Az infokommunikációs és technológia jog alapjai

Szerkesztette: Tóth András

A kiadvány a KÖFOP-2.1.1-VEKOP-15-2016-00001 „A közszolgáltatás komplex kompetencia, életpálya-program és oktatás technológiai fejlesztése” című projekt keretében készült el és jelent meg.

Szerkesztette:
Dr. Tóth András

Szerzők:
Dr. Grad-Gyenge Anikó
Dr. Klein Tamás
Dr. Szabó Endre Győző
Dr. Tóth András

Szakmai lektor:
Dr. Koltay András

Olvasószerkesztő:
Vörös Ferenc

A kézirat lezárásának dátuma:
2018. március 31.

Kiadja:
© NKE, 2018

Felelős kiadó:
Prof. Dr. Kis Norbert
Dékán

1. TARTALOM

1. BEVEZETÉS

Dr. Klein Tamás írása.

Az infokommunikációs és technológia jog tananyaga és a ráépülő képzés célja bizonyos értelemben rendhagyó, nem csupán a közszolgálati továbbképzésben, de még a jogászképzésben is. Az alábbi tananyag arra vállalkozik, hogy rendkívül rövid terjedelemben ízelítőt adjon a jogtudomány és jogi szabályozás azon legújabb kihívásairól, amelyek a modern infokommunikációs eszközökhöz és az új technológiák alkalmazásához kötődnek.

A jegyzet két nagy jogterületbe nyújt bepillantást. Ezek közül az első az infokommunikációs jog, mely az információs társadalom jogi vonatkozásaival foglalkozik, a második pedig a technológia jog, ez a mai digitális gazdaság jogi kihívásaira kíván válaszokat adni, és értelemszerűen fiatalabb jogterület, mint az előbbi. Természetesen az infokommunikációs jog is viszonylag új jogterületnek számít, de a technológia joghoz képest több mint egy évtizede volt arra, hogy tárgyát és tárgyalási módját körvonalazza. Erre tekintettel az infokommunikációs jog részének kell tekintetnünk az adatvédelmi jogot, az elektronikus hírközlés és kereskedelem jogát (ezek jelen szakanyagban meg is jelennek), de ide tartozik az elektronikus közigazgatás és az elektronikus aláírás, valamint bizonyos szerzői jogi vonatkozások is (melyek terjedelmi okokból nem részei jelen szakanyagnak). A technológia jog – újszerűsége miatt – még rendkívül képlékeny, és egy erről szóló oktatási anyagot különösen körültekintően kell megalkotni annak érdekében, hogy a leírtak legalább középtávon megállják a helyüket a téma kapcsán. Ennek megfelelően törekedtünk a kérdés absztrakt ismertetésére, melynek jegyében szó esik a technológia és azon belül is különösen a robotok jogi szabályozásának általános jogelvi megfontolásairól. Ezen kívül igyekeztünk olyan technológiai jelenségeket, újításokat kiválasztani (pl. sharing economy) és olyan vizsgálódási szempontokat azonosítani (mint a fogyasztóvédelmi), amelyekről azt gondoltuk, szélesebb körben lehetnek érdekesek, és létezik már olyan, jogilag megragadható lényegük, amely legalább középtávon változatlan marad (pl. robotok). A kibertér biztonsága mintegy keretbe foglalja az infokommunikáció és technológia azon részét, amely kifejezetten az internethez kapcsolódik, és emiatt jogi vonatkozásainak ismertetését elengedhetetlenül szükségesnek gondoltuk.

Az **információs társadalmakban** a korábbiakhoz képest soha nem látott mértékben nőtt az információáramlás intenzitása – elsősorban az új információs csatornák, a nyilvánosság új platformjainak megjelenése miatt –, amely jelentős mértékben hat a társadalmi folyamatokra és az (állam)polgárok életére. A demokratikus társadalmi rend, a demokratikus organizmusok oxigénje, a demokratikus eljárások fűtőanyaga az **információ**. Az információk hozzáférhetősége az első szükséges, de közel sem elégséges feltétele a demokratikus eljárások és a magánérintkezések megfelelő szintű biztosításának. A hozzáférhetőség **kvantitatív** jellemzői mellett a **kvalitatív jellemzőknek** is meghatározó jelentőségük van, vagyis annak, hogy az elérhető, hozzáférhető információk mind mennyiségileg (minden releváns kérdésben rendelkezésre álljon az informálódást elősegítő információ), mind minőségileg (a megalapozott döntéshozatalt elősegítő tényszerű, valós tények és a vélemények sokszínű együttese alkossa a nyilvánosságot) is alkalmasak legyenek a polgárok demokratikus diskurzusokban való megalapozott részvételre.

Az internet mára a modern **interperszonális és tömegkommunikáció**, valamint az **információs szabadság** szinonimájává vált. Az internetes nyilvánosság állami szabályozására vonatkozó tartalmi összetevők meghatározása előtt arra az elméleti előkérdésre kell választ adni, hogy technikailag lehetséges-e és alkotmányos (alapjogvédelmi) szempontból megengedhető-e egyáltalán az online

kommunikációs tér állami szabályozása. Az egyes álláspontokat áttekintve azt tapasztalhatjuk, hogy alapvetően két nézet csatázik egymással. Az egyik az internet romantikus felfogásaként azt vallja, hogy az internet technológiája által teremtett nyilvánosság a tömegkommunikáció egy minőségileg új korszakát jelenti. A tömegdemokráciákban korábban jelen lévő hozzáférés szűkösségének kérdése végleg megoldódik, hiszen az internet, mint minden idők legdemokratikusabb médiuma képes megteremteni a politikai diskurzusok korábban soha nem tapasztalt sokszínűségét. Az internetes nyilvánosság e felfogása okszerűen tagadja az állami szabályozás megengedhetőségét, és azt az online piactér mechanizmusaira bízza. Érvelésük 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. Azok tehát, akik az internet technológiája által biztosított nyilvánosságban a szólásszabadság utópiájának a megvalósulását üdvözölték, az állami be nem avatkozás korszakát vizionálták. Ezzel szemben realistább és általunk is támogatott nézet az, 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. Az online tér nem önmagában való érték, ezért minden megszorítás nélkül nem is mentes az offline valóság szabályai alól. Ennek megfelelően pl. 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 újmédián (közösségi hálózatokon) keresztül terjesztik. **Az internet** – amiként arra az Alkotmánybíróság is rámutatott – **nem jogmentes terület,** nem szabályok nélküli virtuális vadnyugat. Az interneten történő emberi tevékenység, így a kommunikációs tevékenység is, **függetlenül annak technológiai hátterétől, a jogi szabályozás tárgya lehet**, nem *terra incognita* a jog számára. 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 érvényesítendők az Alaptörvényben rögzített alapvető jogok és kötelezettségek." [19/2014. (V. 30.) AB határozat 50. bekezdés.]

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. cikkének értelmében az alapvető jogok védelme az állam elsőrendű kötelezettsége. Az állam aktív intézményvédelmi kötelezettségének elsősorban jogalkotás révén (alapjogok esetében kizárólag törvényben) tesz eleget.

Az egyes modern technológiák, különösen pedig a robotjogi szabályozás kapcsán rendkívül fontos alkotmányos követelményként szükséges utalni az élethez és emberi méltósághoz való jogra. Az emberi élet és a méltóság feltétlen védelme megköveteli, hogy ezek **az új technológiák kizárólag az ember védelmét szolgálják, és ne üresítsék ki emberi méltóságát.**

Az intézményvédelmi kötelezettség teljesítése során **a törvényhozó olyan szabályozási környezetet alkot, amely biztosítja az alapjogok érvényesülését** mind az állammal szemben, mind a magánviszonyokban, közjogi (vertikális) és magánjogi (horizontális) jogviszonyokban egyaránt. Az infokommunikációs és technológia jogi tananyag ezeknek az egyes esetekben már kiforrott, máshol még csak formálódó szabályozási kihívásoknak a rövid bemutatására vállalkozik.

