronikus számlálásra lehetett felhasználni, így azt a célt szolgálta, hogy az 1880-as népszámlálás adatait feldolgozza. A találmány nemcsak az USA-ban, de Európában is nagy sikert aratott, a statisztikai felmérések kedvelt eszköze lett. 1939-re Konrad Zuse német mérnök történelmet írva elkészítette az

32 SZABÓ i.m. (4. lj.) 301–324.

33 A Clemson University (USA) büntetőjogi professzora.

34 CHARLES BABBAGE to Sir Humphrey DAVY, July 3, 1822.; MORRISON and MORRISON: *Charles Babbage and His Calculating Engines*. Dover Publications Inc., 1961. 305.

első, jelfogókkal működő számítógépet, a Z1-et. 1945-ig további prototípusokat³⁵ készített, így született meg az első kereskedelmi forgalomba került digitális számítógép³⁶ is. A fejlődés további lényeges állomásaként megemlítenénk még a Mark 1-est, az első nulladik generációs, valamint az ENIAC-ot, az első elektroncsöves, első generációs készülékeket is. Később, a tranzisztorok alkalmazásával létrejöttek második generációs gépezetek is, melyek által az eszközök mérete és energiafogyasztása is jelentősen csökkent.

Az 1970-es évektől egészen napjainkig a számítógépek negyedik generációjáról beszélhetünk, melyek nagy integráltságúak, magas szintű nyelveken írják programjaikat és microprocesszorokkal működnek. Az ötödik generációs, mesterséges intelligenciával működő számítógépek fejlesztése kezdeti stádiumban van, így megjelenésük a jövő záloga.

3.1. Az első számítógépes bűncselekmények

A számítógépeket már a kezdetekben is felhasználták csalásokhoz és adatállományok manipulálására, majd az első vírusok, trójai programok táptalajává váltak, melyeket főként károkozásra, információszerezésre hoztak létre. 1959-ben a Walston and Co. alelnöke hamis lyukkártyák segítségével 250000 dollárt sikkasztott, ám ez az eset akkoriban még kivételnek számított, így a tudományos élet és a nyomozó hatóságok nem tulajdonítottak különösebb jelentőséget a jelenségnek. Az integrált áramkör feltalálásával Jack S. Kilby³⁷ 1958-ban a harmadik generációs számítógépek tömegtermelését aktivizálta. 1963 és 1974 között az Equity Funding Corporation cég munkavállalói a szervezet készülékeit használva, hamis kötvényeket készítettek fiktív kifizetések céljából, így 2 000 000 dollárt csaltak ki a vállalkozásból. Tettük olyan volumenű bűncselekmény-sorozatot eredményezett, melyet a Guinness Rekordok könyve is számon tart. A nyolcvanas évek elején megjelent az FBI számítógépes csalásról szóló jelentése, melyből kiderült, hogy míg egy átlagos fegyveres rablás alatt körülbelül 10 000 dollárt zsákmányoltak az elkövetők, addig egyetlen virtuális bűntettükkel ennek az összegnek akár a százszorosát is megkereshették. Magyarországon 2006 márciusában televíziós csatornák vételére szolgáló kódkártya hamisításával és terjesztésével a tettesek 64 milliárd forintot zsebeltek be.

3.2. A kiberbűnözés jellemzői

Az internet nyitott, decentralizált, interaktív jellegéből adódóan, a bűnözés ideális elkövetési területe. Az elkövetőknek előzetesen be kell szerezniük az eszközként szolgáló információkat, szoftvereket, valamint kellő szakmai tapasztalatot kell szerezniük az elkövetés sikerességéhez.

A fejlődő technika és az internet világszintű elterjedése lehetővé teszi, hogy a bűntények egyre nehezebben ellenőrizhetőek, gyakran a sértett előtt is rejtve maradnak. E magas láten-

35 A Z2 már relés elektromechanikus áramkörökkel működött, a Z3 pedig ennek továbbfejlesztéseként, az első programvezérlésű, kettes számrendszerben dolgozó számítógép volt.

36 A Z3 utódjaként ZUSE elkészítette a Z4-et, melyet először a repülőgép-tervezésben, majd 1950-től a zürichi Műszaki Főiskolán használtak.

37 Jack St. Claire KILBY (1923. november 8.-2005.június 20.) Nobel-díjas amerikai fizikus, ő a kézi számítógép és a hőnyomtató feltalálója is.

cia leggyakrabban a bankokat, hitelintézeteket és biztosítókat érinti, ebben vélhetően közrejátszik az a tény is, hogy e szervezetek önös érdekeik miatt, gyakorta nem jelentik a megtörtént káreseteket. A tettesek kiléte nehezen deríthető fel, mivel a kommunikációs csatornákon könnyedén rejtve maradhatnak. Az internet egy államhatárok nélküli virtuális világ, a bűncselekmények nemzetközi jellegűek, ami a visszaélések nyomon követését jelentősen megnehezíti. Egy újonnan megjelenő hardver, szoftver idővel általában az elkövetés új eszközévé válik, az így elkövetett cselekményeket azonban csak az elméleti alapvetések megalkotása révén lehetünk képesek megelőzni és csökkenteni.

3.2.1. A *cybercrime* cselekmények elkövetőinek tipológiája

Napjainkra bármely szakismerettel rendelkező személy a jogtalanság területére léphet szak tudása felhasználásával, s akár megalapozott informatikai tudás hiányában is bárki képes olyan online magatartást kifejezni – különösen kártékony programot vagy vírust használni –, amely képes informatikai eszközben, hálózatban, vagy azok segítségével más eszközben vagy másnak kárt okozni. Azt azonban fontos leszögezni, hogy az információtechnológia önmagában nem veszélyes tudomány, csupán annak nem megfelelő célokra való felhasználásával válhat egy bűntény melegágyává.

A 21. századi elkövetői kör igen sokszínű.³⁸ Napjaink komputer undergroundjának tagjai közé tartoznak a *hackerek* és *crackerek*,³⁹ akik védett rendszereket törnek fel (differenciálja őket, hogy a *crackerek* legtöbbször pénzszerzés céljából teszik ezt), az ártalmas kódokat készítő vírusírók,⁴⁰ a kalózkodók,⁴¹ akik tevékenységükkel szoftverek, védelmi rendszereinek feltörését célozzák, illetve az anarchisták,⁴² akik az információ szabad áramlását szándékoznak megakadályozni. E körbe tartoznak továbbá a *phreakerek*,⁴³ akik telefonvonalakba próbálnak technológiai eszközök használatával behatolni, valamint a *cypherpunkok*, akik olyan programokat írnak, melyekkel más párhuzamos számítógépeket sajátos kódolással látnak el. Megemlíten-dők még azon terrorista szervezetek is,⁴⁴ amelyek adathalász rombolás és toborzás céljából követik el az erőszakos cselekményeket. A legújabb kori terrorista szervezetek (pl. *ISIS*) tevékenységének már egy jelentős része zajlik az online térben, a fizikai valóságban megvalósítani szándékozott terrorista cselekményeiknek előkészítése, megszervezése informatikai hálózatok közbejöttével történik. Magyarország esetében a konfliktusoktól nem mentes szomszédság-politika bármikor eljuthat arra a pontra, hogy a kormányoktól független csoportosulások minimális befektetéssel, sikeresen zavarják meg hazánk mindennapos működését.⁴⁵

38 SZEGEDINÉ Lengyel Piroska: Számítógépes bűnözés, avagy fiatalok a cyber-térben. *Hadmérnök*, V. évfolyam 2. szám, 2010.június. 372.

39 Uo.

40 Uo.

41 Uo.

42 Az anarchisták olyan személyek, akik törvénysértő, vagy legalábbis morálisan kétes megítélésű információk terjesztését végzik. Minden, az információ szabad áramlását akadályozó rendelkezést elutasítanak.

43 SZEGEDINÉ i.m. (38. lj.) 372.

44 Uo.

45 Uo.

Az elkövetők motivációja is sokrétű, a céltalan, önmagáért való károkozástól, a politikai véleménynyilvánítás alkotmányos védelemben nem részesíthető kinyilvánításától, a kifejezett vagyoni előny megszerzésén keresztül, a terrorista motívumig terjed. Ezen elkövetői csoportokat számos tényező motiválhatja, többek közt a tapasztalatszerzés, a károkozás vagy a védett adatok megszerzése. Mivel az elkövetők leggyakrabban deviáns magatartású, érzelmileg labilis fiatalok vagy fiatal felnőttek, így véleményünk szerint nem csupán a virtuális világban kell védekeznünk ellenük, hanem biztosítanunk kell a serdülő gyermekek családcentrikus, információtudatos nevelését, mellyel a Z generációban csökkenthetjük a későbbi, elkövetésre irányuló hajlamot s így nagyobb eséllyel redukálhatjuk a jövőbeli jogsértések számát. A terrorizmus elleni védekezés nem lehet egységes, hiszen maga a terrorizmus sem az. A terrorizmus teljeskörű kiirtása lehetetlennek tűnő feladat, ezért meg kell próbálnunk azt a lehető legkisebb mértékűre visszaszorítani, elsődlegesen a lehetséges célpontok biztonságának fejlesztésével.⁴⁶

3.2.2. A bűncselekmények érintettjeiről általában

Az interneten elkövetett bűncselekményeknek naponta körülbelül egymillió áldozata van. A számítógépes bűnözők hozzávetőlegesen 750 milliárd eurót profitálnak Európában, és 4000 milliárd dollárt az Amerikai Egyesült Államokban. Világviszonylatban csaknem 50 milliárd internethez kapcsolt eszközről van tudomásunk. A számítógépes bűntények tulajdonképpen bárki ellen irányulhatnak, ám többségüket – adatok megszerzését, manipulálását célozva, vagy anyagi haszonszerzés végett – vállalatok ellen követik el. A PwC 2016-ban globális gazdasági bűnözés felmérést készített,⁴⁷ melyben világszerte 6337, míg Magyarországon 95 vállalat, vezető beosztású munkatársa válaszai alapján mérték fel a vállalatokat érintő bűnözési helyzetet.

A megkérdezett szervezetek 46%-a szerint Magyarországon a deliktumok legelterjedtebb formája a hűtlen kezelés, bár ehhez hozzá tartozik az a tény is, hogy ez az egyik legkönnyebben felderíthető gazdasági bűncselekmény. Az elmúlt két évben a hazai cégek 25%-a legalább egyszer találkozott valamilyen gazdasági bűncselekménnyel. Magyarország öt leggyakoribb ilyen bűncselekménye a hűtlen kezelés (46%), a korrupció és vesztegetés (38%), az adócsalás (21%), a számítógépes bűnözés (17%) és a közbeszerzési csalás (17%). A számítógépes bűnözés régiós áldozatainak átlaga 22%, a globális átlag pedig 32%, vagyis jóval több, mint a hazai 17%-os átlag, így feltételezhetjük, hogy a magyar cégek egy része tudtán kívül válhatott online bűntény áldozatává. A vállalatoknak a pénzügyi veszteségen túlmenően egyéb járulékos kára is keletkezik, nem beszélve a vállalat jó hírnevére gyakorolt negatív hatásairól. A magyarországi válaszadók 42%-a nyilatkozott úgy, hogy a cégénél bekövetkezett csalást vállalati ellenőrzési mechanizmus segítségével leplezték le (a régiós arány 54%, míg globálisan 47%). A vállalatok az utóbb említett tényezők miatt, gyakran tartják titokban az ellenük irányuló támadásokat, ezzel azonban a bűncselekmények elleni hatékony védekezést hátráltatják. Véleményünk szerint a vállalatvezetőknek ezért szükséges lenne nagyobb hangsúlyt

⁴⁶ A terrorizmus elleni védekezés,

www.debrecebijogimuhely.hu/archivum/3_2005/a_terrorizmus_elleni_vedekezes/.

⁴⁷ Alábecsült veszélyek? 2016. évi felmérés a globális és magyar gazdasági bűnözésről, https://www.pwc.com/hu/hu/kiadvanyok/globalis_gazdasagi_bunozes_felmeres/assets/gazdasagibunozes2016_web.pdf

fektetniük a védekezési mechanizmusok elsajátítására, és egy ilyen helyzetben büszkeségüket félretéve, nem szégyellni segítséget kérni.

3.2.3. A digitális bizonyíték

A kiberbűncselekmény végrehajtásával előtérbe kerül a bűnüldözés egyik kiemelkedő problematikája, a digitális bizonyítékok kezelése. Ezek ugyanis rendkívül egyszerűen manipulálhatóak és beszerzésük komoly nehézségekbe ütközhet a hatóságok számára.

Azokban az esetekben, ahol az ügyben informatikai tartalmak is érintettek, digitális bizonyítékok használata és szakértő bevonása is lehetséges. E tudományterület szülőhazája az Amerikai Egyesült Államok, mely szövetségi szabályozásában a bináris formában tárolt vagy továbbított, bizonyító erejű információként határozza meg a digitális bizonyítékot. Egy digitális nyom akkor válhat bizonyítékká, amikor a nyomozó hatóság vagy az erre feljogosított szerv a büntetőeljárásban vagy más keretek között nyomozást indít. A házkutatás során jelenhet meg először a digitális bizonyíték és szakértő kettőse, ez a felállás azonban ritka: az esetek többségében a házkutatást végző szerv munkatársainak kell a kulcsfontosságú tevékenységeket (bizonyítékok tárolása, szállítása, stb.) elvégezni.

A digitális bizonyítékok értelmezésénél a vizsgálati eljárás szabványok hiánya problémát okoz, mivel az egyes hordozó eszközök megtekintése és elemzése megfelelő készségeket kíván meg. Ez különösen a bírói testület munkáját nehezíti, ezért a szakértőknek nagyobb gondot kell fordítaniuk a bizonyítás digitális eszközeinek prezentálására. Máté István Zsolt igazságügyi informatikai szakértő szerint⁴⁸ a digitális bizonyítékoknak a büntetőeljárásban csak akkor lehet teljes bizonyító erejük, ha az eljárás valamennyi szereplője rendelkezik a szerepéhez mértén megfelelő szintű kompetenciával a digitális írástudás területén. A várhatóan 2018. január 1-jén hatályba lépő új büntetőeljárási törvény új bizonyítási eszközként határozza meg az elektronikus adatot, mellyel a jövő kihívásaira választ adni képes bizonyítási eszközök biztosítását célozza.⁴⁹

3.3. A technológiai fejlődés konzekvenciái

A technológiai fejlődés az évszázadok folyamán mindenkor kihívás elé állította a társadalmakat, sok esetben a társadalmi folyamatok nem álltak a technikai fejlettség szintjén. A technológia, mint jelenség mindig társadalmi környezetben hat és vizsgálata is kizárólag egy társadalmi közegében vizsgálható. A technológia és a társadalom egymásra hatásából számos következmény fakad, amelyek közül számos konfliktus is kialakul, ezekre kell a jogtudománynak és a jogi szabályozásnak adekvát válaszokat találni. A technológiai fejlődés társadalmi hatásainak elméleti vizsgálata során nem kerülhető meg a *Collengridge- dilemma*

48 Máté István Zsolt: *The Digital Evidence – A digitális bizonyíték*. https://www.academia.edu/5105387/A_digit%C3%A1lis_bizony%C3%ADt%C3%A9k_The_Digital_Evidence.

49 A téma elemzését adja SORBÁN Kinga: A digitális bizonyíték a büntetőeljárásban. *Belügyi Szemle*, 2016/64. 81-96., továbbá SORBÁN Kinga: A digitális bizonyíték a büntetőeljárásban, In: CHRISTIÁN László (szerk.): *Rendészettudományi kutatások: Az NKE Rendészetelméleti Kutatóműhely tanulmánykötete*. Budapest, Dialóg Campus, 2017. 129-136.

felemlítése, amely jól kontúrozza azokat a problémákat, amelyekkel a jogi szabályozásnak új technológiák, korábban nem létező műszaki megoldások társadalmasítása, jogiasítása során rendszerint szembe kell néznie.