A tananyag a modern társadalmak három új kihívását kontúrozza, az évtizedes múltra visszatekintő infokommunikációs jog, a napjainkban formálódó technológia és robotjog, valamint a cyberjog egyes kérdéseinek vizsgálatával. Az infokommunikációs jogi kérdések közül a digitális gazdaság adatvédelmi kihívásainak a körében a személyes adatokat fenyegető veszélyekből és szabályozási megoldásokból adunk ízelítőt, mint például a kamerás megfigyelés, az online adatgyűjtés, vagy éppen az online felhőszolgáltatások. Az elektronikus kereskedelem szabályozási kérdéseinek kapcsán

arról lesz röviden szó, hogy az információs társadalommal összefüggő egyes szolgáltatásokra milyen sajátságos előírások vonatkoznak. Az elektronikus hírközlésjog az információáramlás infrastrukturális kérdéseiről ad összefoglalást. A technológia és robotjogi fejezet sokszínű tematikát vonultat fel. Bemutatja a jog és technológia viszonyát, elemzi a digitális technológiák jelentette fogyasztóvédelmi problémákat, az olyan online alkalmazások által felvetett jogi problémákat és lehetséges megoldásaikat, amelyek összekapcsolják a magántulajdonukat üzleti, kereskedelmi célokra hasznosítókat a lehetséges fogyasztókkal, továbbá felvillantja a mesterséges intelligencia és a robotika jogi szabályozása előtt álló kihívásokat, azzal, hogy a valaha még csak a sci-fi írók által álmodott, mára azonban reális közelségbe került jelenségek lehetséges jogi megoldásait is számba veszi. Ez utóbbi kérdéskör kapcsán kitérünk az intelligens robotok jogalanyiságának és felelősségének a kérdésére. Az utolsó fejezetben a cybertér egyes sajátságos szabályozási kérdéseivel foglalkozunk, külön vizsgálva az interneten jelentkező specifikus devianciákat és a cyberbiztonság követelményét.

2. A DIGITÁLIS GAZDASÁG ADATVÉDELMI VONATKOZÁSAI

Dr. Szabó Endre Győző és Dr. Klein Tamás írása.

2.1. Bevezetés[1]

Az adatvédelem a magánszféra oltalmát szolgálja a természetes személyekre vonatkozó adatok védelme révén. **A magánszférát a természetes személyhez tartozó fizikai, pszichikai és virtuális értelemben is meghatározható azon közegnek tekintjük, amelybe belépni csak a jog által elismert célból, módon és terjedelemben lehet**.

Az adatok védelme terén **az egyénnek a közösségen**, társadalmon **belüli boldogulását kell** elsősorban **szem előtt tartani**. A magánszféra körébe tartozó **adatok jogellenes kezelése, így továbbítása, nyilvánosságra hozatala[2] eltérő mértékben befolyásolja az egyén** közösségen belüli **boldogulását**. A jog absztrakt szabályai nem tudnak minden eset között előre tételezett módon különbséget tenni, ezért általános védelmet nyújtanak a magánszféra körébe tartozó adatok számára. A joggyakorlat feladata, hogy az esetek közötti különbségeket figyelembe vegye.

A személyes adatok védelméhez való jog tartalmát alapvetően két jogszabály határozza meg:

- 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 irányelv hatályon kívül helyezéséről (az angol jogszabálynév rövidítése: GDPR), valamint
- A 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.).

A rendelet az Infotv.-hez hasonlóan közvetlenül alkalmazandó az Európai Unió valamennyi tagállamában. Az említetteken túl ágazati jogszabályok is tartalmaznak rendelkezéseket az adatok kezelésére, illetve védelmére vonatkozóan.

Az adatok alanyát a jogi terminológia érintettnek nevezi. **Személyes adat az élő természetes személlyel kapcsolatba hozható adat.[3] A személyes adatból levonható, az** érintettre vonatkozó következtetés is személyes adatnak minősül. A következtetésnek tárgyilagosnak kell lennie, a szubjektivitáson alapuló információ (pl. vélemény) nem tekinthető személyes adatnak.

---

1 Az alfejezet Dr. Szabó Endre Győző írása.

2 „Személyes adat kezelésének tekintendő a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés” (GDPR 4. cikk 2. pont)

3 A jogszabályi definíció szerint: „személyes adat: azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható” (GDPR 4. cikk 1. pont)

A személyes adatot a jog addig tekinti az egyén magánszférája részének, **amíg az adat és az egyén között helyreállítható a kapcsolat**: mindaddig, **amíg az adat kezelése az egyén helyzetét befolyásolni képes**, addig indokolt az adat védelme.[4]

Az Alaptörvény VI. cikkének (3) bekezdése szerint a személyes adatok védelméhez és a közérdekű adatok nyilvánosságához fűződő jog érvényesülését sarkalatos törvénnyel létrehozott, független hatóság ellenőrzi. A sarkalatos törvény az Infotv., a független hatóság pedig a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: Hatóság). A Hatóság **autonóm államigazgatási szerv**, **csak a törvénynek van alárendelve, feladatkörében nem utasítható, a feladatát más szervektől elkülönülten, befolyásolástól mentesen látja el. [5] Számára feladatot csak törvény állapíthat meg**.

A Hatóság a **személyes adatok védelmét érintő kérdésekben** nem csupán informális, ún. vizsgálati eljárást folytathat le, hanem **jogosult hatósági eljárást indítani**. A hatósági eljárás a közigazgatási eljárásra vonatkozó szabályok szerint döntéssel zárul, amelyben bírság kiszabására is sor kerülhet.

A személyes adatok kezelésével összefüggő jogsértések esetén az Infotv. az érintett számára egy **háromlépcsős jogorvoslat**ot kínál. Kérelmével, illetve igényével az érintett fordulhat az adatkezelőhöz, a Hatósághoz, továbbá a bírósághoz.

Ha az adatkezelő az érintett adatainak jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével másnak **kárt okoz, köteles** azt **megtéríteni**.[6] A káron túl az adatok jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével az érintett személyiségi jogának megsértése esetén az érintett az adatkezelőtől **sérelemdíj**at[7] követelhet.

A következő fejezetekben olyan adatkezeléseket tekintünk át, amelyek az alkalmazott technológia révén különös kockázatokat rejtenek a magánszféra, valamint az adatvédelem szempontjából. Természetesen vannak témák, melyek a terjedelmi korlátok miatt ebben a tananyagban nem kaphatnak helyet. Viszont a lentebb bemutatott technológiákhoz és adatkezelési módokhoz hasonlóan valamennyi említett terület és eszköz alkalmas arra, hogy a magánszférába újszerű módon avatkozzon be. A következő fejezetek tekinthetők bizonyos szintig letisztult és a joggyakorlat által már valamennyire feldolgozott területeknek.

2.2. Kamerák[8]

A kamerás megfigyelés az elmúlt évtizedekben a magánszférával (privacy) kapcsolatos gondolkodás egyik legvitatottabb területévé vált. A kamera és az egyén magánszférájának konfliktusa természetesen adódik a következő sajátosságok alapján:

- A kamera szükségszerűen nem csak tárgyakra, hanem az emberi testre is irányul.
- A kamera emberi magatartást tesz megfigyelhetővé, a felvételek alapján visszakereshetővé.[9]
- A kamera látóterébe került egyén kiszolgáltatottá válik a kamera üzemeltetőjével szemben, mert nem tudja, mi történik a róla készült felvételekkel.

---

4 Ha valaki például Debrecen város polgármesteréről beszél, mindenki számára azonosítható az adat alanya. Ha azonban csak egy vidéki politikusra utalnak, úgy ebben az esetben az érintett és az adat közötti kapcsolat nem állítható helyre, következésképpen az ilyen információ (ha más módon sem hozható létre a kapcsolat) nem tekinthető személyes adatnak.

5 Infotv. 38. § (5) bekezdés

6 Az Infotv. 23. § (1) bekezdése szerint

7 Az Infotv. 23. § (2) bekezdése szerint

8 Az alfejezet Dr. Szabó Endre Győző írása.

9 Az Alkotmánybíróság a 36/2005. (X. 5.) AB határozatban fejtette ki bővebben a kamerák működtetésével kapcsolatos részletes álláspontját.

- Nem mindig egyértelmű, hogy hol vannak kamerák elhelyezve, és mi van a látómezejükben.
- A vagyonvédelem körében elsősorban a védett érték áll a középpontban, ehhez képest az egyén „mellékszereplő”.