A nyilvánosság az elmúlt egy évtizedben olyan szerkezetváltozáson ment keresztül, amelyben szükségszerűen újra kell gondolnunk a jogi szabályozás évszázados fogalmi kereteit. A régi keretek közül kvantitatívan (a társadalmi interakcióra rendelkezésre álló nyilvánosság mérete, befogadóképessége és átvételi potenciálja exponenciálisan növekedett), de még inkább kvalitatívan kilépő, új struktúrájú társadalmi nyilvánosságban jelenlévő kommunikációs eszközök, csatornák hatására a rájuk alkalmazott, de egy korábbi fejlődési szinten kiérlelt fogalmak jelentése szükségszerűen átalakításra, finomhangolásra szorul. Az internetes tömegkommunikációval a jog (saját régi fogalmainak foglyaként) sokszor nehezen tud mit kezdeni. A joggyakorlat sok esetben nem tudja a régi szabályokat az új keretek között alkalmazni, a jogi szabályozás pedig rendszerint csak kullog a technológiai fejlődés által támogatott társadalmi valóság nyomában. A jogi szabályozás tehát kizárólag ott próbál több-kevesebb sikerrel, ad hoc jelleggel belépni, utánkötéssel akadálymentesíteni, ahol hirtelen 'sűrűsödési probléma' jelentkezik. Bár számos megoldandó probléma észlelhető az internetes nyilvánosságban, napjainkban még részlegesen látszanak csupán a nemzeti jogalkotók által választható szabályozási modellek. Természetesen az interneten működő nyilvánosság szabályozási területén különös jelentősége van a *ius – non ius* elhatárolás kérdésének; meddig szabályozzon a jog, és honnan kapjon szerepet az ön– és társszabályozás. Erre a jogelméleti kérdésre azonban jelen írásban nem térünk ki.

A technológiai fejlesztések szükségszerűen generálják a számítógépes bűncselekmények sokszorozódását és kezelhetetlenebbé válását, ezért lényeges hangsúlyt kell fektetni a megfelelő védelmi stratégiák kialakítására, ehhez pedig elengedhetetlen az internet-szolgáltatók és a bűnüldöző hatóságok szorosabb együttműködése, illetve a jogalkotás reakciójának gyorsítása és a joghatósági problémák kiküszöbölése. Az elkövetők gyakran használnak számítógépes banki rendszereket pénzügyi tranzakciók, illegális átutalások lebonyolítására, vagy a sértett zsarolása céljából. Az Eset biztonságtechnikai cég szerint az idén a legnagyobb fenyegetést többek között ezek a zsarolóvírusok jelentik, melyek különösen gyakran vesznek célba egészségügyi intézményeket, vagy célozzák a játékipart⁵⁰, kedvelt fizetőeszközük az internetes pénz, a bitcoin. A számítástechnika rohamos innovációjának köszönhetően veszélybe kerülhetnek olyan nyílt rendszerek is, melyek pénzügyi, katasztrófavédelmi szervek vagy egyéb infrastruktúrák működését szolgálják. Ezért nemcsak a védekezés lényeges, hanem a megelőzés is: a kormányoknak kiemelt figyelmet kell fordítani a megfelelő informatikai oktatás megszervezésére, hogy a holnap szakemberei minél alaposabban felkészülhessenek a társadalmat fenyegető veszélyre. Az IP címek⁵¹ az informatikai eszközök csatlakozási helyének és idejének beazonosítására szolgálnak, mára azonban egy egyszerű *proxy szerverre*⁵² kijátszhatók, a hackerek pedig erre irányuló szolgáltatások, például az *Onion network*⁵³ ki- és továbbfejlesztésén

50 Kórházakat és mobilokat támadnak a zsarolóvírusok, www.tozsdeforum.hu/extra/tech-tudomany/korhazakat-es-mobilokat-tamadnak-a-zsarolovirusok-84370.html.

51 (Internet Protocol-cím) Egy egyedi hálózati azonosító, amelyet az internetprotokoll segítségével kommunikáló számítógépek egymás azonosítására használnak.

52 Olyan szerver (számítógép vagy szerveralkalmazás), amely a kliensek kéréseit köztes elemként más szerverekhez továbbítja.

53 Másik elnevezése a Tor hálózat, az internet láthatatlan részét képezi, az e területen futó hálózati kapcsolatok és szolgáltatások nem azonosíthatók.

dolgoznak. Aktuális probléma a *szteganográfia*⁵⁴ is, mellyel titkosított információ tárolására alkalmas helyhez juthatnak az elkövetők.

Az internet globális jellege miatt, a nemzetállami határoknak csekély a jelentősége, hiszen nem szükségszerű, hogy az elkövető a sértettel azonos országban, kontinensen tartózkodjon. A jogalkotóknak nincs könnyű dolguk, hiszen az a technológiai környezet, amelynek szabályrendszerét ki kellene alakítaniuk permanens fejlődésben van, így a bűnelkövetők mindig egy lépéssel a jog előtt járnak. Mindezen nehézségek ellenére, a tagállamok és a nemzetközi szervezetek az utóbbi esztendőkből – összehangolt munkájukkal – egy átfogó szabályrendszer megalkotásán törekcsenek. A technológia-semlegesség⁵⁵ elve segít a gyorsan változó technológiai környezet kezelésében, hiszen a szabályozás nem a szolgáltatásra, hanem magára a tevékenységre koncentrál.

4. Nemzeti jogforrásaink

4.1. A Nemzeti Kiberbiztonsági Stratégia

Magyarország Nemzeti Kiberbiztonsági Stratégiája az 1139/2013. (III.21.) Kormányrendeletben született meg. Fő célja, hogy – illeszkedve a biztonságos és innovatív 21. századi nemzetközi környezetbe – hazánk nemzeti érdekei a kibertérben is érvényesülhessenek. Ehhez elengedhetetlen a kibertérből eredő fenyegetések kezelése, a kormányzati összhang és eszköztár előremozdítása. A rendelet megalkotásához az 1035/2012. (II.21.). Kormányrendeletet vették alapul, valamint az Európai Unió kiberbiztonsági előírásait követték. Fontos volt továbbá az is, hogy a nemzeti szabályozás illeszkedjen a NATO csúcs- dokumentumaiban foglalt elvekhez is. Az így megalkotott jogszabály számos betartandó követelményt határoz meg a biztonságos világháló megteremtése érdekében, így elsődlegessé vált az innovativitás a gazdaságban, a kiberfenyegetések elhárítása és az állami informatikai szolgáltatások fejlesztése.

A Nemzeti Kiberbiztonsági Stratégia rövid bemutatását nem csupán azért tartjuk fontosnak, mert kiemelten sok pozitív változást eredményezett az internetes fenyegetések megelőzésére és elhárítására vonatkozóan, hanem azért is, mivel a kormányrendelet hatására számos új szervezet és sikeres együttműködés jött létre. Első lépésként a 484/2013. (XII.17.) Kormányrendelet, mintegy a kormányzati koordináció gyümölcseként, létrehozta a Nemzeti Kiberbiztonsági Koordinációs Tanácsot. A kormány célkitűzésévé vált olyan szakosított intézmények létrehozása is, amelyekben specifikus szakértelmű személyek kerültek az adat- és titokvédelmi területek élére. A Stratégia egyik fő eredményeként megszületett a Gyermekvédelmi Internet-kerekasztal, mely 2014 óta a Nemzeti Média és Hírközlési Hatóság tanácsadó testületeként, kiemelt figyelmet fordít a gyermekbarát internetezés megvalósítására és a szűrőszoftverek átható fejlesztésére. A kerekasztal elnöke a Médiatanács egy tagja, akit a Mé-

54 Az adatelrejtés egyik kedvelt módszere, a felhasználó háromdimenziós képekbe menti el adatait, a képek eredeti méretének megtartásával. Mára egy üzenetet bármiben el lehet rejtteni. Amiben elrejtjük, az a hordozó, az eredmény pedig a *stegotext*. A szteganográfia párja a kriptográfia, ahol az üzenet, illetve a titkosított tartalom létét nem álcázzák, de a tartalmát csak megfelelő rejtjel segítségével olvashatja a fogadó.

55 A technológia-semlegesség értelmében nem részesíthető előnyben és nem zárható ki egyetlen technológia vagy hálózati platform sem a szélessávú szolgáltatásokat nyújtók közül.

diahatóság elnöke két másik taggal együtt saját jelölés alapján nevezett ki, a testület további 8-8 tagját a gyermekvédelemmel foglalkozó szervezetek, illetve az internetpiaci szakmai szövetségek ajánlásai, két tagját az illetékes minisztériumok javaslata alapján nevezett ki a törvényi rendelkezéseknek megfelelően. Megbízatusuk 3 évre szól, munkájuk önzetlen, díjazásban nem részesülnek. A 21 tagú tanácsadó testület célja⁵⁶, hogy ösztönözze a kiskorúak védelmét a világhálón, és támogassa a Nemzeti Média- és Hírközlési Hatóság elnökének munkáját. Ennek érdekében állásfoglalásokat, ajánlásokat dolgoz ki a gyermekbarát internetezés elterjesztésére, így a szűrőszoftverek hatékony alkalmazására is, valamint a gyerekek és szüleik médiatudatosságának növelésére. A grémium nagy hangsúlyt fektet a kiskorúak szellemi és lelki fejlődésére, valamint a gyermekek és szüleik médiatudatosságra való nevelésére.

4.2. Magyarország Digitális Gyermekvédelmi Stratégiája

2016-ban, a Digitális Jólét program részeként elkészült Magyarország Digitális Gyermekvédelmi Stratégiája, mely aktuális megoldásként szolgál a gyermekeket fenyegető új típusú veszélyforrások kezelésére, elhárítására. Az 1488/2016. (IX.2.) számú Kormányhatározat a biztonságos internetszolgáltatás megteremtéséről, a tudatos internethasználatról és Magyarország digitalizált gyermekvédelmi stratégiájáról szól. A 2016 szeptemberétől induló program a magyar nemzetgazdaság digitális fejlesztését célozza, elsődleges célkitűzése, hogy megvédje a gyermekeket az internet veszélyes, káros tartalmaitól és tudatos, értékteremtő internethasználatra nevelje őket. Mindez nem valósulhatna meg a gyermekek védelmét szolgáló szabályok és intézkedések kiemelt érvényesülése és érvényesítése nélkül. A stratégia további célja, hogy a védelmi mechanizmusok megfelelően funkcionáljanak, kiküszöbölve a gyermekekre leselkedő veszélyeket és káros hatásokat.

A Kormány a magyarországi internetszolgáltatókkal kötött megállapodás keretében, a „Gyermekek Számára Biztonságos Internetszolgáltatás” új feltételeit kívánja megteremteni. Ingyenesen hozzáférhető, magyar nyelvű gyermekvédelmi szűrőszoftverek kifejlesztését kezdeményezi, célkitűzése továbbá egy kiskorúak számára biztonságos tartalmakat bemutató honlap létrehozása és működtetése is. Átfogó tájékoztatási programokat kíván indítani a gyermekek megóvását célzó jogszabályi rendelkezések megismertetése és a digitális világban megjelenő sérelmekkel szembeni fellépési lehetőségek bemutatása érdekében. Ingyenes képzési és továbbképzési programokat indít, melyek célja a szülők, pedagógusok, valamint a gyermekekkel foglalkozó más szakemberek médiaműveltségének fejlesztése.

4.3. Magyarország Digitális Oktatási Stratégiája

A digitalizáció ma már nem választás kérdése, a 21. században Magyarországon nincs olyan ember, aki kizárhatja életéből a digitális világot, hiszen valamilyen szinten mindenkit érint.⁵⁷

56 A Gyermekvédelmi Internet-kerekasztal feladata és tagjai, nmhh.hu/cikk/162718/A_Gyermekvedelmi_Internetkerekasztal_feladata_es_tagjai.

57 A digitalizáció már nem a jövő, hanem a jelen, www.kormany.hu/hu/miniszterelnoki-kabinetiroda/digitalis-jolet-program/hirek/a-digitalizacio-mar-nem-ajovo-hanem-a-jelen.

Ennek fényében 2016 nyarán elkészült Magyarország Digitális Oktatási Stratégiája (DOS),⁵⁸ mely minden elemében illeszkedik a kormányzati elképzelésekhez. E stratégiában jóval nagyobb szerepet kap az oktatás területén a digitalizálás, s ez nagymértékben kihat az oktatás szemléletmódjára, módszertanára, az új tanulási folyamatokra és az oktatási környezetre is. A stratégia foglalkozik a pedagógusok digitális felkészültségének fejlesztésével, az oktatási tananyagok újragondolásával, a fizikai infrastruktúrával és az intézmények eszközellátásával is. A tervek szerint 2020-ra befejeződik a magyar oktatási rendszer digitális átalakítása. Az új nemzeti alaptantervben (Nat) a digitális képességek és eszközök használata kiemelt szerepet kap majd.

5. Nemzetközi jogforrások

5.1. A Számítástechnikai Bűnözésről Szóló Egyezmény és újragondolása

Az Európa Tanács Számítástechnikai Bűnözésről szóló Egyezménye⁵⁹ (a továbbiakban: Cybercrime-Egyezmény) 2004. július 1-jén lépett hatályba. Elsődleges célja, hogy megvédje a társadalmat a kiberbűnözéssel szemben, s megteremtse a részt vevő tagállamok között az ehhez elengedhetetlen összhangot. A Cybercrime-Egyezmény számos korábbi megállapodás eredményeit viszi tovább, ezek közé sorolható a korábbi 1950-es Emberi Jogok és Alapvető Szabadságok Védelméről szóló Egyezmény, az 1960-ban elfogadott Polgári és Politikai Jogok Nemzetközi Egyezségokmánya, valamint az 1989-ben ratifikált Gyermekek Jogairól szóló Egyezmény.

Ezen egyezmények megerősítik a véleménynyilvánítás szabadságához, a vélemény kifejtése miatti hátrányos következményektől való védelemhez való jogot, ide értve azt a jogot, hogy mindenki szabadon, határookra tekintet nélkül kereshessen, megszerezhesen és közölhesen bármilyen tartalmú eszmét és információt, továbbá a magánélet tisztelőben tartásához fűződő jogot is⁶⁰. A Cybercrime-Egyezmény egy jól működő nemzetközi együttműködés⁶¹, azonban az esetek többségében reaktív jellegű, tehát a bekövetkezett támadás esetére nyújt megoldást. A tagállamok azonban megkívánják, hogy ne csak a már megtörtént támadások elbírálására adjon jogi keretet, hanem preventív jelleggel is bírjon. A jelenlegi szabályozás némely esetekben elmarad a kor és a technológiai színvonal követelményeitől, mivel akár egy mit sem sejtő felhasználó számítógépével is végrehajtható olyan támadás, amit a jog szankcionál. A támadó hálózatok napjainkra oly mértékben elterjedtek, hogy egy átlagos anyagi

58 Magyarország Digitális Oktatási Stratégiája, www.kormany.hu/download/0/cc/d0000/MDO.pdf.

59 2004. évi LXXIX. törvény az Európa Tanács Budapest, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről, http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0400079.TV.