Mindezek a jellemzők egyben érvek is amellett, hogy szükségessé vált a kamerás megfigyelés részletes szabályozása.

2.2.1. Kamerás megfigyelés magánterületen

Magánterületen személy- és vagyonbiztonsági megfontolásokból jogszerűen üzemeltethetők kamerák Magyarországon.[10] A jogszerű adatkezelés legfontosabb követelményei a következők:

- A megfigyelés szabályai előre rögzítettek legyenek.
- A kamerás megfigyelés tényéről a területre belépőket tájékoztatni kell.
- Az adatkezelő személyét és az adatkezelés legfontosabb jellemzőit jól látható módon fel kell tüntetni.
- A törvény által kivett területeken, ahol az az emberi méltóságot sértheti, nem folytatható kamerás megfigyelés (például öltözőben, próbafülkében, kórteremben).
- A felvételeket a törvényes határidőn belül törölni kell.
- A felvételek csak az előre rögzített célra használhatók fel.

2.2.2. Kamerás megfigyelés a munkahelyen

A Munka Törvénykönyve szerint a munkaviszony körébe eső adatkezelések esetében nem általános elvárás, hogy az érintettek (munkavállalók) az adatkezeléshez hozzájárulásukat adják. Az adatkezelés azonban nem jogszerű, ha azzal kapcsolatban nem kaptak az érintettek minden részletre kiterjedő, dokumentált tájékoztatást. A tájékoztatásnak világosan megfogalmazva, bárki számára érthető írásbeli szövegben kell megjelennie.

Az adatkezelésnek meg kell felelnie a **szükségesség** és **arányosság** kritériumrendszerének, ennek hiányában a kamerás megfigyelés adatvédelmi jogi szempontból kifogásolható.

Az egységes joggyakorlat kialakítása érdekében a Hatóság a tárgyban ajánlást bocsátott ki.[11] Az ajánlás legfontosabb megállapításai a következők: a munkavállalók magánszférája bizonyos pontosan körülhatárolt esetekben, garanciális követelmények megtartása mellett korlátozható, amennyiben a **munkaviszony rendeltetésével közvetlenül összefüggő ok**ból feltétlenül szükséges. Az alkalmazott módszerek nem járhatnak az emberi méltóság megsértésével, illetőleg a munkavállaló magánélete nem ellenőrizhető.

A Munka Törvénykönyvének rendelkezései általános felhatalmazást adnak a munkáltatói ellenőrzéshez kapcsolódó adatkezelésre, azonban ezen kereteket a munkáltatónak, tehát az adatkezelőnek kell tartalommal megtöltenie. A tartalom ebben a kontextusban az adott környezetben érvényesülő paramétereket és érdemi garanciákat jelenti. Ennek megfelelően a munkáltatónak kell igazolnia azt, hogy az általa alkalmazott megfigyelőrendszer megfelel a célhoz kötöttség követelményének, és nem jelent aránytalan beavatkozást az egyének magánszférájába.

---

[10] A személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény alapján.

[11] A Nemzeti Adatvédelmi és Információszabadság Hatóság ajánlása a munkahelyen alkalmazott elektronikus megfigyelőrendszer alapvető követelményeiről. (http://naih.hu/files/Ajanlas-a-munkahelyi-kameras-megfigyelesr-l.pdf)

A megfigyelés elfogadott céljának tekinthető az emberi élet, egészség védelme, a veszélyes anyagok őrzése, titkok védelme, a vagyonvédelem. Nem folytatható megfigyelés olyan területen, ahol az az emberi méltóságot sértheti, így például öltözőben, zuhanyzóban, a munkaközi szünet eltöltése céljára szolgáló helyiségben. Abban az időszakban, amikor az adott területen jogszerűen senki sem tartózkodhat, a kamerás megfigyelés nem esik jogi szempontból korlátozás alá. A kamera közterületre, más magánterületére nem irányulhat.

Amennyiben a munkáltató a megfigyelőrendszer üzemeltetésével vagyonőrt bíz meg, úgy a munkáltató és a vagyonőr is adatkezelőnek fog minősülni.[12] A munkáltatónak pontosan meg kell határoznia, és minden egyes kamera vonatkozásában tájékoztatást kell nyújtania a telepítés céljáról, annak látómezejéről. Rögzíteni kell az adatok tárolásának idejét, a hozzáférés módját, azokat az eljárásokat, amelyek során azokat fel lehet használni (például kártérítés, fegyelmi felelősség).

2.2.3. Kamerás megfigyelés közterületen

A közterületi kamerás megfigyelés néhány olyan szerv privilégiuma, amely a közrend, közbiztonság kapcsán lát el közfeladatokat, illetve gyakorol hatósági hatásköröket. A **rendőrség** és a **közterület-felügyelet** egymáshoz hasonló szabályok alapján helyezhet el kamerákat ott, ahol az közbiztonsági, **bűnmegelőzési és bűnüldözési célból igazolhatóan szükséges**.

Mind a rendőrség, mind a közterület-felügyelet javasolhatja az önkormányzati képviselő-testületnek bizonyos területek megfigyelés alá vonását. Az elhelyezésre kerülő képfelvevő szükségességéről, a képfelvevővel megfigyelt közterület kijelöléséről a rendőrség előterjesztésére az illetékes **települési önkormányzat dönt**.

A képfelvevők elhelyezésére, a megfigyelt területre vonatkozó adatokat a központi szerv honlapján közzé kell tenni, ezen túl a képfelvevő által megfigyelt területre belépő személyek tájékoztatását elősegítő módon **figyelemfelhívó jelzés**t, ismertetést kell elhelyezni a képfelvevők elhelyezéséről, az adatkezelés tényéről.[13]

A rendőrség és a közterület-felügyelet általános felhatalmazásához képest a **fegyveres biztonsági őrség** szűkebb keretek között alkalmazhat közterületen kamerás megfigyelést. A fegyveres biztonsági őr elektronikus megfigyelőrendszert a védett létesítmény (például kormányzati, honvédelmi létesítmények) területe és annak környezete megfigyelésére alkalmazhat.[14] A kép- és hangfelvétel készítésének szabályai egyébként a másik két szervezet adatkezeléséhez hasonlóan alakulnak.

A közterületi, közbiztonsági célú kamerás megfigyeléseket a kezdetektől fogva végigkísérte az áthelyeződés jelensége. Tipikus példa erre a nagyvárosi kerületekben megfigyelhető tendencia, amely szerint a kamerával megfigyelt területekről például a gépkocsifeltörések, lopások, közterületi prostitúció a kamerával fel nem szerelt területekre helyeződnek át.

---

12 A közös adatkezelőkre a GDPR a 26. cikkében külön szabályokat állapít meg.

13 A belga gyakorlat szerint nem csak azt jelzik, amikor a járókelő kamerával megfigyelt területre lép, hanem a tábla túloldalán arra is figyelmeztetik, hogy elhagyja a megfigyelt területet.

14 A fegyveres biztonsági őrségről, a természetvédelmi és mezei őrszolgálatról szóló 1997. évi CLIX. törvény 9/A. § (2) bekezdés

2.3. Online adatkezelések – keresőmotorok és közösségi oldalak[15]

Az internethez kötődő adatkezelések számos jogi kérdést vetnek fel. A világháló a valós („offline") élet egyre több történését képes nemcsak leképezni, hanem helyettesíteni is. Ilyen a ma már magától értetődő elektronikus levelezés használata a postai levelezés helyett, vagy a vásárlások lebonyolítása, pénzátutalás stb. a hagyományos ügyintézés helyett.

Ahogyan a gazdasági, kommunikációs események egyre inkább a virtuális térben valósulnak meg, úgy válik egyre értékesebbé minden információ, ami ide kapcsolódik. A banki ügyintézés, adóbevallás, céges ügyek intézése, egyes közigazgatási cselekmények, a kommunikáció számos módja, és mindezek nyomon követhetősége megköveteli az interneten megforduló adatok gondos kezelését és védelmét. E nélkül ugyanis a világháló megbízhatatlan lenne, és nem lenne képes szerepét betölteni.

A **virtuális valóság nem csupán** a való világ **leképezés**éről, **hanem valami újnak a megteremtéséről**, egyelőre kifogyhatatlannak tűnő elképzelések megvalósításáról **is szól**.