60 Uo.

61 A Cybercrime-Egyezményt a legtöbb uniós tagország aláírta, de csatlakozott hozzá Kanada és Dél-Afrika és az USA is. Az egyezmény 2. cikkelye foglalkozik a jogosulatlan belépéssel, és kimondja azt, hogy minden aláíró állam megteszi majd azokat a jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy bűncselekménynek minősüljön a számítástechnikai rendszerbe, vagy annak bármely részébe történő jogosulatlan és szándékos belépés.

helyzetben lévő felhasználónak sem kell mélyen a zsebébe nyúlania ahhoz, hogy *botnet*⁶² üsse a markát, sőt, hozzáértőnek sem kell feltétlenül lennie annak használatához.

Ezek a tények félelemre adnak okot, annak tudatában, hogy a nyelvi korlátok lehullásának is köszönhetően, a világ más régióiból érkező adathalász, célzott adathalász támadások már nincsenek többé határok közé szorítva. Mindazonáltal szükségesnek tartjuk megjegyezni, hogy a Cybercrime-Egyezmény a jelenlegi legsikeresebb kibervédelmi nemzetközi együttműködés, és a 2018-ban hatályba lépő GDPR adatvédelmi rendelettel társítva, a kibervédelem egy új fejezetét nyithatja meg az online világban.⁶³

5.2. Az Európai Bizottság biztonsági stratégiája

2015. április 28-án az Európai Bizottság által közzétételre került a 2015-2020-ig terjedő időszakra szóló európai biztonsági stratégia, aminek a célja, hogy támogassa a tagállamok együttműködését az online biztonsági fenyegetések kezelése során, és fokozza közös erőfeszítéseiket a terrorizmus, a szervezett bűnözés és a számítástechnikai bűnözés elleni küzdelemben. E fenyegetések ellen a stratégia többek között az informatikai ágazattal folytatott párbeszéd fokozásával és az Európai Unió eszközeinek megerősítésével lehet fellépni.

Így a Bizottság 2015-ben uniós szintű fórumot indított a fő informatikai vállalatokkal az interneten és a médiában folytatott terrorista propaganda megfékezése, és az új titkosítási technológiákkal kapcsolatos módszerek felkutatása érdekében. Prioritást élvez az online bűnügyi nyomozás akadályainak, és az internetalapú bizonyítékokhoz és információkhoz való hozzáférés szabályainak a megállapítása. Deres Petronella szerint a közelmúlt eseményei rávilágítottak annak szükségességére, hogy fokozzuk az erőfeszítéseket, és felgyorsítsuk a stratégiában meghatározott konkrét intézkedések végrehajtását.⁶⁴ Erre szolgál a FIDUCIA kutatási projekt⁶⁵ 9. munkacsomagja is, amelyik a számítógépes bűnözés jogi, kriminológiai és szociológiai vonatkozásait tárja fel, elemzi az egyes bűncselekményeket, az ezekhez kapcsolódó adatgyűjtést, valamint felülvizsgálja a jogi szabályozást és a megelőzés érdekében tett intézkedéseket.

5.3. További kiemelkedő nemzetközi dokumentumok

A számítógépes bűncselekmények tekintetében irányadó nemzetközi dokumentumként, elsőként az 1986-os OECD jelentést szeretnénk megemlíteni. A Gazdasági Együttműködési és Fejlesztési Szervezet⁶⁶ (OECD) iránymutatást adott az európai igazságszolgáltatás tapasztala-

62 A botnet ebben az értelemben olyan hálózatra kapcsolt gépek (botok) összessége, amelyek felett malware programok által átvették az irányítást.

63 L. 5.4. General Data Protection Regulation (GDPR) – a jövő.

64 DERES Petronella i.m. (3. lj.) 243–250.

65 A FIDUCIA – „New European Crimes and Trust-based Policy” egy európai finanszírozású (EU FP7) projekt, amely kifejezetten a büntető-igazságszolgáltatás és az intézményi bizalom összefüggéseit vizsgálja. Célja, hogy kidolgozza a bizalomalapú közpolitika-csinálás modelljét, és ez alapján ajánlásokat fogalmazzon meg a kriminológia új területein, így a kiberbűnözésről is.

66 Az OECD párizsi székhelyű nemzetközi szervezet, melynek célja, hogy segítse a tagállamok kormányait a lehető legjobb gazdasági és szociális politika kialakításában és értékelésében. Fő profilja a tagállamok gazdasági, kereskedelmi és pénzügyi tevékenységének összehangolása. Magyarország 1996 óta tagja a szervezetnek.

tairól, segítve ezzel a számítógépes környezetben elkövetett bűncselekmények megismerését és kodifikálását. 1989-ben megjelent a strasbourgi székhelyű Európa Tanács 9. számú ajánlása, mely a *cybercrime* definiálása során már említésre került. Később, 1995-ben megjelent a 13. számú ajánlása is, amelyik eljárásjogi problémákra reflektál. 1997-ben a G-8 fórum által Bűnözés elleni alcsoporthoz alakult, és elfogadásra került a számítógépes bűnözés elleni harc tíz alapelve. 2001-ben létrejött a korábbiak során már említett Cybercrime-Egyezmény is.

Tíz évvel később, 2011-ben megszületett az Európai Parlament és Tanács 2011/92/EU számú irányelve a gyermekek szexuális bántalmazásáról, szexuális kizsákmányolásáról és a gyermekpornográfia elleni küzdelemről, mely büntetni rendeli a gyermekkel való, szexuális céllal történő internetes kapcsolatfelvételt. Két évvel később, az információs rendszerek elleni támadásokról született meg a 2013/40/EU irányelv, melynek célja, hogy bizonyos minimumszabályok megállapításával, egymáshoz csiszolja a tagállamok büntetőjogát és javítsa a tagállamok hatóságai, a rendőrség, a bűnüldözési szakszolgálatok és az Unió ügynökségei és szervei közti együttműködést. Az irányelv felhívja a tagállamok figyelmét arra, hogy azonos büntetőjogi tényállási elemeket fogalmazzanak meg, szankcionálásuk során a szervezett bűnözés legyen minősítő körülmény, a jogosulatlan adatszerzés, a rosszindulatú szoftverek használata és személyiség-lopás legyen büntetendő, tilalmazandó. Cél továbbá, hogy a szankciók legyenek arányosak a bűncselekmény súlyával és legyen megfelelő visszatartó erejük, s nem utolsónak az alkalmazottak által végrehajtott cselekmények essenek súlyosabb elbírálás alá.

5.4. General Data Protection Regulation (GDPR) – a jövő

Az Európai Parlament és a Tanács 2016/679. adatvédelmi rendelete⁶⁷ 2018. május 25-én lép hatályba, s lényegében minden olyan személyre, szervezetre vagy online szolgáltatásra irányadó lesz, ami kapcsolatban van a digitálisan tárolt személyes adatokkal. Az adatkezelőknek általánosan megfogalmazott szabályoknak kell megfelelniük az Európai Unió lakosairól tárolt adatok kezelése során, az állampolgárok pedig hivatalosan elismert jogokat szereznek saját adataik kezelése felett. Az előírások megszegése akár 20 millió eurós (több mint 6 milliárd forint), vagy az éves árbevétel 4%-kát is elérő büntetéssel járhat. A GDPR kötelezővé teszi az adatkezelő számára a 72 órán belüli incidens bejelentést, minden érintett számára biztosítja a helyesbítéshez és törléshez való jogot és a hordozhatósághoz való jogot is. A személyek külön hozzájárulását kell kérni az adatgyűjtéshez, s ezt a hatóságok felé bizonyítani is kell, ez nem vélelmezhető. Az érintetteknek jogot kell biztosítani az adatkezelő vagy adatfeldolgozó által használt automatikus elbíráló rendszer döntése elleni fellebbezésre. Az elszámoltathatóság tükrében az adatkezelőnek ténylegesen bizonyítania kell, hogy megfelel a GDPR elvárásainak.

Az Egyesült Államok Adatvédelmi Hivatala, az ICO⁶⁸ 2016. március 14-én közzétett egy útmutatót⁶⁹, amely 12 lépésben segít felkészülni az új adatvédelmi rendeletre. A magyar

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

www.eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32016R0679&from=HU.

68 Az Egyesült Államok Adatvédelmi Hivatala.

69 Preparing for the General Data Protection Regulation (GDPR), www.huntonprivacyblog.com/wp-content/uploads/sites/18/2016/03/preparing-for-the-gdpr-12-steps.pdf.

Infotv.⁷⁰ kapcsán más alapokból kell majd kiindulni, s ezért mások lesznek a prioritások is, de a listára így is érdemes figyelmet fordítani. Az ICO által javasolt 12 lépés:

- 1) Tudatosság
- 2) A meglévő információ
- 3) Az adatvédelmi információk átadása
- 4) A személyhez fűződő jogok
- 5) Az érintettek hozzáférési kérvényei
- 6) A személyes adatok feldolgozásának jogalapja
- 7) Beleegyezés
- 8) Gyermekek
- 9) Az adatokat érő jogsértések
- 10) Beépített adatvédelem és adatvédelmi hatásvizsgálatok (DPIA)
- 11) Adatvédelmi munkatárs
- 12) Nemzetközi szint.

5.4.1. Reflekciók az általános adatvédelmi rendeletrre

Az Európai Parlament és Tanács 2016/679 rendelete elsőre egyszerűnek és távolinak tűnhet, ám a helyzet mást mutat. Bár a GDPR mind az adatkezelőket, mind az adatfeldolgozókat érinti, a szerepek gyakran felcserélődhetnek és könnyen megeshet, hogy az adatkezelő egyben adatfeldolgozóvá is válik. Véleményünk szerint az adatok kezelése szintén problémákat okozhat. Az adatkezelőknek többek között előzetesen vizsgálniuk kell a tárolandó adatok megfelelőségét, a tárolás jogszerűségét, az arra irányadó helyet, időt, és a lehetséges másolatokat, kivonatokat is. Mindez egy nagyobb szervezetnél, ahol az adatok áramlanak és feldolgozások esetenként kiszervezésben történik, igen körülményes feladat. A rendelet szinte kizárólag általánosan megfogalmazott pontokat tartalmaz, technikai részleteket nem – így komoly feladatot okoz majd az érintetteknek, hogy megfelelően implementálják az új rendelkezéseket. A GDPR komoly pénzbüntetés kiszabásával rendeli büntetni az előírások megszegőit, ez azt sugallja, hogy nem csupán opcionális ajánlásról van szó: 2018 májusa az adatkezelés új korszakának nyitányát hordozza magában.

6. EU-s jogforrások

6.1. Az Európai Unió számítógépes bűnözésre vonatkozó jogforrásai

Az Európai Unió Bizottsága kiemelt fontosságú veszélyként tekint az információs rendszerek elleni támadásokra, célkitűzése egy biztonságon és jogérvényesülésen alapuló térség megvalósítása. A Tanács 2005. február 24-én megalkotta a 2005/222/IB. számú kerethatározatot, amely lényegét tekintve közel azonos a Cybercrime-Egyezmény számítástechnikai bűncse-

70 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról, http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1100112.TV.

lekményekre vonatkozó tényállásaival. A kerethatározat uniós jogforrás, így kötelező erővel bír az unió valamennyi tagállamára nézve, tehát jelentős lépésnek tekinthető az informatikai bűncselekmények elleni uniós együttműködésben.

A jogforrások közé sorolható még a 2001/413/IB. számú kerethatározat a nem készpénzes fizetőeszközökkel összefüggő csalás és hamisítás elleni küzdelemről, valamint a 2002/58/EK elektronikus hírközlési adatvédelmi irányelv is. Utóbbi arra kötelezi a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtóit, hogy biztosítsák szolgáltatásaik biztonságát, továbbá rendelkezéseket tartalmaz a kéretlen levelek és kémprogramok ellen is. Az internethasználat biztonságosabbá tétele érdekében a hálózat-és információbiztonsági politika számos fellépéssel lett gazdagabb, például a biztonságos információs társadalomra irányuló stratégiáról szóló közleménnyel (COM(2006)251.), valamint a kéretlen levelek, a kémprogramok és a rosszindulatú szoftverek elleni küzdelemről szóló közleménnyel (COM(2006)688.). A 460/2004/EK rendelet az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) létrehozásáról szól. A nemzetközi bűnügyi együttműködés fejlesztése érdekében számos egyezmény született és több kiváló nemzetközi szervezet jött létre, köztük az Interpol, az Europol és az Eurojust. E szervezetek mindegyike a határon átnyúló valamennyi bűnözési forma visszaszorítására jött létre, így többek között a számítógépes bűnözés visszaszorítására is kiterjed a tevékenységük. A bűnügyi együttműködés egyszerűsítésére a 2006/960/IB. kerethatározat is tett lépéseket, célként tűzte ki, hogy a bűnüldözési operatív információkhoz való gyors és pontos hozzáférést biztosítson. A kerethatározat érvényesülésének érdekessége, hogy amennyiben valamely tagállam a beszerzett információt vagy bűnüldözési operatív információt bíróság előtt bizonyítékként kívánja felhasználni, be kell szereznie az információt vagy bűnüldözési operatív információt szolgáltató tagállam beleegyezését a tagállamok között hatályban lévő, az igazságügyi együttműködésre vonatkozó eszközök alkalmazása útján. A beleegyezés beszerzése nem szükséges, amennyiben a megkeresett tagállam az információ vagy bűnüldözési operatív információ átadásakor beleegyezését adta annak bizonyítékként történő használatához.

A Tanács 2009/316/IB. határozatában döntött az Európai Bűnügyi Nyilvántartási Információs Rendszer (ECRIS)⁷¹ létrehozásáról. Az EU Stockholmi Programja⁷² a 2011-2015. közötti időszakra vonatkozóan, előírta az európai bizonyítékgyűjtési rendszer kidolgozását.

6.1.1. Az ENISA szerepe

Az Európai Hálózat- és Információbiztonsági Ügynökség székhelye a görögországi Iráklionban van. A 2004-től működő szervezet célja, hogy az Európai Unió, a tagállamok és az üzleti szféra fokozottabb mértékben legyen képes a hálózat-és információbizton-

71 Az ECRIS egy egységes elektronikus hálózat, információcsere-rendszer, amely az egyes tagállami bűnügyi nyilvántartások információinak elektronikus cseréjét, így az unió polgárainak védelmét szolgálja. Alapját az egyes tagállamok bűnügyi nyilvántartásai képezik. Gyakorlati szempontból az összes tagállam bűnügyi nyilvántartásának elektronikus úton történő összekapcsolását jelenti. A büntetőjogi felelősséget megállapító ítéletekre vonatkozó információk cseréjére gyorsan, egységesen és számítógép útján könnyen továbbítható formában kerül sor.

72 A Stockholmi Program meghatározza az Európai Unió által a jog érvényesülésén, a szabadságon és a biztonságon alapuló térségre vonatkozóan, a 2010 és 2015 közötti időszakra megállapított prioritásokat.

sággal kapcsolatos problémák megelőzésére, kezelésére és az azokra történő reagálásra. Továbbá, felkérés esetén segíti a Bizottságot az uniós jogszabályok korszerűsítését és kidolgozását szolgáló technikai előkészítő munkájában. Ezen felül fokozza az együttműködést az állami és a magánszektor szereplői között, hogy kielégítően magas szintű biztonság valósulhasson meg az EU-tagállamokban. Ezen célkitűzések elérése céljából, az ENISA összegyűjti a megfelelő információkat a jelenlegi és jövőbeni kockázatok elemzéséhez, és kutatási eredményeiről tájékoztatja a tagállamokat és a Bizottságot. Az Európai Parlament, a Bizottság és az illetékes európai és nemzeti szervek számára tanácsot ad, segítséget nyújt, valamint fokozza az ágazati szereplők közötti együttműködést. Célja még, hogy elősegítse a Bizottság és a tagállamok közötti együttműködést a biztonsági problémák megelőzésére szolgáló közös módszerek kidolgozása során, s hozzájáruljon a tudatosság növeléséhez és a naprakész, átfogó információk szolgáltatásához valamennyi felhasználó számára. Segíti a Bizottságot és a tagállamokat az iparról, illetve a hardver- és szoftvertermékek biztonságáról folytatott párbeszédnek során, nyomon követi a biztonsági termékek és szolgáltatások szabványainak kialakítását, előmozdítva a kockázatértékelési és kockázatkezelési tevékenységeket. Az ENISA hozzájárul az EU-n kívüli országokkal és nemzetközi szervezetekkel folytatott együttműködéshez azzal, hogy elősegíti a biztonsági kérdésekre vonatkozó globális szemlélet terjedését, és megfogalmazza saját következtetéseit, iránymutatásait, tanácsot ad a segítségkérőknek.

6.2. European Cybercrime Centre

Az Europol Kiberbűnözési Központ testesíti meg az Európai Unió informatikai bűnözés elleni küzdelmét, tevékenységével hozzájárul a határon átnyúló bűncselekményekre való gyors reagáláshoz. Elsősorban a bűnszervezetek, bűnszövetségek általi kibertámadásokra összpontosít, ennek céljából együttműködik a számítógépes bűnözésben eljáró hatóságokkal, a tagállamok nyomozati szerveivel, nemzetközi bűnüldöző hatóságokkal, illetve a civil szférával. Adatokat gyűjt a számítógépes bűnözésről, kiberbűnözési helpdesket üzemeltet, támogatja a közös nyomozócsoportok létrehozását egy vagy több tagállam együttműködésével, összhangot teremt az Európai Unió kívüli tagokkal, és koordinálja a nemzetközi ügyek nyomozását. Értékeli a kibertérből érkező fenyegetéseket, elemzi a trendeket és előrejelzi a legújabb fejleményeket a kiberbűnözés alakulásában. Szoros együttműködést épített ki az Európai Rendőr-akadémiával, képzéseket szervez a nyomozó hatóságok tagjainak, a bírácoknak és ügyészeknek, emellett *forenzikus* eszközöket fejleszt ki. Egy olyan információs infrastruktúra kialakításán dolgozik, melyben a vele együttműködő szervezetektől származó minden adatot rögzítenek, melyek ez által visszakereshetőek lesznek a kiberbűnözésre vonatkozóan. A Kiberbűnözési Központ mellett speciális feladatokra felállított munkacsoport (*European Cybercrime Task Force*⁷³) jött létre. Az Europol rendelkezik egy több elemből álló kiberbűnözési platformmal, melynek része többek közt az internetes bűncselekmények

73 Az EUCTF kurzusok szervezésével és technikai eszközökkel támogatja a tagállamok hatóságait, valamint a magánszektorral és a tudományos világgal is kapcsolatot tart a nyomozások fellendítése érdekében. Az internetes szervezett bűnözésről évente ad ki stratégiai elemzéseket (iOCTA), amelyek főként a kiberbűncselekmények értékeléseit tartalmazzák.

bejelentésére szolgáló online rendszer (*Internet Crime Reporting Online System*), amelyre a világhálón észlelt deliktumokkal kapcsolatos információk tölthetők fel; egy kiberbűnözési munkafajl (*AWF*), valamint a technikai szakismeret bővítését ellátó internetes kriminalisztikai szakértői platform (*Internet Forensic Expertise Platform*). A Központ szervezetén belül három fókuszpont működik, az első az *FP Cyborg* (Kiberbűncselekményekkel foglalkozó fókuszpont), mely a tisztán informatikai jellegű bűncselekmények nyomozásával foglalkozik, illetve a számítógépes bűntények megelőzését és az ellenük való küzdelmet támogatja. A második az *FP Twins*, amely a gyermekek szexuális kizsákmányolásával foglalkozik, célja az elkövetők azonosítása és a tagállamok közötti kapcsolatok kialakítása. A határon átnyúló esetekben feladata még az elkövetési mód, a *modus operandi* feltárása, illetve a bűnelkövetői hálózatok kommunikációs módszereinek elemzése azok felbontása érdekében. A harmadik fókuszpont az *FP Terminal*, mely támogatja az EU tagállamok nyomozásait számos bankkártyás csalással kapcsolatban.

7. A csúcstechnológiai bűnözés elleni harc régen és ma

A csúcstechnológiai bűnözés elleni egység legkorábbi elődje az Országos Rendőr- főkapitányság (ORFK) sajtófigyelő csapata volt. Az ő feladatuk a rendőrségi sajtómegjelenésekhez kapcsolódó tartalmak követésére terjedt ki. Később hatáskörük bővült az internetes jogsértések monitorozásával, majd 2007 februárjában nyomozati jogkört kapott az egység, ekkor hozták ugyanis létre a témával jelenleg foglalkozó osztályt, akkor már a Nemzeti Nyomozó Iroda részeként.

Jelenleg Magyarországon inkább számítógépes bűnözésről lehet beszélni, de a technika fejlődési irányai és üteme tekintetében, átfogóbb a csúcstechnológia kifejezés. A kiberbűnözők ellen harcoló rendőrök az internetes jogsértések mellett bejelentések, feljelentések, illetve saját nyomozásaik alapján értesülnek egy-egy újabb esetről. Bár a teljes internet monitorozása lehetetlen feladat, a már megismert bűncselekmények kapcsán felmerülő területeket visszatérően vizsgálják. Kisebb ügyekben megyei, városi, illetve a Budapesti Rendőr-főkapitányság és a kerületi szervek is nyomozhatnak. A Nemzeti Nyomozó Irodához (NNI) a nagyobb felkészültséget igénylő ügyek kerülnek. 2008 óta a Budapesti Rendőr-főkapitányságon is van egy kiberbűnözés elleni fellépésre specializált egység. A nyomozók munkáját a hagyományos rendőri kellékek mellett speciális felkészültségű nyomozók, illetve 'law enforcement' eszközök segítik. Utóbbiak nagy teljesítményű szoftverek és hardverek, melyeket kifejezetten igazságszolgáltatási célokra alakítottak ki. A nyomozók a jól felkészült bűnözők ellen így is lépéshátrányban vannak technológiai szempontból, de ezt a hátrányt igyekeznek minél kisebb szintre szorítani. Egyre több a bejelentett számítógépes bűntény, a jelentősebb ügyek száma 1% körüli hazánkban. Gazdag Tibor⁷⁴ szerint a legjellemzőbb bűncselekmények az internetes csalások, a pornográf felvételek, valamint a személyes adatokkal való visszaélések. Jellemzőek még a szerzői jogsértések, ezekkel viszont 2011. január 1. óta a Nemzeti Adó- és Vámhivatal (NAV) foglalkozik.

74 Az NNI Csúcstechnológiai Bűnözés Elleni Osztályának vezetője.

7.1. A Nemzeti Kibervédelmi Intézet megalakulása

A 2013. évi L. törvény⁷⁵ módosításával⁷⁶, 2015. október 1-én megalakult a Kormányzati Eseménykezelő Központ (GovCERT-Hungary⁷⁷), a Nemzeti Elektronikus Információbiztonsági Hatóság, és a koordináltabb információáramlást lehetővé tevő Nemzeti Kibervédelmi Intézet⁷⁸. Az Intézet az elektronikus információs rendszerek teljes információbiztonsági életciklusára vonatkozóan feladatkörrel rendelkezik⁷⁹, feladata annak nyomon követése és segítése, a tervezési szakasz koordinálása, a szabályozás, ellenőrzés és incidenskezelés megvalósítása. Ennek céljából együttműködik az Információbiztonsági Hatósággal, az Eseménykezelő Központtal, valamint a Biztonságirányítási és Sérülékenységi vizsgálati területtel⁸⁰. Kapcsolatot ápol továbbá számos nemzetközi kibervédelmi szervezettel, úgymint az ENISA, a FIRST⁸¹, a TI⁸², az IWWN⁸³, illetve a *Central European Cyber Security Platform*⁸⁴. Feladata az ügyfelek és rendszerek nyilvántartása, a biztonsági osztályba és szintbe sorolás ellenőrzése, sérülékenység vizsgálat elrendelése, javaslattevő létfontosságú rendszer kijelölésére, valamint információbiztonsági felügyelő kirendelésére.

A napjaink információs társadalmát érintő fenyegetések miatt, kiemelten fontos a nemzeti elektronikus adatvagyon és az ezt kezelő információs rendszerek és rendszerelemek biztonsága. Az alapvető elektronikus információbiztonsági követelmények közé tartozik a kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása, valamint a rendszer és elemeinek sértetlensége és rendelkezésre állása. A szervezeteknek külön jogszabályban előírt logikai, fizikai és adminisztratív védelmi intézkedéseket kell meghatározniuk, melyek támogatják a megelőzést, a reagálást, az észlelést és a biztonsági események kezelését. A Nemzeti Elektronikus Információbiztonsági Hatóság feladatai közé tartozik az Európai Unió tagállamaiban történő elektronikus információs rendszer üzemeltetése, az EU tagállamokon kívül eső információs rendszerek ellenőrzése, és az információtechnológiai fejlesztési projektekben megjelölt követelmények érvényesülésének ellenőrzése. A Hatóság további kormányzati információtechnológiai és hálózatbiztonsági információ-megosztási, incidens-kezelési munkacsoportot működtet, amelynek fő profilja az információbiztonság növelése. A munkacsoport tagjait a Hatóság által felkért szervezetek, a szakhatóság és a kormányzati eseménykezelési központ delegálják.

75 2013. évi L. törvény az állami és önkormányzati szervezetek elektronikus információbiztonságáról.

76 2015. évi CXXX. törvény az e-kártya megvalósításához szükséges egyes törvények, valamint az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény módosításáról, <http://mkogy.jogtar.hu/?page=show&docid=A1500130.TV>.

77 A magyar kormányzat információ-megosztó és incidens-kezelő szervezete, szolgáltatásait a kormányzati szervezetek és az önkormányzatok részére nyújtja. Főbb feladatai a biztonsági események kezelése, ügyeleti szolgálat, elemzés/értékelés, kibervédelmi gyakorlat, képzés, tudatosítás, sérülékenység vizsgálat.

78 A Nemzeti Kibervédelmi Intézet a korábbi, E-biztonsági Intelligencia Központot (NBF-CDMA) egységes keretben magába foglalja, ezáltal hatékonyabb feladat-végrehajtást biztosít.

79 Rövid áttekintés a Nemzeti Kibervédelmi Intézet meg alakulásáról, működéséről és előzményeiről, www.hadmernok.hu/154_23_orboka.pdf.

80 Feladata a sérülékenység vizsgálat és a biztonsági események kivizsgálása, valamint az EMIR / FAIR rendszerekkel kapcsolatos informatikai biztonsági feladatok ellátása.

81 Forum of Incident Response and Security Teams.

82 Trusted Introducer.

83 International Watch and Warning Network.

84 Visegrádi Négyek és Ausztria kiberbiztonsági szervezeteit tömörítő platform.

8. Az online-tér devianciái

Mára mind a személyes használatban lévő, mind az üzleti vagy állami célra használt számítógépek és számítástechnikai rendszerek az elkövetők keresett eszközei, célpontjai lettek. Az internet technológiája nemcsak új bűncselekmények megjelenését idézte elő, hanem új teret adott a már létező és a büntetőjog által fenyegetett cselekményeknek is. Ezzel egyetemben számos újszerű deviáns magatartás tűnt fel az információs társadalomban, olyanok is, amelyek a társadalom egy korábbi technológiai fejlettségi szintjén a szükséges technológia hiányában nem létezhetek, és olyanok is, amelyek más formában, de jelen voltak a társadalomban.

Az online-tér devianciái a következők:⁸⁵ az internetes zaklatás, az internetes kibeszélés, a provokáló hozzászólás, a *sexting*⁸⁶, az internetes pedofília, az online behálózás, az online játékok és a személyes adattal való egyéb visszaélések⁸⁷. Tanulmányunkban – a teljesség igénye nélkül – a devianciák legelterjedtebb két formájával, az online zaklatással és egyes típusaival, valamint az adathalászattal foglalkozunk kiemelten.

Az elkövetők indítéka, valamint az elkövetés célja, módja és célzott személyi köre alapján, eltérő zaklatási típusokról beszélhetünk. Eszerint a zaklatás munkahelyi, szexuális, faji-etnikai alapú vagy személyes indíttatású cselekvésként kategorizálható. A munkahelyi, szexuális zaklatók főként olyan férfiak, akik pozícióféltségből, hatalmi erőfölényükkel visszaélve, vagy szexuális kapcsolat létesítésére keresik áldozataikat. Az Európai Parlament és a Tanács társjogalkotásából született 2002/73/EK irányelv tartalmazza a diszkriminációval és szexuális zaklatással kapcsolatos legújabb rendelkezéseket. A faji-etnikai megkülönböztetés elleni küzdelem fegyvere az Európai Tanács 2000/43/EK irányelve, mely a faji- vagy etnikai származásra való tekintet nélküli, egyenlő bánásmódot hirdet. A legtöbb zaklatásról elmondható, hogy a sértett és a tettes között a cselekmény megvalósulása előtt már valamilyen kapcsolat áll vagy állt fenn. Hazánkban először a 2003. évi CXXV. törvény⁸⁸ említette a zaklatást, olyan magatartásként, mely az egyenlő bánásmódot, az emberi méltóságot sértő, szexuális vagy egyéb természetű jelenség, amelynek célja valamely személlyel szemben ellenséges, megfélemlítő, megszégyenítő vagy támadó környezet kialakítása.⁸⁹ A jogalkotó célja azon súlyosabb jogszétsékek pönalizálása volt, melyek más személy rendszeres vagy tartós háborgatását eredményezik, jelentős érdeksérelmet okozva a magánéletébe való önkényes beavatkozással. A törvény indokolása szerint általános tapasztalat, hogy a zaklató magatartása az idő múlásával egyre fenyegetőbb, durvább lesz, ami súlyos pszichés zavarokhoz, de akár tulajdon vagy személy elleni erőszakos bűncselekmények elkövetéséhez is vezethet.

A hatályos jogi szabályozást a 2012. évi C. törvény rendelkezései között találjuk. Az információs társadalom devianciáinak jelenléte nagymértékben az infokommunikációs technika elterjedt használatához köthető. A devianciák a társadalmi értékrendek, szokások változását is példázzák. Amíg egy-egy új magatartás nem rendelkezik egységes társadalmi megítéléssel, addig a hazai büntetőjog sem mutathat megfelelő szankcionálást. Mivel az infokommuni-

85 Nemzeti Adatvédelmi és Információszabadság Hatóság: Kulcs a net világhoz! www.naih.hu/files/2013-projekt/fuzet-internet.pdf

86 L. 8.1.2. Sexting.

87 L. 8.2. Adathalászat: phishing és pharming.

88 2003. évi CXXV. törvény az egyenlő bánásmódról és az esélyegyenlőség előmozdításáról, http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0300125.TV.

89 Uo., 10. § (1.) bek.

kációs eszközök könnyen elérhetők, így a fiatal generációk nagyobb része birtokolja, és napi rendszerességgel használja őket. Meglátásunk szerint a technológia terjedésének jelentős hatása van az interneten elkövetett bűncselekmények növekedésére.