A jegyzet kereteit meghaladná az online adatkezelések átfogó áttekintése, ezért a továbbiakban csupán két kiválasztott területre szorítkozunk: a keresőmotorokra és a közösségi oldalakra.

2.3.1. A keresőmotorok

A keresőmotorok fontos szerepet játszanak az interneten elérhető információk szempontjából: egy adott keresési szempont szerint a világhálón elérhető információk közül jelenítik meg azokat, amelyeket a felhasználó el kíván érni, legyen szó szöveges tartalomról, képekről, vagy akár videókról. Keresni gyakorlatilag a felhasználó által megadott bármilyen tartalomra lehet. Témánk szempontjából annak van különös jelentősége, hogy a jog miként értékeli azokat az eseteket, amikor egy **természetes személy nevére** indítanak kereséseket. Ennek kapcsán fogalmazódott meg az a panasz, amely végül az Európai Unió Bíróságának ítéletéhez vezetett. Az alábbiakban ezen ítélet alapján mutatjuk be a keresőmotorok és a magánszféra konfliktusát.

Az alapügy panaszosa egy spanyol polgár, Costeja González volt, akinek még az 1990-es években felhalmozódott köztartozásai miatt ingatlanát a spanyol szabályok szerint elárverezték. Costeja González azt panaszolta, hogy az erről közzétett korabeli internetes közlemények a nevére keresve továbbra is megjelennek a Google keresőmotorjának találatai között. Nem az eredeti források közléseit kifogásolta (azok jogszerűen kerültek nyilvánosságra és maradtak is nyilvánosak), csupán azt, hogy **miért kell** még másfél évtized után is **olyan információkról számot adnia, amelyek életének már egy régen lezárt szakaszához kapcsolódnak?**

Az Európai Unió Bírósága a spanyol bíróság előtt indult ügyben, és általa előzetes döntéshozatali eljárásban elbírált ítéletében helyt adott a kérelemnek, és kötelezte a keresőmotort az európai adatvédelmi szabályok betartására. [16]

Az ítélet középpontjában az a kérdés áll, hogy mi a személyes adatok védelméről szóló szabályozásnak a **társadalmi rendeltetés**e.

A Bíróság a keresőmotorok által végzett tevékenységet elemezve kiemeli, hogy alkalmasak egy többé-kevésbé részletes **profil** kialakítására. A profil adatvédelmi megközelítésben azért érdemel különös védelmet, mert a személyiség olyan képét nyújtja, amely alkalmas akár a jövőbeni cselekvések prognosztizálására is. De adott esetben már a múltbeli események „elfelejtése" is sokat segítene az egyénen. Ez fordult elő egy másik esetben akkor, amikor egy erotikus tartalmú videó került fel az

[15] Az alfejezet Dr. Szabó Endre Győző írása.

[16] Az Európai Unió Bíróságának C-131/12 számú ítélete, 2014. május 13.

internetre a szereplők civil nevével együtt, a videó elkészítését követően sok évvel.

Az ítélet egyik első és legfontosabb jogi megállapítása, hogy a keresőmotornak a nyilvánosan elérhető személyes adatokon végzett tevékenysége önálló adatkezelői felelősséggel jár. Az eredeti források felelősségével összevetve jogi szempontból a minőségbeli különbség abban áll, hogy **saját céljából végez műveleteket az adatokon** – az eredeti céltól függetlenül.

A Bíróság érvelése szerint azáltal, hogy a Google európai polgárok adatait elemzi profitjának elérése céljából, valamint a keresési szokások és egyéb mutatók alapján teszi nyereségessé szolgáltatását, az európai jog fennhatósága alá lép. A fogyasztó preferenciájához (keresőszavakhoz) igazítja a reklámokat. A reklámozási tevékenység tehát szorosan az európai joghoz és fogyasztókhoz köti a céget.[17] Következésképpen az EU joga alkalmazandó, és ennek alapján annak a nemzeti jognak a hatósága alá esik, amelynek területén a tevékenységet kifejtik. [18] A konkrét esetben tehát a spanyol jog alapján a spanyol hatóságok járhattak el.

Mire köteles az ítélet nyomán a keresőmotor? A találati listában a kifogásolt találat (link) megjelenítése tiltott meghatározott esetekben. Az egyén akkor kifogásolhatja alappal a link megjelenését a találati listában, ha a róla szóló nyilvánosan elérhető információ **már nem releváns**.

Az ítélet szerint **három érdeket kell elemezni**: az egyén magánszférájához, illetve személyes adatainak védelméhez fűződő jogát. A második érdek a felhasználók tájékozódáshoz fűződő joga, tehát adott esetben egy-egy természetes személlyel összefüggésben is értelmezhető, hogy valamilyen tájékozódási lehetősége szűkül azáltal, ha a találati eredmények közül bizonyosak kikerülnek. A harmadik érdek pedig értelemszerűen a keresőmotor gazdasági érdeke. Nem vitás, hogy legitim érdeke fűződik a cégnek a profit megszerzéséhez és a keresőmotor üzemeltetéséhez.

A Bíróság a három konkuráló érdek, **az egyén magánszférájának védelme, a felhasználók tájékozódási joga valamint az üzleti érdek** közül úgy ítélte meg, hogy az egyén magánszférájához, **adatvédelemhez fűződő joga részesítendő előnyben** akkor, amikor egy találat eltávolítását kell mérlegelni. Nyilvánvalóan vannak ez alól **kivételek**. Ilyen kivétel például a **közszereplő**, amely fogalmat tágabban kell értelmezni, mint amire a magyar nyelvben asszociálnánk. Így az európai konszenzus szerint egy **orvos** tevékenysége **például** a köz érdeklődésére tart számot, így egy műhiba kapcsán tett közlést nem fognak a kérelmére eltávolítani.

Az elemzés alapján tehát Costeja González nevével összefüggésben el kellett távolítani a keresési találatok közül azokat, amelyek a kifogásolt árverésre utaltak. A másik említett példánál szintén lehetetlenné kellett tenni, hogy az erotikus videó és a szereplők civil neve a keresőmotor révén összekapcsolható maradjon. A közszereplő azonban nem kérheti sikerrel, hogy a rá nézve kényelmetlen információra mutató linket ne jelenítsék meg a találati listán.

Ha a keresőmotor elutasítja az érintett kérelmét, akkor az illetékes tagállami adatvédelmi hatósághoz, végső soron pedig a tagállami bírósághoz lehet fordulni. A hatóságok minden ügyet egyedileg mérlegelnek, esetről esetre alakítják gyakorlatukat.

2.3.2. Az elfeledtetéshez való jog

Az Európai Unió adatvédelmi rendelete új érintetti jogként teremtette meg az ún. elfeledtetéshez való jogot.[19] Ez lényegében a törléshez való jog internetes közegre alkalmazott végrehajtása, amelynek lényege abban áll, hogy az adatot nyilvánosságra hozó adatkezelő minden észszerű lépést megtesz

[17] Ha a keresőmotor működtetője az egyik tagállamban olyan irodát nyit vagy leányvállalatot hoz létre a keresőmotor által kínált reklámhelyek értékesítésére és reklámozásra, amelynek tevékenysége az adott állam lakosai felé irányul – ítélet 60. pontja.

[18] A konkrét esetben tehát a spanyol jog alapján a spanyol hatóságok járhattak el, egy magyarországi ügyben pedig – a Google Magyarország Kft. érintettsége révén – a magyar hatóságok, illetve bíróságok eljárása válna lehetővé.

[19] Az angol „right to be forgotten” magyar fordítása.

annak érdekében, hogy az adatokat kezelő további adatkezelőket tájékoztassa a törlés végrehajtásának kötelezettségéről. Minden olyan lépést meg kell tennie, amely a **technológia nyújtotta keretek között észszerű költségek mellett elvárható**. A törléshez való jogot tehát abban a közegben kell érvényesíteni, ahol az adatkezelés megvalósul, és az érintett nem kerülhet hátrányosabb helyzetbe attól függően, hogy az adatkezelésre milyen eszközökkel kerül sor (papír alapon vagy digitálisan). Az uniós jogalkotó az új jog megalkotása révén kívánja elérni, hogy az érintettek az interneten is „elfeledtethessék" magukat, illetve a rájuk vonatkozó információkat.