8.1. Cyberbullying

A zaklatás napjainkra mindennapossá nőtte ki magát az internetes világban. A *cyberbullying* egy új típusa az elsősorban tinédzser korúak közt tapasztalható iskolai kiközösítésnek. Megvalósulhat fenyegető üzenetek formájában, *grooming*⁹⁰ során, az áldozat nevében vagy akár személyes adataival való visszaéléssel is. A gyermekekre káros internetes tartalmak kiszűrését támogató Biztonságos Böngészés Programhoz (BBP) már több száz iskola csatlakozott, illetve több ezer munkaállomás programtag. A BBP projekt során a diákok által használt komputerekre olyan szűrőszoftvereket telepítenek, melyek kiszűrik a fiatalokra káros tartalmakat és az internetes zaklatást. Magyarországon a gyerekközösségekben megnyilvánuló erőszakra egyre több figyelem vetődik. A Nemzeti Média- és Hírközlési Hatóság 2011-től elrendelte az *Eu Kids Online I-III* projekteket, amelyek átfogó célja a gyerekek internethasználati jellegzetességeinek, illetve az ezekhez kapcsolódó kockázatok és veszélyek megismerése, megértése. A felmérés szerint a magyar gyerekek 19%-át érte a kérdezést megelőző évben a kortársai részéről zaklatás. Az érintettek 73%-át személyesen érte a sérelem, és csupán 30%-ukkal fordult elő az interneten (is).

Az internetes zaklatások helyszínei nagyrészt a közösségi oldalak és az azonnali üzenetküldők. A zaklatottak 49%-a említette ezt a két alkalmazást a zaklatás 'helyszínéül'. A gyerekek 15%-a maga is viselkedett már zaklatóan a világhálón. A projekt eredményei azt mutatják, hogy bár a magyar gyerekeket viszonylag kis számban érintik a vizsgált kockázatos tevékenységek, a tanácsadóknak és szülőknek fel kell készülniük a veszélyeztetettség eme új dimenzióira. A *cyberbullying*nek számos alfaja ismert, ezek közül kiemelendő a *flaming*, az identitáslopás, a *stalking* illetve a *sexting*. A *flaming*⁹¹ során a fórumokon trágár hozzászólások kerülnek a nyilvánosság elé, a vita gyakran vallási, ideológiai vagy politikai kérdéseken alapszik. Az identitáslopás gyakran jár az áldozat e-mail fiókjának vagy közösségi oldalának feltörésével; legtöbbször azzal a szándékkal történik, hogy a nevében kompromittáló üzenetet továbbítsanak ismerősei számára. A *cyber-stalkingot* elszenvetettek folyamatos fenyegetés alatt állnak, adataik vagy online szokásaik rendszerint erőszakos tartalmú üzenetek formájában kerülnek nyilvánosságra, ezáltal az elkövetők a veszélyeztetettség érzését keltik bennük. Végül, de nem utolsósorban a *sexting* provokatív, szexuális tartalmú fényképek, videók készítését és terjesztését jelenti, melyek napvilágra kerülése akár egy életen át üldözheti a szívenbe hozott személyt.

Fontosnak tartjuk hangsúlyozni, hogy minden korosztály válhat internetes bűncselekmények áldozatává, életkortól függetlenül. A megfelelő szakértelemmel, technológiai ismeretek

90 Bár a grooming, azaz az online behálózás önmagában nem bűncselekmény, alkalmas a gyermekek személyes adatainak kicsalására, „szexuális játékokba” való bevonására, az áldozatok szégyenérzetének erősítésére.

91 A flaming vagy másnéven flame war során szándékosan jogsértő, ellenséges, témához nem kapcsolódó hozzászólásokat küld az elkövető az internetes fórumra. A kifejezés mára bizonyos fókig elavult, pontosabb definíció lehet a problémakörre a trolling, mely azonban valamivel tágabban, a teljes provokatív, vitagerjesztő magatartást leírja.

elsajátításával, helyzetük mihamarabbi felismerésével viszont jelentősen mérsékelhető a bűnelkövetési ráta. Konkrét segítséget jelenthet, ha a lehető leggyorsabban eltávolítják a veszélyes tartalmakat, ezért fontos, hogy a hatóságok és civil szervezetek együttműködjenek az áldozatokkal és azok hozzátartozóival. Sosem lehetünk eléggé felkészültek az internetes kockázatok és ártalmak semlegesítésében. A megfelelő kezeléshez először a probléma létezésének tudatosítására kell rávilágítanunk.

8.1.1. *Cyber-stalking*

J. Reid Meloy napjaink egyik kiemelkedő pszichológus professzora, aki az Egyesült Államok tagállamaiban megjelenő, zaklató magatartásokat kutatja. Kutatásai szerint a *stalking* fogalma tagállamról tagállamra változik, néhány fogalmi elem azonban minden definícióban megtalálható. Eszerint a *stalking* olyan másra irányuló, nem kívánt, háborgató viselkedés, amely burkoltan vagy kifejezetten fenyegető, és hatására a megfenyegetett komoly félelmet érez.⁹² Pszichiátriai-klinikai értelemben, a *stalking* meghatározott személy rendellenes vagy tartós fenyegetése vagy nyugtalanítása. Akkor tekinthető egy fenyegetés komolynak, ha az egy ésszerűen gondolkodó személyben nagymértékű aggodalmat kelt, ha az áldozat hisz abban, hogy az elkövető beváltja fenyegetéseit, vagy ha azok jelentős érdeksérelemmel jártak.

A zaklatás nem kizárólag az áldozatra korlátozódik, érintheti annak barátait, családtagjait, a tulajdonát, és az elkövetőnek tisztában kell lennie tettei súlyával. A személyes jellegű inzultálás elkövetője rendszerint hosszabb ideje, visszatérően molesztálja áldozatát az infokommunikációs környezetben. Az internet és a mobiltechnológia alapvetően két lehetőséget teremt az elkövető és áldozata kapcsolatát tekintve: a távoli hozzáférést és az állandó hozzáférhetőséget. A távoli hozzáférés annak lehetőségét biztosítja, hogy az elkövető bárhol is tartózkodjon, elérje áldozatát. Az állandó hozzáférhetőség az áldozat helyzetétől független. Egyes kommunikációs módok, például az e-mail vagy a *chat* csak írásbeli alapúak, az észlelés más módon nem valósul meg. A kommunikáció során nincs hang, mely segítene a közlő nemének, életkorának felismerésében, nem értelmezhető reakciói, mimikája. Ugyanakkor az üzenetek mellé csatolt képek, zenék, linkek árulkodóak lehetnek a zaklató szándékait illetően. Emocionális és fizikai távolságot létesít az elkövető és áldozata között a közvetlen kapcsolat hiánya, mely az elkövetés érzelmi megkönnyítéséhez vezet. A *stalking* nem kizárólag e két fél között zajlik, példának okáért a *proxy-stalking* megvalósításával, a tettes más online résztvevőket befolyásolva érheti el egy személy zaklatását.

J. Reid Meloy szerint az internetnek sokoldalú szerepe van a zaklatás során. Egyrészt eszközként szolgál az elkövetőnek az információgyűjtéshez, másrészt olyan kommunikációs csatorna, melyen keresztül az áldozat könnyen megfenyegethető, inzultálható. Nem utolsó sorban az időhöz fűződő függetlensége miatt azt az érzetet keltheti a sértettben, hogy zaklatója bárhol, bármikor a közelében van. Az anonimitás az áldozat alávetettségét fokozza, azt az érzetet kelti benne, hogy az elkövető a környezetéből bármely személy lehet.

92 J. Reid MELOY: Stalking – An Old Behaviour, A New Crime. *The Psychiatric Clinics Of North America* (1999) 85. www.drreidmelo.com/wp-content/uploads/2015/12/1999_Stalking_anOldB.pdf.

8.1.2. Sexting

Félelem, depresszió, szorongás, önértékelési problémák: csak néhány olyan következmény, melyeket a zaklató magatartások okoznak. A *sexting* során a felhasználók önmagukról készített erotikus tartalmú fényképeket, videókat és szexuális töltetű üzeneteket küldenek egymásnak infokommunikációs eszközeikkel, vagy e felvételeiket internetes közösségi oldalakon közzéteszik. A jelenség a tinédzser korosztályt érinti a legszámtottevőbben, ennek valószínűsíthető oka a serdülő korosztály szexuális túlfűtöttsége, kísérletező magatartása, illetőleg tetteik súlyosságának fel nem ismerése. Míg a *cyber-bullying* más magánszférájának a semmibe vételét jelenti, addig a *sexting* a felhasználó saját magánszférájának teljes nyitottságát eredményezi. A magyar társkereső oldalakra évente több ezer gyermekpornográfiával kapcsolatos hirdetés kerül fel. A *Pew Internet & American Life Project* nevű, független Egyesült-államokbeli szervezet 2009-es kutatása alatt összegyűjtött adatokból az derül ki, hogy a 12 és 17 év körüli korosztály 15%-a kapott már erotikus jellegű képet Amerikában. Az *Eu Kids Online* felmérés⁹³ második projektjének adataiból kiderült, hogy a 9-16 éves magyar gyerekek csaknem 16%-a találkozott már szexuális jellegű képpel, vagy videóval. ⁹⁴Az érintettek 4%-a mondta, hogy napi szinten találkozik ilyen felvételekkel, 13%-uk egyszer-kétszer a héten, 19%-uk egyszer-kétszer a hónapban, míg 49%-uk ennél ritkábban. ⁹⁵ Ez azt jelenti, hogy a teljes 9-16 éves korosztály 10%-a szembesült ilyen jellegű tartalommal az interneten. Ugyanakkor a pornográf felvételek még mindig fontos forrása a televízió illetve a filmek, az érintettek csaknem fele és a teljes korosztály 8%-a ezeken a csatornákon jutott hozzá a tiltott tartalmakhoz. Az érintettek csaknem harmada állította, hogy automatikusan felugró lapokon látott ilyeneket, 29%-uk videómegosztó-oldalakon, negyedük pedig felnőtteknek szóló, korhatáros oldalakon látta a képanyagokat. A szexuális jellegű üzenetekkel kapcsolatos kérdések csupán a 11 éves és annál idősebb gyerekek kérdőívében szerepeltek. A 11-16 év közötti fiatalok 7%-a állította, hogy a kérdezést megelőző egy évben kapott szexuális jellegű üzeneteket az interneten keresztül. 62%-uk a havi gyakoriságnál ritkábban kapott ilyen üzeneteket, 21%-uk havonta, 7%-uk hetente, 4%-uk pedig naponta szembesült ilyen levelekkel. ⁹⁶

A fiúknak és az idősebbeknek nagyobb esélyük van arra, hogy ilyen üzeneteket kapjanak. Minél régebben használja valaki a világhálót, annál valószínűbb, hogy érkezik hasonló üzenete. A szexuális jellegű tartalmak legtöbbször vagy véletlenül jutnak el a fiatal korosztályhoz, vagy üzenetküldőn keresztül kapják azokat. A legtöbb esetben konkrét üzenetről van szó, de előfordul az is, hogy valakit arra kérnek, vegyen részt szexuális jellegű párbeszédben vagy intim testrészéről osszon meg fotókat. Gyakori még, hogy az érintett fiatal másvalakik szexuális aktusának lesz tanúja valamiképp az interneten. A megkérdezett gyermekek csupán 1%-a állította, hogy *sextingelt* már. A magyar gyerekek csaknem negyede került már kapcsolatba olyan emberrel a világhálón, akit nem ismert. Harmaduk személyesen is találkozott valamilyen ismeretségével. Ez azt jelenti, hogy a 9-16 évesek 7%-a vett már részt ilyen találkozókon. Már a 13-14 évesek körében is átlag feletti az ismerkedők aránya, ami azonban a

93 L. 8.1. Cyber-bullying.

94 EU Kids Online II. A magyarországi kutatás eredményei – Készült a Nemzeti Média- és Hírközlési Hatóság megrendelésére. Szerkesztő: ITHAKA Nonprofit Kft., 2011. szeptember.

http://nmhh.hu/dokumentum/3886/ITHAKA_EU_KIDS_Magyar_Jelentes_NMHH_Final_12.pdf

95 Uo., 3-4.

96 Uo., 5.

15-16 éves korosztálynál 43%-ra ugrik. Az internetet tapasztaltabban, napi szinten használók nagyobb arányban alakítanak ki ilyen kapcsolatokat.⁹⁷A 15-16 éves, online ismeretséget kötő lányok csaknem fele találkozott már interneten megismert személlyel.

Érdekes tény, hogy Új-Mexikóban legálissá tették a *sextinget*, így a serdülő korosztály is szabadon oszthat meg szexuális tartalmakat egymás között. George Muñoz szenátor szavával élve, a gyerekek mindig gyerekek maradnak, és el fognak követni hibákat. Az államfő szerint nem lehet életük végéig büntetni őket azzal, hogy gyermekpornográfia terjesztésével vádoljuk őket. Az állampolgárok többsége osztja Muñoz szenátor véleményét, egyesek szerint azonban ezzel egy kiskaput nyitottak a pedofilok számára, akik így egyszerűbben és gyakrabban követhetnek majd el gyermekpornográfiával kapcsolatos tevékenységeket. Az Európai Parlament az interneten terjedő pedofil tartalmak alaposabb kivizsgálását, az elkövetők bíróság elé állítását, az áldozatok védelmét és az illegális tartalmak eltávolítását szorgalmazza.

8.2. Adathalászat: phishing, pharming

A *cybercrime* elkövetésének egy másik lehetséges esete az adathalászat. A *phishing* támadások során kiberbűnözők potenciális áldozatok millióinak küldenek levelet világszerte, amelyekkel átverik vagy támadják őket. Az üzenetek látszólag megbízható forrásból érkeznek, gyakran sürgető határidővel egybekötve, és a mit sem sejtő online felhasználók személyes adatainak, banki azonosítóinak, jelszavainak megszerzését célozzák. A *pharming* során, ezt tetéztve a levelek általában egy káros kódot tartalmazó, támadó honlapra mutatnak. Támadónak nevezzük az olyan weboldalakat, melyek megpróbálják rosszindulatú szoftverrel (*malware*) megfertőzni a látogatók számítógépét. A *malware*-eket személyes adatok elsajátítására, levélszemét küldésére, számítógép és cserélhető meghajtóinak megfertőzésére, illetve további hasonló szoftverek terjesztésére használják. Az is előfordulhat, hogy az adathalász levél egy fertőzött mellékletet tartalmaz, mely megpróbálja beszennyezni gépünket és átvenni felette az irányítást. A *spear phishing*, vagyis célzott adathalász támadás során a támadók jóval célirányosabb leveleket küldenek, az áldozatok listája ez esetben igen rövid, körülbelül 5-10 tagból áll. Ennek célja a kiszemelt 'célpontok', felhasználók, online szokásainak tanulmányozása, például Google- vagy Facebook fiókjaik átolvasásával, fórumokon közzétett üzeneteik vizsgálatával. Ezt követően a támadók egy személyre szabott, relevánsnak tűnő levelet készítenek a kiszemelt személy számára, így az még nagyobb valószínűséggel válhat áldozattá. A célzott adathalászat sokkal veszélyesebb fenyegetés az egyszerű adathalász támadásoknál, mivel e támadások felfedése is jóval nehezebb.

A támadásokkal szembeni védekezés első lépése annak megértése, hogy mi magunk is lehetünk célpontok. Mi, illetve a cégünk is birtokolhat olyan bizalmas információt, amelyet valaki más szeretne megszerezni. Minél több személyes információt osztunk meg magunkról az online-térben, annál kiismerhetőbbek, egyúttal támadhatóbbak leszünk a támadók számára. A legelterjedtebb webböngészők már felveszik a harcot az adathalászok ellen, a biztonsági csomagokból ismert phishing szűrő vészjelzést ad a gyanús oldalak meglátogatásakor. Eszerint elkülöníthetjük a megbízható oldalak fehér listáját és az ismert phishing oldalak fekete listáját, melyek ezután automatikusan frissülnek a számítógépen. A rendszeresen fris-

97 Uo., 7.

sített operációs rendszer és tűzfal jó alapjai a támadások elkerülésének. Lényeges továbbá a homográf⁹⁸ weboldalak elkerülése, és gyanakvásunk állandó fenntartása.

8.2.1. A phishing szabályozásának új koncepciója

A *cybercrime* legsérülékenyebb szereplője maga a felhasználó, ezért fogékonyabbá kell tenni a 'kiberéberségre'. Ennek orvoslását a hazai internetszolgáltatókra vonatkozó jogszabályok módosításában látjuk, úgy gondoljuk, hogy lényeges lenne a strukturált adatszolgáltatási kötelezettség előírása számukra. Az általuk alkalmazott kéretlen levél-szűrő rendszerekre, implementált adatfeldolgozó alkalmazások készítését javasoljuk. Az adatgyűjtés kulcsfontossága megkívánja egy ennek folytatására szakosodott szerv életre hívását, esetleg egy már működő szervezet kijelölését erre a feladatra. Úgy véljük, hogy a Nemzeti Kibervédelmi Intézet erőforrásai és képességei tekintetében alkalmas lehet erre a pozícióra.

A vállalatok kötelességévé javasoljuk tenni a kockázatok tudatosítását a társadalmi szférával, oktatási és egyéb kezdeményezéseiken keresztül. Ennek azért látjuk szükségét, mert a *cybercrime* legsérülékenyebb szereplője maga a felhasználó, ezért fogékonyabbá kell tenni a 'kiberéberségre'. Az IT-cégek ehhez szoftvereik biztonságosabbá tételével járulhatnak hozzá. Egyre több szervezet beszél nyíltan az elszenvedett adatlopásokról, online támadásokról, az Egyesült Államokban erre már törvény is kötelezi őket. Hogy egy példát említsünk, a CNN Money oldalán megjelent cikk szerint, 2016 szeptemberében amerikai olimpiai bajnokok egészségügyi adatait is hackertámadás érte.⁹⁹ Egy erre irányuló törvényi kezdeményezés a hazai szabályozásra is pozitív hatással lenne, a piaci szereplők körében redukálna az elhallgatott biztonsági események száma. A vállalatok és intézmények rendszerei sérülékenyek, feltörhetők, ezt nem szabad elhallgatni, hiszen az információk megosztása mindannyiunk biztonságát növelheti.

Európai uniós fejleményként említhető, hogy a 2016-os holland uniós elnökség idején a tagállamok elfogadtak egy törvényjavaslatot, amely a szervezeteket a biztonsági események felelősségteljes nyilvánosságra hozatalára köteleznél, ez pedig kedvezően hatna a következmények kezelésére és elhárítására. Kiváló védekezési módszernek tartjuk az egyre ismertebb kiberhírszerzést is, mely a fenyegetési környezetet világszinten elemzi, és az összegyűjtött információkból regionális sajátosságokat azonosít, amelyekkel a biztonsági cég akár egy kibontakozó támadás kivédésére is képes lehet. Ennek naprakész működéséhez szükséges lenne az ügyféloldalon is felállítani egy biztonsági műveleti központot. A *threat intelligence*¹⁰⁰ szolgáltatások hazai bevezetését a vállalatok korlátozott pénzügyi lehetőségei is nagyban befolyásolják, ezek azonban rendkívül hasznos eszközök lehetnek a kibertámadások kivédésében.

Támogatjuk továbbá az ún. *bug bounty* programok¹⁰¹ létrehozását, melyek a hibakereső magánszemélyek elismerésével és jutalmazásával a szervezetek sérülékenységeinek

98 A számítástechnikában a homográfia olyan webcímet jelent, amely látszólag ismert cím, de valójában eltér attól. Az adathalászat során használt hamis webhivatkozások célja az áldozat megtévesztése.

99 Ivana KOTTASOVA: Hackers steal medical data of US Olympic stars. money.cnn.com/2016/09/13/news/wada-hacked-russian-spies/index.html.

100 E szolgáltatások célja, hogy a vállalatok proaktívan részt vegyenek a fő infrastruktúrájukban, adataikat és vezetőiket célzó kibertámadások felismerésében, azonosításában és az ellenük való védekezés során.

101 Hibafelderítési jutalomprogram, mely biztonsági rések felkutatására szolgál.

vizsgálatát és fejlesztését indukálhatják. Az etikus hackereket¹⁰² anyagi megfontolásból csupán alkalmanként veszik igénybe a szervek, de jó, ha róluk sem feledkezünk meg: az Óbudai Egyetemen és a KÜRT Akadémián már képzésük is zajlik, mely az EC Council által kiadott *Certificied Ethical Hacker* képzettség megszerzésével jár együtt. Összességében mind felhasználói, mind vállalati szinten szükség van módosításokra, melyek alkalmazásával az adathalászat egy sokkal áttekinthetőbb és könnyebben leküzdhető jelenséggé válhat.

9. A jogellenes tartalmak és a cybercrime viszonya

Hazánkban az önálló internetjog hiánya és a sajtótermékek interneten való közlése számos jogi problémát felvet. Az első felmerülő kérdés, hogy maga az internet önálló sajtóorgánumként kezelhető-e a rajta keresztül történő közlés esetén, tehát kiterjed-e rá a sajtótörvény sajtótermékekre vonatkozó meghatározása, avagy sem? A 2010. évi CIV. törvény 1.§-ának értelmében sajtótermék:

„[a] napilap és más időszaki lap egyes számai, valamint az internetes újság vagy hírportál, amelyet gazdasági szolgáltatásként nyújtanak, amelynek tartalmáért valamely természetes vagy jogi személy szerkesztői felelősséget visel, és amelynek elsődleges célja szövegből, illetve képekből álló tartalmaknak a nyilvánossághoz való eljuttatása tájékoztatás, szórakoztatás vagy oktatás céljából, nyomtatott formátumban vagy valamely elektronikus hírközlő hálózaton keresztül.”

A hatályos szabályozás tehát arra ad bizonyítékot, hogy az internetes tartalmak önálló sajtótermékként kezelendők.

Az internet szereplői: a felhasználó¹⁰³, a hozzáférést biztosító szolgáltató¹⁰⁴, az internet-tartalmat nyújtó szolgáltató és az internet-szolgáltatást nyújtó szolgáltató. Az online világban minden jogsértő lépésnek jogi következményei lehetnek: a jogellenes tartalomért¹⁰⁵ pedig nemcsak a tartalom-, hanem az internetszolgáltató is felelőssé tehető, tartalomhoz fűződő kapcsolatának erőssége szerint. Tartalomszolgáltatónak nevezzük az interneten megjelenő tartalom megalkotóját, internetszolgáltatónak pedig azt, aki az interneten elérhetővé teszi a tartalmat, és tényleges internet-szolgáltatásokat nyújt (tárhely fizikai biztosítása, tárhelyet megkönnyítő program elkészítése és futtatása, e-mail cím biztosítása, stb.). A továbbiakban az internetszolgáltató kifejezést fogjuk alkalmazni az internetszolgáltatást nyújtó szolgáltatókra.

102 Speciálisan képzett informatikai biztonsági szakértő, aki képes a vállalati informatikai rendszerek sérülékeny pontjainak felderítésére, a csálások felfedezésére, és megoldási javaslatokat tesz a problémák kezelésére.

103 A felhasználó veszi igénybe a másik három szereplő által nyújtott szolgáltatásokat. A hozzáférés-szolgáltatóval szerződéses kapcsolata is fennáll. Ő az előállított tartalom tulajdonképpeni fogyasztója, és lehetősége van arra, hogy ő maga is tartalom-szolgáltatóvá váljon.

104 A gyakorlatban mára nemcsak kizárólagos hozzáférést biztosít, hanem egyéb szolgáltatásokat is nyújt (pl. e-mail cím, tárhely), ezáltal egyre kevésbé különíthető el az internet-szolgáltatást nyújtó szolgáltatóktól.

105 A büntetőjogba ütköző, illetve az ártalmas tartalom.

9.1. Az egyes tartalmak közötti különbségtétel

A kiskorúak védelmének érdekében, lényegesnek tartjuk az internetes tartalmak kategorizálását. A korlátozás megengedhető intenzitásának mércéje vonatkozásában, a tartalmak két csoportját különbözteti meg az Európai Bizottság¹⁰⁶ a korlátozhatóság mértéke alapján differenciálva a jogellenes és a káros tartalmak között. Egyes jogellenes tartalmak magánjogi, mások büntetőjogi szabályozás alá esnek. Magánjogi szabályozás alá esik a szerzői jogot sértő, diszkriminációra alkalmas közlés, valamint a más képmásával, személyes adataival való visszaélés. Az erőszakot, gyermekpornográfiát ábrázoló tartalomra, a gyűlöletkeltésre és az online zaklatásra (emberi méltóság megsértése) a büntetőjog (is) irányadó. A kiskorúak szellemi, lelki, erkölcsi vagy fizikai fejlődésének káros befolyásolására alkalmas azon média-tartalom, amely pornográfiát vagy szélsőséges, illetve indokolatlan erőszakot tartalmaz.¹⁰⁷ Kiemelten fontos ezért az egyes kiberbűncselekmények és az ezek során megjelenő jogellenes vagy káros tartalmak átfogó, összevont vizsgálata. E két típus közötti legfőbb különbséget az adja, hogy a jogellenes tartalmak teljes egészében tiltottak mindenki számára, míg a káros tartalmak – bár nem jogellenesek –, a kiskorúak számára nemkívánatosak. Ebből kifolyólag a két kategória más-más megközelítést és megoldásokat kíván. A jogellenes (illegális) tartalmak nem élvezik a véleménynyilvánítás szabadságának védelmét, azok a szabad véleménynyilvánítás alkotmányos jogának védelmi zónáján kívül esnek, az ilyen közlésekhez való hozzáférés a társadalom minden tagja számára tilalmazott, függetlenül a felhasználók életkorától, a hozzáférés módjától, illetve a címzetti körtől. A káros (ártalmas) tartalmakra kiterjed a véleménynyilvánítás szabadsága, eszerint szabadon közzétehető és terjeszthetők. Az ilyen tartalmak a felnőttek számára hozzáférhetőek, a kiskorúak számára azonban ártalmasnak minősülnek, mert erős befolyásoló erővel bírnak a gyermekek fizikai, szellemi, erkölcsi fejlődésére. Indokolt ezért, hogy e tartalmak elérhetőségét az adott médium sajátosságaihoz mérten, valamennyi médium adekvát technikai eszközeivel korlátozza.

Szükséges olyan eszközök meghatározása és alkalmazása, amelyek biztosítják a kiskorúak számára a káros tartalmakkal szembeni védettséget, nem korlátozva a felnőttek további hozzáférését. Kiskorúakra ártalmasak lehetnek az erőszakos és a szexuális tartalmak, a kábító-szer-és alkoholfogyasztás megjelenése, valamint a trágár nyelvhasználat. A kiskorúak védelme érdekében az internet valamennyi szereplője és az állami szabályozás együttes fellépése szükséges, és ennek érdekében célszerű a kiskorúak közötti, korosztályonként való különbségtétel, hogy a védelem minél differenciáltabb lehessen.

A káros tartalmak megítélését az államok értékrendje, erkölcsi és kulturális felfogása is befolyásolja. E médiatartalmak kérdését két törvény rendezi, az Smtv.¹⁰⁸, illetve az Mttv.¹⁰⁹. Az Mttv. 9. §-a hat kategóriába (I.-VI.) sorolja a műsorszámokat attól függően, hogy azok milyen életkorú nézők számára ajánlottak (klasszifikáció). A lineáris médiaszolgáltatók által a különböző korcsoportoknak ajánlott műsorszámok, meghatározott időintervallumban tehetők közzé az Mttv. 10. §-a alapján. Internetes sajtótermékek esetén az Smtv. 19. §. (3) bekez-

106 E megkülönböztetést az Európai Bizottság által 1996-ban kiadott „A kiskorúak és az emberi méltóság védelméről az audiovizuális és információs szolgáltatásokban” című Zöld Könyv alkalmazta először.

107 2010. évi CIV. törvény a sajtószabadságról és a médiatartalmak alapvető szabályairól (a továbbiakban: Smtv.) 19. § (1) – (4) bek.

108 Uo.

109 2010. évi CLXXXV. törvény a médiaszolgáltatásokról és a tömegkommunikációról.

dése az irányadó, mely leírja, hogy azon médiatartalmak, melyek pornográfiát vagy szélsőséges, illetve indokolatlan erőszakot tartalmaznak, illetve súlyosan károsíthatják a kiskorúak szellemi, lelki, erkölcsi vagy fizikai fejlődését, csak valamely műszaki vagy egyéb megoldás alkalmazásával tehetők közzé, ezzel biztosítva, hogy a kiskorúak ezen tartalmakhoz ne férhessenek hozzá. Ha ilyen megoldás alkalmazása nem lehetséges, akkor az Smtv. rendelkezése alapján, a médiatartalom csak a kiskorúak lehetséges veszélyeztetéséről szóló tájékoztatást tartalmazó, figyelmeztető jelzéssel tehető közzé. Ugyan a lineáris médiaszolgáltatások esetén a klasszifikációs szabályok, mint tartalomszabályozás bevezetésére van lehetőség, ez hasonló formában a lekérhető tartalmak esetében nem lehetséges.

Az NMHH Médiatanácsa ajánlást tett közzé¹¹⁰ a lekérhető és lineáris médiaszolgáltatások esetén alkalmazott hatékony műszaki megoldások fejlesztése céljából. Az ajánlás egy gyerekszűrő program (gyerekzár) telepítését javasolja a kiskorúak számára káros tartalom elérése előtti figyelmeztetés mellett. A megoldás két okból is előremutató: egyrészt nem okoz versenyhátrányt a hazai médiatartalom-szolgáltatóknak, mivel a káros tartalmakat nem teszi elérhetetlenné, másrészt jelentősen segíti az edukációt azzal, hogy a szülőknek a nem csak magyarországi tartalomszolgáltatóktól származó káros tartalmak szűrésére is alkalmas, gyermekszűrő szoftver telepítését javasolja.

9.2. Az internetszolgáltatók felelőssége

Az internetszolgáltatók, ahogy az már említésre került, tartalomhoz fűződő kapcsolatuk erőssége szerint oszthatóak. Eszerint beszélhetünk teljes, korlátozott, illetve csekély befolyású internetszolgáltatókról. A tartalom feletti teljes befolyás esetén az internetszolgáltató saját tartalmat is közzétesz az interneten, tehát tartalomszolgáltatóként is fellép. Korlátozott a befolyása akkor, ha nem tesz közzé saját tartalmat, csupán a más által létrehozott tartalmat szerkeszti, s csekély a befolyása akkor, ha műszaki segédletet nyújt, ennek leggyakoribb példája a *hosting*¹¹¹. A jogellenes tartalomért való felelősség szempontjából csak az internetszolgáltatók felelőssége lehet kétséges, a tartalomszolgáltatók felelősségének jellemzői nem képezik vita tárgyát. Az internetszolgáltatók számára az „Elektronikus kereskedelemről szóló 2000/31/EK irányelv” határozza meg azokat a feltételeket, amelyek esetén mentesülnek a jogellenes tartalom miatti felelősség alól. E feltételek szerint a szolgáltató akkor mentesül, ha csupán közvetíti a tartalmat és nem ő kezdeményezi az átvitelt, nem ő választja ki az átvitel címzettjét és a továbbított tartalmat, illetve nem is módosítja azt. Mindez természetesen csak abban az esetben érvényesül, ha az internetszolgáltató azonnal eltávolítja a jogellenes tartalmat és meggátolja a hozzáférést. Harmadik személy tartalmának tárolása esetén akkor mentesül a szolgáltató, ha nincs tudomása arról, hogy a tevékenység jogellenes, de amint tudomására jut, végrehajtja az előbbieken elvártakat. Lényeges továbbá, hogy a hozzáférésszolgáltatók és hálózatszolgáltatók nem tehetők felelőssé a segítségükkel áramoltatott tartalomért.