2.3.3. Közösségi oldalak

A közösségi oldalak a világháló olyan szolgáltatásai közé tartoznak, amelynek előzménye a virtuális téren kívül nem létezett. Olyan kapcsolatok építését, megújítását teszi lehetővé, amelyek a földrajzi távolságot áthidalják, tetszőleges számú felhasználóval lehet kapcsolatba lépni, csoportok hozhatók létre, gyors kommunikációs megoldásokat kínálnak. A kapcsolattartást és kapcsolatépítést megkönnyítő szolgáltatások sora hosszan folytatható lenne.

A magánszféra védelme szempontjából a közösségi oldalak **sok lehetőséget**, egyszersmind **kockázatot is rejtenek**. Az **emberi méltóság** az egyén személyiségének, illetve általában az életének **kibontakozás**át, illetve ennek lehetőségét is magában foglalja. Bizonyos felhasználók (fogyatékosok, egymástól távol élő barátok, családtagok stb.) számára a közösségi oldalak sokáig nem ismert lehetőségeket nyújtanak.

A nyilvánosság azonban kétélű: egyik oldalon a közösség számára előnyt jelent a másik elérhetősége, képeinek megtekinthetősége stb., a másik oldalon azonban az adatok **olyan célokra is felhasználhatók, amelyekkel** az egyén a regisztráció alkalmával **nem** feltétlenül **számolt**. Így például a közösségi oldalon létrehozott profil adott esetben a munkáltató által megtekinthető, a nyilvánosan vállalt kommentek bárki számára hozzáférhetők. A nyilvánosságra kerülő adatok védelméről az érintettnek gyakorlatilag le kell mondania, ezért is int óvatosságra a jog az adatok megosztása előtt.

Az alábbiakban azokat a magánszférát érintő kérdéseket vesszük vázlatosan számba, amelyek a közösségi oldalak kapcsán felmerülnek:

- A közösségi oldalak közzétesznek tájékoztatót üzleti működésükről és a személyes adatok kezeléséről is. A gyakorlat szerint ezek azonban nem minden részletre terjednek ki és hallgatnak a személyes adatok üzleti célú felhasználásáról, profilok kialakításáról.
- Profilt bárki létrehozhat bárkinek a nevében. Az álprofilok alkalmasak lehetnek a másik lejáratására, adott esetben az ismerősök megtévesztésére.
- A létrehozott profil beállításai általában bonyolultak, nem magától értetődőek. Amennyiben érvényesülnének a privacy by default[20] beállítások, akkor a felhasználót kevesebb meglepetés érné.
- A közösségi oldalakon szabadon oszthatók meg adatok, képek egymásról. Tipikus esetben a képeken többen is láthatók. A megosztást a jog definíciója szerint nyilvánosságra hozatalként kell értékelnünk, ehhez pedig az összes érintett hozzájárulására szükség lenne. Külön gyakorlati problémát okoz azon érintettek joggyakorlása, akik nem felhasználói a közösségi oldalnak, róluk mégis adatok válnak mások számára elérhetővé.
- A felhasználók magatartását, preferenciáit figyelemmel kísérik, róluk felhasználói profilt alkotnak.
- A megosztott képek jelentős része okostelefonnal készül. A funkció tudatos letiltása nélkül a készülék rögzíti a kép készítésének geolokációs (földrajzi helymeghatározási) adatait is. Ilyen

[20] A GDPR önálló alapelvként vezeti be az alapértelmezett adatvédelem elvét (25. cikk (2) bekezdés).

módon pedig a megosztott képek java része arról is árulkodni fog, hogy a kép hol készült.[21]

- A közösségi oldal általában igényt tart arra, hogy a feltöltött képeket ingyenesen (van, ahol a letiltás lehetősége nélkül) használhassa reklámozási célokra. [22]
- Az egyik közösségi oldal felhasználóit az üzemeltető akkor is követi az interneten, amikor már elhagyták a közösségi portált. Adatvédelmi jogi szempontból nyilvánvalóan túlmutat az ilyen jellegű adatgyűjtés azon a célon, amelynek érdekében a felhasználó az oldalon regisztrált.

Az egyik közösségi portál olyan módon kívánja korlátozni a felelősségét, hogy száz amerikai dollárban maximálja a vele szemben támasztható igényeket. A személyes adatok védelmével összefüggő igények (kártérítés, sérelemdíj) ilyen limitálása nyilvánvalóan ellentétes nem csupán a magyar adatvédelmi szabályozással, hanem a nemzetközi üzleti kapcsolatok logikájával, szokásaival is.

A virtuális közösségek mögött létezik ugyan egy valóságos, bejegyzett gazdasági társaság, de a legtöbb ország esetében semmilyen formában nem telepedtek le. Az egyéni igények érvényesítése nagyban megnehezül azáltal, ha nem világos, hogy az érintett, jogainak kikényszerítése érdekében, mely hatóság / bíróság közreműködését kérheti. E tekintetben az Európai Unió adatvédelmi rendelete világos szabályozást[23] vezetett be: amennyiben a harmadik országban letelepedett adatkezelő árukat vagy szolgáltatásokat[24] kínál az Unióban tartózkodók számára, vagy az Unión belül tanúsított magatartások megfigyelésére irányul a tevékenysége, akkor a rendelet szabályai alkalmazandók. Az ilyen adatkezeléseket annak a tagállamnak a hatósága vizsgálhatja, ahol az érintettek tartózkodnak, illetve panaszt tesznek.

2.4. Felhőalapú szolgáltatások[25]

A jogi szabályozás számára a felhőalapú szolgáltatások és a használatuk során keletkező jogviszonyok, felelősségi viszonyok rendkívül komplex jelenségként azonosíthatók, hiszen a jól érzékelhető adatvédelmi jogi kihívások mellett szerzői jogi, elektronikus kereskedelmi jogi, kötelmi jogi kérdések sorát veti fel.

2.4.1. 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.

A felhőalapú számítástechnika egy olyan modell, amely széleskörű, kényelmes, igény szerint rendelkezésre álló hálózati hozzáférést kínál konfigurálható számítástechnikai erőforrásokhoz, ame-

---

21 Ennek illusztrálására hozta létre egy amerikai professzor az iknowwhereyourcatlives.com oldalt, ahol „macskás képek” gyűjteménye révén mutatja be a funkció sajátosságait.

22 Ennek révén nincs akadálya annak, hogy egy jól sikerült esküvői fényképet például egy rendezvényszervezéssel összefüggő reklámban fognak felhasználni.

23 A GDPR 3. cikk (2) bekezdése szabályozza az EU területén túlra is kiterjedő (extraterritoriális) hatály kérdését.

24 Függetlenül attól, hogy az érintettnek fizetnie kell-e érte, vagy sem.

25 Az alfejezet Dr. Klein Tamás írása.

lyek gyorsan, minimális kezelési ráfordítással és minimális, a szolgáltatóval folytatott interakcióval igénybe vehetők, és nyilvánosan rendelkezésre állhatnak.

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 mindenkori 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 közbeiktatásával a szolgáltató biztosítja, hogy a végfelhasználó a számítóközpont telephelyétől függetlenül hozzáférjen az adatokhoz.

2.4.2. A felhőszolgáltatás legfontosabb tulajdonságai

1. **Igény szerinti önkiszolgálás**: A felhasználó (pillanatnyi) tárolási szükséglete szerint igényelhet tárolási kapacitást, amelyhez bármikor hozzáférhet, a szolgáltató bármilyen közrehatása nélkül.

2. **Széleskörű hálózati hozzáférés**: A tárolási kapacitások hálózaton keresztül érhetők el, és informatikai eszközök széles körével hozzáférhetők.

3. **Erőforrások összevonása**: erőforrások koncentrációja annak érdekében, hogy több felhasználó részére, a felhasználói igények messzemenő figyelembevételével a szolgáltató diverzifikálja azokat.

4. **Teljes flexibilitás**: A koncentrált erőforrások felhasználók részére történő diverzifikálását a rendkívüli rugalmasság, igényekhez való alkalmazkodás jellemzi, a kapacitások megosztása az igényekhez igazodik, újra és újra felosztásra kerül.