110 A Médiatanács ajánlása a kiskorúak védelmében a lineáris és lekérhető médiaszolgáltatók által alkalmazandó hatékony műszaki megoldásokra (aktuális változat), http://nmhh.hu/cikk/184785/%20A_Mediatanacs_ajanlasa_a_kiskoruak_vedelmeben_%20a_linearis_es_lekerheto_mediaszolgáltatok_alta_alkalmazando_hatekony_muszaki_megoldasokra_aktualis_valtozat

111 Az internetszolgáltató a felhasználó tartalmát saját rendszerében tárolja, vagy a már rögzített tartalmat továbbítja.

9.3. A hiperlink (hiperhivatkozás) mint a jogsértés eszköze

A hiperhivatkozás egy olyan informatikai eszköz, amely egy adott (szöveges) tartalomban kerül elhelyezésre oly módon, hogy másik tartalomra mutat. A felhasználót választása esetén (kattintást követően) a jól azonosítható színében eltérő *hiperlink* átvezeti a javasolt oldalra, és az ott található tartalomra.

Az internet sajátosságaként említhető, hogy egyik honlapról a másikra mutató hivatkozások, úgynevezett hiperlinkek helyezhetők el rajta, amelyek ráklikkeléssel a jelzett oldalra vezetik a felhasználót. A phishinget¹¹² elkövető kiberbűnözőknek az egyik kedvelt elkövetési technikája a hiperhivatkozások alkalmazása. Amennyiben a hiperhivatkozás által felajánlott tartalom jogellenes, a hiperlink elhelyezése és annak jogsértéshez való kapcsolata vizsgálat tárgyát képezi, kapcsolatuk erősségének arányában a jogsértés különböző mértékű felelősséget von maga után, s első, avagy második szintű hiperkapcsolatról beszélhetünk. Az első szintű hiperkapcsolatnak két esete fordulhat elő, az egyik, amikor a klikkelés új ablakot hoz létre a képernyőn, és ezáltal az előző oldal nem található, a másik eset során a kattintással a felhívott honlap beágyazott linkként beépül az eredeti weboldalba. Ez utóbbi esetben a kapcsolat erősebb, a tartalomért való felelősség valószínűsíthető. Második szintű a hiperkapcsolat, ha a weblap egy másik weboldalra utal, amely egy harmadikra mutat. Nem tételezhető fel azonban az eredeti oldalon hiperkapcsolatot szolgáltató felelőssége, ha a jogsértő anyagot a harmadik weboldal tartalmazza.

9.4. A jogellenes tartalmak blokkolása

Az állami szervek által fogatosított internetblokkolási lehetőségek számbavétele kiemelten fontos a jogellenes tartalmak elleni fellépésben. Az internetblokkolás eszközül szolgál a felhasználók online tartalmaktól való megóvásához. A blokkolással lehetséges az elérhető tartalom korlátozása, a tartalomközvetítő IP címek hozzáférhetetlenné tétele, a weboldalak eltávolítása, valamint a szűrőprogramok használata is, amelyek szintén a tartalom elérhetetlenné tételére szolgálnak.

Az alapvető jogok védelme érdekében, a blokkolás módját minden esetben körültekintően kell megválasztani. Az illegális tartalom három módon szűrhető ki: önszabályozással¹¹³, korregulációval, illetve kógens szabályozás által. Az önszabályozás kedvelt eszközei a tűzfalak és a szűrőszoftverek, ezek elsődleges szintű védelmet nyújtanak, tipikusan iskolákban és munkahelyeken alkalmazzák őket. Míg az önszabályozás rendszere személyi szűrés alapú, a további két szűrési módszer az intézményi szintű szűrés alapkategóriájába tartozik. Az intézményi szintű szűrés során az internetszolgáltató szűrőprogramot telepít a rendszerébe, mely a felhasználókhoz nem engedi tovább a kéretlen tartalmat. Ezt jellemzően az e-mail fiókok kezelése során alkalmazzák. A harmadik szűrési módszer, a kógens szabályozás pedig az illegális tartalmak állami szinten történő blokkolását jelenti. Az önszabályozás és a korreguláció rendszereit a túl-, illetve az alulszűrés veszélye fenyegeti, nehéz ugyanis megtalálni a szűrés esetén azt az egyensúlyt, ami már elegendő védelmet biztosít, de még nem korlátoz feleslegesen

112 L. 8.2. Adathalászat: phishing, pharming.

113 A felhasználó saját elvei alapján, saját internethasználatához telepíti a megfelelő védelmi mechanizmust.

más tartalmat. Az önszabályozás és az állami szintű szabályozás önmagukban nem nyújtanak teljes védelmet, ezért a nyugat-európai gyakorlat mindinkább a két rendszert vegyítő eljárást (N&TD eljárás)¹¹⁴ helyezi előtérbe. Az N&TD eljárás belföldön átlagos ideje belföldön és az EU tagállamokban található szolgáltató esetén 12-36 óra, az Egyesült Államokban *hostolt* tartalom esetén, 24-48 óra¹¹⁵. A gyermekpornográfia az egyik legmeghatározóbb ilyen blokkolást kiváltó tartalom, de a skála egyre bővül, hiszen naponta jelennek meg újabb nem kívánatos tartalmak, és e tartalmak feltöltői folyamatosan próbálják kijátszani a blokkolás módszereit.

10. Mary esete a kiberbűnözéssel

2015-ben született tanulmányában¹¹⁶ Cameron S. D. Brown információs biztonsági szakértő, egészen új oldaláról mutatta be a *cybercrime*-ot. Kutatásában egy kitalált személy, Mary esetén keresztül összegzi a kibertérben megjelenő felderítési folyamatokat, kérdéseket, nyomozati és infrastrukturális problémákat. Mary egy húszas évei végén járó egyetemista lány Ausztráliában, aki szexuális tartalmú e-maileket és sms-eket kap, amelyek a lány magánéletének részleteit tartalmazzák. Véleményünk szerint az eset azért különleges, mert aktuális képet mutat a 21. századi jelenségekről, ráadásul globálisan érvényesül, számos országban megjelenő és egészen aktuális problémakört vet fel. A következőkben Mary történetét szeretnénk részletesen bemutatni, párhuzamba állítva Brown kutatási eredményeivel és az olvasóközönségben felmerülendő kérdésekre adott válaszaival.

„[M]iután Mary jelentős mennyiségű szexuális tartalmú e-mailt és sms-t kap, szüleitől kér segítséget. Az üzenetekből kiderül, hogy a küldő tudja, Mary hova jár egyetemre, ismeri a baráti körét és egyéb személyes adatait. A zaklató a személyazonosságát nem fedi fel a lány előtt. Mary apja online kutatásba kezd, mely során felfedez néhány külföldi, erotikus tartalmú weblapon közzétett kommentet, melyekben lányát említik. Mind Mary, mind a szülei vonakodnak jelenteni az esetet a rendőrségen, mivel nem hisznek annak megfelelő felderítési képességeiben. Mi több, a lány nem tartja elég komolynak az esetet a rendőrségi feljelentéshez.”¹¹⁷

A műszaki szakértők, a rendőrség, a jogászság, a kriminológusok és a nemzetbiztonsági szakértők más-más módokon értelmezik a számítógépes bűnözés koncepcióját. Egyre nehezebben eldönthető, hogy a *cybercrime* jogi, szociológiai vagy műszaki fogalomként határozható-e meg. Brown szerint a jognak tartózkodnia kell a számítógépes bűnözés *sui generis* jogi kategóriájának megalkotásától és a jogi hézagpótlástól annak érdekében, hogy abba beleférjenek az új technológiai vívmányok. A kutató azt az elvet vallja, hogy a jognak a már meglévő hagyo-

114 Az illegális tartalom eltávolítására szolgáló eljárás. Érdekeség, hogy az INHOPE, a legnagyobb nemzetközi forródróthálózat (mára 33 országban van nemzetközi forródróttja) azzal a feltétellel veszi fel a tagjait, hogy azok helyi és országos szinten egyaránt a nyomozóhatóság támogatását élvezzék. Magyarország 2005 óta INHOPE-tag.

115 INHOPE Annual Report 2010. www.inhope.org/Libraries/Annual_reports/2010_Annual_report.sflb.ashx

116 Cameron S. D. BROWN: Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice. *International Journal of Cyber Criminology* (2015) 55. <http://www.cybercrimejournal.com/Brown2015vol9issue1.pdf>.

117 Uo., 58.

mányos bűncselekmény-kategóriákat kellene kiszélesítenie, mivel az általa említett eljárásjogi és felderítési problémák nagy látenciát és alacsony nyomozati eredményességet okoznak. Mivel számos internetes bűncselekmény határokon átívelő, ezért a létező nemzeti jogszabályok nem képesek megfelelő számú eszközt biztosítani az elkövető felderítéséhez. Az anonimitás szintén a nyomozás eredménytelenségéhez vezethet, hiszen a világ bármely pontjáról bárki elkövetheti az adott cselekményt. Így Mary reakciója nem okoz nagy meglepetést az olvasónak, hiszen konzisztens a nyomozati szervek felderítési potenciáljába vetett alacsony bizalommal.

„[E]gy héttel később Mary elmeséli szüleinek, hogy ismeretlen hívása volt egy idegentől, aki szexuális fantáziálásra invitálta őt a vonal másik végéről. Valamivel később egy online hirdetőn talál egy, a nevében írt és telefonszámát is tartalmazó bejegyzést azzal a tartalommal, hogy arról fantáziál, hogy megrontsák őt. A lány kap egy e-mailt is, amely fenyegető stílusban íródott, és amelyhez mellékelteként több személyes jellegű fényképet is csatoltak, többek között a lány lakhelyéről, illetve róla készült pillanatképekről, melyeken barátaival a kávézóban vagy az egyetemen tölti idejét. Van még egy fotó, mely a lány egyik olyan ruhadarabját ábrázolja, amit úgy hiszi, hogy a ruhásszekrényéből vihettek el. Mary és szülei még aznap jelentik az esetet a rendőrségnek.”¹¹⁸

Mary esetében az eljáró hatóság a *Police Central E-crime Unit*¹¹⁹ lenne, amelyik azonban csak a leg súlyosabb e-bűnözési incidenseket vizsgálja és az online zaklatást nem tartja keretrendszerébe tartozónak. Érdekességgént, az FBI például 5000 dollárban állapította meg a nyomozás megindításának küszöbét. Ha a lány mégis a hatóságokhoz fordul és az *E-crime Unit* megindítja a nyomozást, a szerző szerint két irányba indulhat el a nyomozati szerv. Vizsgálhatja a cselekmények informatikai oldalát, vagy koncentrálhat a lányt körülvevő körülményekre és a hagyományos felderítési módszereket alkalmazva keresheti meg az elkövetőt. A tapasztalatok azonban azt mutatják, hogy e két módszer inkább együtt vezethet eredményre.

„[M]iután a rendőrség felvette Marytól a jegyzőkönyvet, továbbítja azt az E-crime Unitnak. Lyon rendőrfőnököt bízzák meg az ügygel. A sürgető fenyegetések az eset kiemelt fontosságú kezelését eredményezik. Lyon kapcsolatba lép Maryvel és interjút szervez a lánnyal, melynek során megkapja tőle az összes elektronikus levelezés másolatát, melyet a zaklatóval folytatott, valamint Mary minden számítógépes és egyéb adatát. Lyon figyelmezteti a lányt, hogy az online zaklatás kinyomozása nehéz feladat, főleg ha a tettes vagy a bizonyítékok más ország területén vannak. Lyon továbbá érdeklődik arról is, hogy a lány szakította-e meg mostanában a kapcsolatot valakivel az ismerősei közül, vagy van-e valamilyen elképzelése a zaklató személyazonosságáról. Azt a választ kapja, hogy a lánynak nemrég volt egy rosszul végződő szakítása előző barátjával, Paullal, miután rajtakapta őt, hogy megcsalja az egyik barátnőjével.”¹²⁰

Brown hisz abban, hogy a nyomozás sikerességéhez a nyomozó hatóság elkötelezettségére, 'soft' és 'hard' képességeire és a technikai kompetenciák megfelelő alkalmazására van szükség. A 'soft' kompetenciákkal meghatározható az elkövetők viselkedésprofilja, melyből már kikövetkeztethető az elkövető lehetséges magatartása, célja, motivációja. A 'hard' képességek a

118 Uo., 59.

119 Ausztrál Szövetségi Rendőrség.

120 Uo., 63.

számítógépek és hálózatok ismeretét, a mérnöki és informatikai tudást képezik. Mary ügyében a hatóság megfelelően jár el, egyszerre kezdi meg a Maryhez érkező képek és üzenetek forrásának keresését, és a lány környezetének kriminalisztikai módszerekkel történő átvizsgálását.

„[L]yon felkeresi az E-crime Unitot, hogy lássa, sikerült-e már dekódolniuk Paul telefonját. Bár a Blackberry biztonsági rendszerét még nem sikerült teljesen feltörniük, felfedeztek rajta olyan fotókat, melyek megegyeznek a Marynek küldöttekkel. Lyon levelet küld az Ügyészi Hivatalnak, majd pár héttel később James Keller ügyész informálja őt arról, hogy levél érkezett Paul ügyvédjétől, mely szerint a férfi tagadja az ellene felhozott vádakat. Lyon továbbra is úgy gondolja, hogy Paul telefonját kiberzaklatásra használta. A rendőrfőnök Kellertől azt a tanácsot kapja, hogy nyújtson be egy keresetet a bíróságon, melyben követeli a gyanúsítottól a Blackberry biztonsági jelszavainak megadását.”¹²¹

A vizsgálati eredmények a lány egykori barátjához, Paulhoz vezetnek, így a hatóság lefoglalja a férfi infokommunikációs eszközeit. A felderítés során kiderül, hogy különböző maszkolási módszerek alkalmazásával a szexuális tartalmú képeket Moldovában, a fórumüzeneteket az Egyesült Államokban, az e-maileket Szerbiában, az sms-eket pedig Oroszországban továbbították. Közülük csak az USA volt hajlandó kiadni a szükséges információkat a küldő IP címéről és egyéb ismert adatairól, ez megnehezítette a nyomozó hatóság munkáját. Az államok segítőkészségének hiányát egyrészt a nemzetközi együttműködés keretrendszerének hiánya okozza, másrészt a hatóságra háruló adminisztratív teher. Az idővesztés miatt megsérülhetnek, rosszabb esetben hozzáférhetetlenné válhatnak a bizonyítékok, ami szintén megnehezíti a felderítést. A szerző szerint a moldovai, szerb és orosz példa elkerülése végett nyílt konferenciákat kellene tartaniuk és több informális kapcsolat kiépítésére törekedniük, melyek a transznacionális bűnelkövetés során nagyobb kooperációt teremtenének az egyes szervek, például az Europol vagy az Interpol között.