5. **Mért szolgáltatás**: A felhőszolgáltatások automatikusan ellenőrzik és optimalizálják az erőforrásaik felhasználását. Mivel az erőforrás felhasználása matematikailag mérhető, így folyamatosan biztosítható a szolgáltatás zavarmentes szervezése és átláthatósága.

2.4.3. A felhőszolgáltatások legfontosabb előnyei a felhasználók számára

1. A felhőszolgáltatások egyik leginkább érzékelhető előnye, hogy a felhasználók számára megszűnik a kapacitásszűkösség, tekintve, hogy az adattárolásuk nem az általuk megvásárolt és működtetett adattároló eszközökön történik. Ez 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.

2. A felhasználók számára a felhő továbbá csaknem teljes rugalmasságot biztosít az igénybe vett tárhely és eszközök tekintetében.

2.4.4. A felhőszolgáltatások általános adatvédelmi kockázatai

A személyes adatok felhőszolgáltatás útján történő feldolgozása a technológia jellegéből fakadó sajátságos kockázatokat hordoz. Különös kockázatot jelent az adatok felett érvényesülő kontroll és az adatfeldolgozási műveletekkel kapcsolatos transzparencia esetleges hiánya.

2.4.4.1. Az információbiztonság áttörése – az ellenőrzés hiánya

A két tipizált kockázati forrás közül az egyik az információbiztonság általános követelményének áttörése, vagyis a teljes körűen érvényesülő ellenőrzés hiánya, hiszen a felhőszolgáltatás igénybe vevője, miután – 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 visszássághoz vezet, tekintettel arra, hogy az ellenőrzés (potenciális, de 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.

2.4.4.2. Adathordozhatóság kétségessége

Az adatok folyamatos, és feltétlen rendelkezésre állása bizonyos körülmények között kétségessé 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.

2.4.4.3. 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.

2.4.4.4. Az adatvédelmi szint univerzalitásának hiánya

A felhőszolgáltatások határokon átívelő, globális szolgáltatások. A szolgáltatók gyakorta több országban párhuzamosan hoznak létre adatközpontokat, így a szolgáltatás tényleges helye és ezáltal a vonatkozó nemzeti jog időszakosan változhat, pl. csúcsterhelés esetén valamely adatközpont kapacitásának hiánya miatt. 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 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.

3. ELEKTRONIKUS KERESKEDELEM JOGA

A fejezet Dr. Grad-Gyenge Anikó írása.

3.1. Szerepe és jelentősége

Az elektronikus kereskedelem szerepe a gazdaságban elsősorban a kiskereskedelemben, azaz a végfelhasználókat célzó kereskedelmi forgalomban jelentős, de a nagykereskedelmi forgalom nem jelentéktelen része is bonyolódhat elektronikus úton. A jelen fejezet az elektronikus kereskedelem előbbi részével foglalkozik.

A kereskedelmi forgalom növekvő arányú része bonyolódik elektronikus kereskedelem útján a Központi Statisztikai Hivatal hozzáférhető adatai alapján. E növekedés okai az elektronikus fizetési módok iránti bizalom növekedése, az elektronikusan elérhető áruk és szolgáltatások számának növekedése, de a háttérben meghúzódik a szélessáv nagyobb elterjedtsége és az elektronikus írástudás növekedése is.

3.2. Az elektronikus kereskedelem szabályozásának célja

Bár az internet hajnalán voltak olyan elképzelések, amelyek támogatták volna az internetes tevékenységek szabályozásmentességét, az elektronikus kereskedelem legnagyobb része ma már valamilyen állami vagy önszabályozás alá tartozik. A magyar jogrendszerben e szabályok magját az elektronikus kereskedelemről szóló törvény (az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény – a továbbiakban: Elkertv.) adja, amely jogharmonizáció eredményeként került be a magyar jogba. Ennek köszönhetően az EU más tagállamaiban is igen hasonló rendelkezések találhatók az elektronikus kereskedelem tekintetében. E törvény az elektronikus kereskedelem sajátosságainak megfelelő szabályokat tartalmazza.

Ugyanakkor az elektronikus kereskedelem szabályozása messze nem csupán erre az egy törvényre korlátozódik, mivel számos más jogszabály is alkalmazandó ezen a területen.

3.3. Az elektronikus kereskedelem és résztvevői

Az elektronikus kereskedelmi szabályozás alapja a kereskedelemben részt vevő szereplők, illetve a kereskedelem tárgyának, a kereskedelmi szolgáltatásnak a definíciója.

Az elektronikus kereskedelmi szolgáltatás egyúttal mindig információs társadalommal összefüggő szolgáltatás is.

Az információs társadalmi szolgáltatások
- elektronikus úton,
- távollevők részére,
- rendszerint (de nem kizárólag) ellenszolgáltatás fejében nyújtott szolgáltatások,
- amelyhez a szolgáltatás igénybe vevője egyedileg fér hozzá.

Az elektronikus kereskedelmi szolgáltatásra ezen belül jellemző, hogy:
- célja valamely birtokba vehető forgalomképes ingó dolog – ideértve a pénzt és az értékpapírt, valamint a dolog módjára hasznosítható természeti erőket –, szolgáltatás, ingatlan, vagyoni értékű jog (a továbbiakban együtt: áru)
- üzletszerű
- értékesítése, beszerzése, cseréje vagy más módon történő igénybevétele.

Míg információs társadalommal összefüggő szolgáltatás lehet egy személyes blog működtetése, addig az elektronikus kereskedelmi szolgáltatások között a legtipikusabb az online webshopok működtetése.

Szolgáltató lényegében bárki lehet. A szabályozásban kiemelkedő jelentősége van az ún. közvetítő szolgáltatóknak, akik mások szolgáltatásának az igénybe vevők számára való eljuttatásában játszanak meghatározó szerepet.

A magyar szabályozás jelenleg négyféle közvetítő szolgáltatót ismer, ezek a következők:
- az igénybe vevő által biztosított információt távközlő hálózaton továbbítja, vagy a távközlő hálózathoz hozzáférést biztosít (egyszerű adatátvitel- és hozzáférés-biztosító szolgáltató);
- az igénybe vevő által biztosított információt távközlő hálózaton továbbítja, és az alapvetően a más igénybe vevők kezdeményezésére történő információtovábbítás hatékonyabbá tételét szolgálja (gyorsítótárolást végző szolgáltató);
- az igénybe vevő által biztosított információt tárolja (tárhelyszolgáltató);
- információk megtalálását elősegítő segédeszközöket biztosít az igénybe vevő számára (keresőszolgáltatást nyújtó szolgáltató).

A szolgáltatás igénybe vevője az a természetes, illetve jogi személy, aki/amely információs társadalommal összefüggő szolgáltatást vesz igénybe.

3.4. A szabályozott szolgáltatások

Számos olyan szolgáltatás van például, amely technológiailag nem, vagy csak részben kapcsolódik Magyarország területéhez (valósul meg Magyarország területén), mégis számos elemében kötődik Magyarországhoz, például az igénybe vevői magyar állampolgárok. Mivel tehát az elektronikus kereskedelem jelentős része határon átnyúló tevékenység, igen nagy jelentősége van annak, hogy mely szolgáltatások tekintetében alkalmazandó a magyar jog és azon belül az Elkertv.

Az Elkertv. szabályai alkalmazandók bármely, Magyarország területéről nyújtott szolgáltatásra. Ennek megítélésénél a tényleges tevékenységvégzés helye a döntő, ilyen lehet a szerverek üzemeltetése, de akár egy webshop raktárkészletének elhelyezése, vagy a számlázási tevékenység is.

Akkor is a törvényt kell alkalmazni, ha szolgáltatást nem Magyarország területéről, hanem Magyarország területére irányulóan nyújtanak.[26] Magyarország területére akkor irányul a szolgáltatás, ha a szolgáltatásról a használt nyelv, a pénznem és egyéb körülmények alapján valószínűsíthető, hogy magyarországi igénybe vevők számára kívánják elérhetővé tenni.