„Az ügyész bemutatja az esetet a bíróságon, minden addig ismert bizonyítékkal együtt. Úgy véli, nincs más értelmes magyarázat, minthogy Paul követte el a zaklató magatartást Mary ellen. Azt állítja, hogy a vádlott anonim módon követte el a bűncselekményt, hogy elrejtse személyazonosságát és egy olyan, adatok végleges törlését szolgáló szoftvert töltött le a számítógépére, mellyel eltüntethette böngészési előzményeit, melyek bizonyítékkul szolgálhattak volna. Továbbá a vádlott késleltette a rendőrség munkáját azzal, hogy minden előzményt kitorölt mobiltelefonjáról, szintén a szóban forgó szoftverrel. A továbbiakban egy információs biztonsági szakértőt kérnek fel arra, hogy ismertesse az eset lehetséges aspektusait. A védelem felteszi a kérdést a szakértőnek, hogy a talált digitális fényképek megegyeznek-e a sértett számítógépén találtakkal. A szakértő ismerteti, hogy a fotók metaadatai egymásnak megfelelőek, így azok a vádlott Blackberry készülékről származnak. A szakértő elmondja továbbá, hogy Mary személyes adatain és fényképein kívül nem talált egyéb olyan információt, mely összekötné a vádlottat az áldozattal. A védelem ezután egy magán biztonsági cég szakemberét szólítja, aki tanúsítja, hogy eltérőek a Mary telefonján talált fényképek idejére vonatkozó adatok a vádlott számítógépén találtaktól. A szakember elmondja még, hogy a fényképeket egy, a vádlott telefonjánál frissebb szoftvert alkalmazó Blackberryn tárolták, így a készülék nem lehet a vádlotté. A szakértői vizsgálatból az is kiderül, hogy minden rejtett adat megtalálható egy megosztott mappában Paul számítógépén, mely összeköttetésben áll a férfi által letöltött szoftverrel,

azonban nem bizonyítható, hogy e mappát a férfi hozta létre. A bíróság ezután a vádlottat szólítja, aki állítása szerint azért hátráltatta a nyomozást, mert nem akarta, hogy kitudódjon katolikus családja előtt még titkolt homoszexualitása. Ezt követően a vádlottat számítástechnikai készségeiről kérdezik, amire azt a választ adja, hogy átlagos felhasználói tudással rendelkezik, építészetet tanult az egyetemen, ott ismerte meg Maryt is, aki mesterképzésben informatikát tanult. Elmondása szerint még számítógépe telepítésében is a lány segédkezett a számára. Paul azt állítja, ő szakított a lánnyal, miután rájött, hogy a férfiak iránt vonzódik, és elmondja a bíróságon, hogy ez a lány nagyon megviselte, hűtlennek állította be barátját, amiért az felvállalta másságát. A felhozottakra az ügyésznek több ellenvetése is támadt.¹²²

A bizonyítékok begyűjtésében fontos szerepet játszanak az internetszolgáltatók. Ugyanis ők bocsáthatják rendelkezésre az adatáramlással, illetve a konkrét tartalommal kapcsolatos információkat. Az információ kinyerése a mobil adathordozók fejlődésével még nehezebb lett. A kereskedelmi és a civil eszközök egyaránt nagy mennyiségű adatot tárolnak különböző e-mail profilokon, a közösségi hálón és egyéb applikációkban, melyekhez a hozzáférés lehetősége egyre korlátozottabb. A 2016-os előrejelzések szerint egy átlagos háztartás 3.3 *terabyte* adatot tárol majd különböző adathordozókon. Ehhez pedig olyan humánpolitikai és technológiai beruházásokra lesz szükség, melyek többletterhet jelentenek az államnak, magas látenchiához vezetnek és csökkentik a nyomozás hatékonyságába vetett társadalmi bizalmatlanságot. A bizonyítási szakaszban problémát jelent még a bizonyítékok és a gyanúsított közötti kapcsolat felderítése. Bár Mary esetében sikerül a számítógépéről és mobiltelefonjáról a bűncselekményhez köthető adatokat letölteni, a nyomozó hatóságok feladata annak bizonyítása, hogy a részben gyermekpornográfiával kapcsolatos tartalmak Paul tudtával, és nem a tudta nélkül kerültek technikai eszközeire. Ehhez a közvetlen és közvetett bizonyítékok megfelelő együtthatása szükséges, annak bizonyítására, hogy a vádlott az adott időben és helyen az eszközt használta. Ez a tevékenység a bűnfelderítés hatáskörébe tartozik.

„A bíróság Mary laccímére elfogatóparancsot ad ki és megbíz egy, a felektől pártatlan szakértőt, hogy egy újabb teljes körű vizsgálatot folytasson le a készülékeken. Erre azért van szükség, mert az E-crime Unit szakértőjének véleményével szemben bizalmatlan. Pár nappal később keresést folytatnak Mary házában. Találnak egy Android vezérlésű másik készüléket, és egy másik Blackberry mobiltelefont is, mely típusában megegyezik a Paultól lefoglalttal. Amikor megkérdezik a lányt a Blackberry hollétéről, Mary szenvtelenül állítja, hogy elvesztette a telefont. A rendőrség talál még jó néhány összezúzott merevlemez is az alagsorban. A lemezek olyannyira sérültek, hogy nincs esély az adatok helyreállítására. Eközben a készülékeket vizsgáló szakértő azt a megállapítást teszi, hogy minden egyes eszközön frissítve lettek az operációs rendszerek és a firmware programok. Mary Androidján a szoftvert szintén újrateremtették, és egy új beállítás került rá, amely automatikusan törli a telefon böngészési előzményeit. Amikor Lyon rendőrfőnök megkérdezi a lányt, hogy miért állított be a készüléken efféle megsemmisítő tevékenységet, Mary védekezni kezd és visszautasítja a kérdés megválaszolását, személyes tényezőkre hivatkozva. Pault felmentik a vád alól és Mary ügyét a bizonyítékok hiánya miatt ejtik.”¹²³

122 Uo., 90.

123 Uo., 97.

Az eszközök alacsony szoftveres védelme gyengíti a tartalmakra alapozott bizonyító erőt a bíróság előtt, főként mivel az elektronikus bizonyítékokat a szakértők legtöbbször inkább valószínűnek, semmint relevánsnak tartják. A hozzáférés a *'chain-of-custody'*¹²⁴ által bizonyítható, mely egy olyan protokoll, ami biztosítja a kinyert adat útjának követhetőségét és a segíti a hatóság munkavégzésének ellenőrzését. A hatékonyság növelésére Brown több megoldást is ajánl. Szerinte a Cybercrime-Egyezményt szükséges lenne kiterjeszteni az ENSZ tagállamokra, és az egyes nemzetközi együttműködések is összehangolásra szorulnának ahhoz, hogy az adatszolgáltatás és információáramlás előrelendüljön. A szerző a bürokratikus teher csökkentését egy folyamatosan üzemelő kommunikációs háló megvalósításában látja, amellyel azonnal kivizsgálhatók az olyan eszközök, melyeknél a bizonyíték megrongálódhat.

Brown szerint hasonlóan jelentős a büntetőeljárás szereplőinek informatika képzési támogatása is. Esetükben elsősorban a digitális bizonyíték feldolgozás, az online bűnözés és ezek bírói, rendőri, ügyési állománnyal való megismertetésére lenne szükség. A büntető-igazságszolgáltatás innovációja még sürgetőbb cél, hiszen egyre több egyedi jellemző nehezíti meg az online környezetben elkövetett jogsértések felderítését. Véleményünk szerint Brown a modern kori informatika egyik nagy úttörője. A *cybercrime*-ről szóló átfogó tanulmányában tökéletesen elemzi a rendszer hiányosságait, univerzális megoldásaival, javaslataival pedig aktualizálni szeretné a bűncselekmények nyomozati fázisát. A tanulmány tanulságaként, számos olyan egyedi jellemző nehezíti az online környezetben elkövetett jogsértések felderítését, mely a büntető-igazságszolgáltatás innovációját igényli. Szükségszerű lenne a büntetőeljárás szereplőinek informatikai képzése is, továbbá a digitális bizonyíték feldolgozás fejlesztése, valamint az online bűnözés és a *Darknet*¹²⁵ sajátosságainak mind a rendőri, mind az ügyési, és bírói állománnyal való megismertetésére is szükség lenne.

11. Néhány megállapítás és egy de lege ferenda javaslat

Az informatikai bűnözés szabályozásának jelenségével foglalkozó tudományos nézetek között, két határozott felfogás kontúrozható. Az egyik, álláspontunk szerint konvencionális nézet szerint, a Büntető Törvénykönyv rendelkezéseinek szükség szerint irányadónak kell lenniük az elektronikus úton elkövetett bűncselekményekre is, és ezekkel a hagyományos büntetőjogi eszközökkel kell a technológiai változás következtében felmerülő kihívásokat kezelni, míg a másik szemlélet képviselői a *cybercrime sui generis* szabályozását kívánják.

Véleményünk szerint mindkét felfogás mellett komoly érvek sorakoztathatók fel. A magyar szabályozásra pillantva, a Büntető Törvénykönyvről szóló 2012. évi C. törvény a büntetőjogi tényállások átfogó, kódexjellegű, dogmatikus egészet alkotó rendszerét summázza, ám nem tarthatjuk távol magunkat az új, hazai és nemzetközi jogalkotási megoldásoktól, stratégiáktól sem. Nem tartjuk szükségszerűen kényszerítőnek a két szemlélet közötti választást, mivel a meglévő számítógépes bűncselekmények folyamatos változása, fejlődése és az új deliktumok nagyszámú megjelenése megkívánja mind a stabil háttérszabályozást, mind az új módszerek kutatását, a regulálás új lehetőségeinek megteremtését is.

124 A bizonyíték dokumentálására, begyűjtésére és védelmére irányuló folyamatok összessége.

125 Azokat az internetes szolgáltatásokat és helyeket nevezik így, amelyeket már kifejezetten illegális célokkal rejtene el a hagyományos internetről.

A klasszikus büntetőjogi elveket érvényesítő szabályozás mellett helye lehet az infokommunikációs technológiára tekintettel lévő szabályoknak csakúgy, mint az ön-és társszabályozás normatív előírásainak is. A büntetőjogi kodifikációnak úgy kell kellően széles tényállásokat alkotnia, hogy azok adaptív módon alkalmazhatók legyenek az újabb és újabb, büntetendő *cyber* tevékenységekre, egyúttal megfeleljenek az alkotmányos büntetőjog kategorikus követelményeinek. Egy ilyen jellegű szabályozás azonban rendkívül nagy körültekintést igényel, tekintettel a büntetőjogi szabályozással szemben megfogalmazott és elvárt alkotmányos követelményekre. Sőt, a jelenlegi, biztos alapokon álló *cybercrime*-szabályozás arra szolgáltat bizonyítékot, hogy a két kibékíthetetlennek látszó teória egyes elemeinek összefésülése pozitív eredményekkel jár.

Összességében azt tapasztaltuk a források elemzése során, hogy a kiberbűncselekmények elbírálására nagyobb hangsúlyt fektet mind a hazai, mind a nemzetközi jogalkotás, mint az azokat megelőző lépések megtételére, valószínűsíthetően abból kifolyólag, hogy a *cybercrime* elkövetője egy lépéssel mindig a jogi szabályozás előtt jár, a folyton változó technológiai kritériumok végett. A számítógépes bűnözés a számítógép-használat konzekvenciája, bár tudatos szabályozással visszaszorítható, az online élet résztvevőiként mindig az életünk része marad. A tanulmány zárásaként ezért ismételtelen a prevenció szükségességére hívjuk fel a figyelmet, annak reményében, hogy ez a következő üzenet megannyi embertársunkhoz eljut: elsődlegesen mi, felhasználók tehetünk a saját biztonságunkért, informatikai felkészültségünk megalapozza jelenlétünket az online-térben. Az áldozattá válás a téma iránti fogékonysággal, illetve folyamatos önfejlesztéssel elkerülhető lehet.

Mindazonáltal nem lehet megkerülni a jogalkotó felelősségét sem. Az állampolgárok nem hagyhatók magukra az 'online Vadnyugaton', az internetes világ kivilágított, nyüzsgő terei, s kihalt sikátorai sem nélkülözhetik az állami kontrollt. A hatékony megoldás kulcsa még élénk vita tárgyát képezi, azt azonban kétséget kizáróan megállapíthatjuk, hogy az internet globális jellegéből fakadóan, az kizárólag a nemzetállami kompetenciát meghaladó, nemzetközi szintű összefogáson alapuló, nemzetek feletti intézményrendszer keretei között valósulhat meg.

A sorozatban eddig megjelent kötetek

1. Apró István (szerk.): *Határon túli magyar nyelvű médiumok 2010/2011* (2012)
2. Dobos Ferenc: *Nemzeti identitás, asszimiláció és médiahasználat a határon túli magyarság körében 1999–2011* (2012)
3. Csink Lóránt – Mayer Annamária: *Variációk a szabályozásra. Önszabályozás, társszabályozás és szabályozó hatóság a médiajogban* (2012)
4. Sarkady Ildikó – Grad-Gyenge Anikó: *A média-értéklánc szerzői jogi vonatkozásai* (2012)
5. Koltay András (szerk.): *A mediaszabályozás két éve (2011–2012)* (2013)
6. Paál Vince (szerk.): *Magyar sajtószabadság és -szabályozás 1914–1989* (2013)
7. Horváth Attila: *A magyar sajtó története a szovjet típusú diktatúra idején* (2013)
8. Koltay András – Nyakas Levente (szerk.): *Összehasonlító médiajogi tanulmányok. A „közös európai minimum” azonosítása felé* (2014)
9. Dobos Ferenc – Megyeri Klára: *Nemzeti identitás, asszimiláció és médiahasználat a határon túli magyarság körében 2.* (2014)
10. Grad-Gyenge Anikó – Sarkady Ildikó: *Közös jogkezelés az audiovizuális médiában* (2014)
11. Apró István (szerk.): *Média és identitás* (2014)
12. Pruzsinszky Sándor: *Halhatatlan cenzúra* (2014)
13. Kóczyán Sándor: *Gyermekvédelem a médiajogban* (2014)
14. Apró István – Paál Vince (szerk.): *A határon túli magyar sajtó Trianontól a XX. század végéig* (2014)
15. Kiss Zoltán – Szivi Gabriella: *A közszolgálati mediaszolgáltatás és a szellemi tulajdonjogok kapcsolódási pontjai és szabályozási környezete* (2015)
16. Dobos Ferenc: *A médiahasználat változása az erdélyi, felvidéki, kárpátaljai és vajdasági magyarság körében 2001–2014* (2015)
17. Grad-Gyenge Anikó: *Az audiovizuális archívumok szabályozási kerete – különös tekintettel a médiajogi és szerzői jogi rendelkezésekre* (2015)
18. Dobos Ferenc: *A médiahasználat változása az erdélyi, felvidéki, kárpátaljai és vajdasági magyarság körében 2001–2014/2* (2015)
19. Apró István (szerk.): *Média és identitás 2.* (2016)
20. Mezei Péter : *Jogkimerülés a szerzői jogban* (2016)
21. Koltay András, Andrej Školkay (szerk.): *Comparative Research on the Approaches of Administrative Judiciaries to Sanctions Issued by Media Regulators in V–4 I.* (2016)
22. Koltay András, Andrej Školkay (szerk.): *Comparative Research on the Approaches of Administrative Judiciaries to Sanctions Issued by Media Regulators in V–4 II.* (2016)
23. Makkai Béla: *Határon túli magyar sajtó – Trianon előtt* (2016)
24. Grad-Gyenge Anikó: *Film és szerzői jog – A megfilmesítési szerződés* (2016)
25. Kőhidi Ákos: *Fájlcseré és felelősség* (2016)
26. Hajdú Dóra: *A törvény által előírt közös jogkezelés a magyar és a francia szerzői jogban* (2016)
27. Tóth J. Zoltán: *A büntetőjogi rágalalmazás és becsületsértés* (2017)
28. Kelemen Roland: *Az első világháború sajtójogi forrásai – Sajtójog a kivételes hatalom árnyékában* (2017)
29. Apró István: *Határon túli magyar médiumok 2016* (2017)

Médiatudományi Intézet, Budapest
A kiadásért felel Nyakas Levente
Szerkesztő: Klein Tamás
Tördelő: Varga Ákos
Megjelent 10,25 (B/5) ív terjedelemben, 300 példányban
Médiatudományi Könyvtár: ISSN 2063-5222
Médiatudományi Könyvtár 30.: ISBN 978-615-5302-27-5