[26] Elkertv. 1. § (1) bekezdés a) pont

3.5. Az előzetes engedélyezést kizáró elv

Figyelembe véve, hogy az internet-hálózat – elméletileg – korlátlan mennyiségű szolgáltatás nyújtására alkalmas, nincs ok arra, hogy a szolgáltatásnyújtás előzetes engedélyezéshez legyen kötve, ezáltal válogatva a nyújtható szolgáltatások között. A szolgáltatásnyújtás szabadságát biztosítja az előzetes engedélyezést kizáró elv, amely szerint az ilyen szolgáltatás nyújtásának megkezdéséhez, illetve folytatásához előzetes engedély vagy bármely ezzel azonos joghatású hatósági határozat nem szükséges. Ez természetesen nem érinti az információs társadalommal összefüggő szolgáltatás útján végzett tevékenységre külön jogszabályban, nem az elektronikus úton történő szolgáltatásnyújtásra tekintettel előírt minősítési, képesítési, engedélyezési vagy bejelentési kötelezettséget (például a gyógyszerek forgalomba hozatali engedélyezését).

3.6. Az információs társadalommal összefüggő szolgáltatással kapcsolatos adatszolgáltatás

Az elektronikus kereskedelemben a szolgáltatást nyújtó személy sokkal nehezebben található meg, azonosítható be, mint a hagyományos kereskedelem szereplői, hiszen nem is történik vele személyes kapcsolatfelvétel (ugyanez igaz egyébként az igénybe vevő személyére is). Annak érdekében, hogy a szolgáltatás igénybe vevője megfelelően informálódhasson arról, hogy kivel lép jogviszonyba, a szolgáltató egyes adatait köteles hozzáférhetővé tenni, így különösen

- a nevét,
- a székhelyét, telephelyét, ennek hiányában lakcímét,
- az elérhetőségére vonatkozó adatokat, különösen az igénybe vevőkkel való kapcsolattartásra szolgáló, rendszeresen használt elektronikus levelezési címét,
- ha erre szükség van, a nyilvántartásba bejegyző bíróság vagy hatóság megnevezését, és a nyilvántartásba vételi számát,
- ha erre szükség van, a tevékenysége engedélyezéséről szóló tényt az engedélyező hatóság megnevezésével és elérhetőségi adataival, valamint az engedély számával együtt,
- ha a szolgáltató ÁFA-alany, az adószámát.

3.7. A szolgáltató és a közvetítő szolgáltató felelőssége a szolgáltatásán keresztül hozzáférhetővé tett információért

Attól függően, hogy a szolgáltató tevékenysége mire terjed ki, igen változatos lehet az, hogy mennyire tudja befolyásolni az általa az igénybe vevőhöz eljuttatott információnak a helyességét, jogszerűségét, így a felelőssége ezért differenciált. Ha valaki maga a tartalomszolgáltató, akkor természetesen nincs lehetőség a mentesülésre, ő mindenképp felel az információért, hiszen az ő cselekménye maga a jogsértő tartalom hozzáférhetővé tétele.[27]

A közvetítő szolgáltatók esetében a mentesülés feltételei négy csoportba oszthatók, a szolgáltatás négy alaptípusának megfelelően.

[27] Ezt megerősíti a BDT2008. 1777. is, amely szerint az internetes tartalomszolgáltató maga állítja elő és teszi közzé az információt, ezért felelőssége közvetlen, míg a közvetítő szolgáltató a tartalom előállításába nem avatkozik bele, ezért felelőssége korlátozott.

Az egyszerű adatátvitelt és hozzáférést biztosító szolgáltató akkor nem felel a továbbított információért (ideértve a közbenső és átmeneti jellegű tárolást is, ha ez kizárólag az információtovábbítás lebonyolítására szolgál és az információt nem tárolják hosszabb ideig, mint az a továbbításhoz szükséges), ha

- nem a szolgáltató kezdeményezi az információ továbbítását;
- nem a szolgáltató választja meg a továbbítás címzettjét, és
- a továbbított információt nem a szolgáltató választja ki, illetve azt nem változtatja meg.

A gyorsítótárolást nyújtó szolgáltató akkor nem felel az információ közbenső és átmeneti jellegű automatikus tárolásával okozott kárért, ha

- a szolgáltató nem változtatja meg az információt;
- a tárolt információhoz való hozzáférés megfelel az információ hozzáférésével kapcsolatban támasztott feltételeknek;
- a közbenső tárolóban az információ frissítése megfelel a széleskörűen elismert és alkalmazott információfrissítési gyakorlatnak;
- a közbenső tárolás nem zavarja meg az információ felhasználásával kapcsolatos adatok kinyerésére szolgáló, széleskörűen elismert és alkalmazott technológia jogszerű használatát; és
- a szolgáltató haladéktalanul eltávolítja az általa tárolt információt vagy nem biztosítja az ahhoz való hozzáférést, amint tudomást szerzett arról, hogy az információt az adatátvitel eredeti kiindulási pontján a hálózatról eltávolították, vagy az ahhoz való hozzáférés biztosítását megszüntették, illetve, hogy a bíróság vagy más hatóság az eltávolítást vagy a hozzáférés megtiltását elrendelte.

A tárhelyszolgáltató akkor nem felel az igénybe vevő által biztosított információért, ha

- nincs tudomása az információval kapcsolatos jogellenes magatartásról, vagy arról, hogy az információ bárkinek a jogát vagy jogos érdekét sérti;
- amint az előzőekről tudomást szerzett, haladéktalanul intézkedik az információ eltávolításáról, vagy a hozzáférést nem biztosítja.[28] A keresőmotor-szolgáltató akkor nem felel az információ hozzáférhetővé tételével okozott kárért, ha
- nincs tudomása az információval kapcsolatos jogellenes magatartásról, vagy arról, hogy az információ bárkinek a jogát vagy jogos érdekét sérti;
- amint az előzőekről tudomást szerzett, haladéktalanul intézkedik az elérési információ eltávolításáról vagy a hozzáférés megtiltásáról.

A szolgáltató a bemutatott szabályok alapján sem mentesül azonban a felelősség alól, ha az igénybe vevő a szolgáltató megbízásából vagy utasításai alapján cselekszik.

Igen fontos azonban, hogy a közvetítő szolgáltató nem köteles folyamatosan ellenőrizni az általa csak továbbított, tárolt, hozzáférhetővé tett információt, továbbá nem köteles olyan tényeket vagy körülményeket keresni, amelyek jogellenes tevékenység folytatására utalnak. Ezt az Európai Bíróság vonatkozó döntései is megerősítik, kitérve arra is, hogy melyek azok a feltételek, amikor ilyen keresésre, szűrésre mégis kötelezhető a szolgáltató.

A Tiscali/Scarlet-ügyben az Európai Bíróság kimondta, hogy az elektronikus kereskedelmi szabályok alapján az egyszerű adatátvitelt, hozzáférést biztosító szolgáltatóval szemben a nemzeti bíróság által alkalmazható „jogsértés abbahagyására kötelezés” nem terjed ki arra, hogy a szolgáltatót

[28] Ezt erősíti meg a BH2011. 294. is, amely szerint az internetes weboldalon megjelenő „*üdülési csekket keresek*” szövegű apróhirdetés nem valósít meg gazdasági reklámot. A közvetítő szolgáltató felelőssége a jogsértő tartalmú apróhirdetésért fennáll, ha a jogsértésről való tudomásszerzést követően annak eltávolításáról nem rendelkezik. Az üdülési csekk névre szólóan kibocsátott utalvány, meghatározott, hogy milyen szolgáltatásra váltható be, ha ettől eltérően jogellenes átruházásra irányuló vételei szándékot fogalmaz meg egy hirdetés, az jogsértő.

kötelezzék a jogsértő tartalom általános szűrésére, illetve blokkolására. A szűrésre, blokkolásra kötelezés során törekedni kell az arányosságra, az nem szolgálhat prevenciós célt, és nem lehet kizárólag a közvetítő szolgáltató költségére előírni.

A Bonnier-ügyben az Európai Bíróság arányosnak tartotta és nem tekintette az uniós jogba ütközőnek azt a (svéd) tagállami megoldást, amely lehetővé teszi, hogy egy adott internet-előfizető vagy internethasználó azonosítása érdekében arra kötelezzék az internet-hozzáférést biztosító szolgáltatót, hogy a szerzői jog jogosultjának vagy ez utóbbi jogutódjának tájékoztatást adjon arról az előfizetőről, akinek a szolgáltató egy adott IP-címet (internetprotokoll) biztosított, amely címről állítólag a jogsértést elkövették.[29]

Az Európai Bíróság a Google France ügyben[30] arra jutott, hogy a Google keresőmotor-szolgáltatásában megjelenő hirdetés nem valósít meg védjegyszerű használatot akkor, amikor a védjeggyel védett kifejezést megjeleníti a keresőmotor találatai között. Ilyen módon pedig nem lehet jogsértő a magatartása. Ezzel szemben a L'Oréal és társai kontra eBay ügyben[31] (C-324/09) a L'Oréal szerint az eBay olyan kulcsszavakkal irányítja védjegyjogot sértő árukhoz a fogyasztókat, amelyek megegyeznek a védjegy-oltalom alatt álló kifejezésekkel, valamint a szűrési rendszerük nem elegendő. A Bíróság itt is azt mondta, hogy az online piac üzemeltetője maga a saját tevékenységével nem használja a védjegyeket, ha csupán annyi a tevékenysége, hogy lehetővé teszi az ügyfelei számára, hogy azok védjegyekkel megegyező megjelöléseket jelenítsenek meg az oldalon. De ha a megjelenítések súlyozását is végzi (optimalizálja), akkor viszont olyan „tevőleges szerepet" is játszik, melynek révén nem mentesülhet a felelősség alól. Sőt, a Bíróság ezt követően azt is kifejtette, hogy egyes esetekben még a „tevőleges magatartásra" sincs szükség, mivel ha megfelelő gondosság mellett tudott vagy tudnia kellett volna olyan tényekről vagy körülményekről, amelyek alapján valamely gondosan eljáró gazdasági szereplőnek fel kellett volna ismernie az online eladásra való felkínálások jogellenességét, akkor haladéktalanul gondoskodnia kell a szóban forgó adatok eltávolításáról vagy az azokhoz való hozzáférés megszüntetéséről is, nem kell ehhez felszólítás sem. Ha ezt nem teszi meg, felelőssége megállapítható, és kötelezhető arra, hogy intézkedéseket hozzon eladóként tevékenykedő ügyfelei azonosításában. A Google Spain ügyben[32] (C-131/12) az Európai Bíróság úgy döntött, hogy a személy ellen vezetett végrehajtásról szóló információk személyes adatnak minősülnek, a keresőmotor-szolgáltatást nyújtó közvetítő szolgáltató pedig adatkezelőnek minősül. Amennyiben pedig a személyes adatok megjelenése a keresőmotorban sérti az érintett személy személyiségi jogait, a szolgáltató kötelezhető az eltávolításra, méghozzá függetlenül attól, hogy végső soron az adatok elérhetősége, hozzáférhetősége okoz-e kárt vagy sem.

Az EJEB egy meghatározó jelentőségű döntésében[33] foglalkozott a kommentekért való felelősség kérdésével.[34] Az EJEB lényegében változatlanul fenntartotta a nemzeti bírósági döntéseket, amelyek a DELFI nevű hírportált nem tekintették közvetítő szolgáltatónak, hanem tartalomszolgáltatónak minősítették, méghozzá azért, mert egyrészt a hozzászólásra felhívta az olvasókat (ami egyébként anyagi érdeke is volt), másrészt a portálon elhelyezett reklámokból bevételre tett szert, végül pedig azért, mert képes volt a kifogásolt kommentek eltávolítására és előre láthatta a jogsértéseket. Az EJEB kimondta, hogy nem feltétlenül elegendő sem az értesítési és eltávolítási eljárás alkalmazása,

---

29 A Bíróság 2012. április 19-i C-461/10. számú ítélete a Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB kontra Perfect Communication Sweden AB ügyben.

30 A Bíróság 2010. március 23-i C-236/08. számú ítélete a Google France, Google Inc. kontra Louis Vuitton Malletier ügyben.

31 A Bíróság 2011. július 12-i C-324/09. számú ítélete a L'Oréal SA és tsai kontra eBay International és tsai ügyben.

32 A Bíróság 2014. május 13-i C-131/12. számú ítélete a Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González ügyben.

33 64569/09. sz. beadvány. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-126635%22]}, és https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-155105%22]}.

34 Az ügyet részletesen elemzi Nádori Péter: Delfi AS v. Észtország: strasbourgi döntés a névtelen kommentekért viselt szolgáltatói felelősségről című cikkében. Infokommunikáció és Jog 56. szám.

sem egy szűrőprogram alkalmazása, de még egy járulékos felvilágosító program sem a személyiségi jogsértések megakadályozására, eszerint pedig a kommentelésre lehetőséget nyújtó (tárhely) szolgáltató lényegében teljes felelősséggel tartozik a rajta keresztül megvalósított személyiségi jogsértésért.

3.8. Értesítési és eltávolítási eljárás

Az értesítési és eltávolítási eljárás azt a célt szolgálja, hogy a szerzői és szomszédos jogi, valamint a védjegyjog által védett szellemi alkotásokon fennálló jogok megsértése ellen a lehető leggyorsabban lehessen fellépni. Az Elkertv. 2014. január 1-je óta biztosítja az eljárás alkalmazhatóságát olyan esetekben is, amikor kiskorú személyiségi jogának megsértésére kerül sor, vagyis az eljárás egy igen korlátozott körben már személyiségi jogok megsértése elleni fellépésre is alkalmas. Az eljárás lefolytatása biztosítja, hogy a felelősség alól a szolgáltató mentesülni tudjon.

Az említett jogok jogosultja felhívhatja a szolgáltatót a jogát sértő tartalom eltávolítására a sérelem tárgyának és a jogsértést valószínűsítő ténynek a megjelölésével; a jogsértő tartalmú információ azonosításához szükséges adatokkal; a jogosult nevének, lakcímének, illetve székhelyének, telefonszámának, valamint elektronikus levelezési címének megadásával.

Az értesítés átvételétől számított 12 órán belül a szolgáltató köteles intézkedni, hogy az értesítésben megjelölt információhoz való hozzáférést a továbbiakban ne biztosítsa vagy az információt eltávolítsa, és feltüntetni, hogy az eltávolítás milyen jogosult jogsértést állító értesítése alapján történt.

Egyúttal a szolgáltató köteles tájékoztatni az igénybe vevőt az eltávolításról. Az érintett igénybe vevő a tájékoztatás átvételétől számított 8 napon belül teljes bizonyító erejű magánokiratban vagy közokiratban a szolgáltatónál indokolt kifogással élhet az érintett információ eltávolításával szemben. A minden adatot tartalmazó kifogás átvételekor a szolgáltató haladéktalanul köteles az érintett információt újra hozzáférhetővé tenni, és erről a jogosultat a kifogás megküldésével értesíteni, kivéve, ha az eltávolítást vagy a hozzáférés megtiltását bíróság vagy hatóság rendelte el.

Ha a jogosult az értesítés átvételétől számított 10 munkanapon belül bírósági jogorvoslattal él, a szolgáltató a bíróság erre vonatkozó, ideiglenes intézkedést elrendelő határozatának kézhezvételétől számított 12 órán belül az értesítésben megjelölt információhoz való hozzáférést ismételten nem biztosítja, illetve az információt ismételten eltávolítja.

A jogosult köteles az eljárásban hozott jogerős érdemi határozatokról – ideértve az ideiglenes intézkedés elrendelését vagy a kérelem elutasítását is – a szolgáltatót haladéktalanul értesíteni. Az érdemi határozatban foglaltaknak a szolgáltató haladéktalanul köteles eleget tenni.

A szolgáltató nem felelős az érintett információ eltávolításának vagy az ahhoz való hozzáférés nem biztosításának eredményes végrehajtásáért, amennyiben az eltávolítás vagy a hozzáférés nem biztosítása során a fentieknek megfelelően és jóhiszeműen járt el.

3.9. Az elektronikus hirdetésre vonatkozó különös szabályok

Az elektronikus hirdetés:

- bármely információs társadalommal összefüggő szolgáltatás vagy – a beszédcélú telefonhívás kivételével – elektronikus hírközlés útján közölt közlés, tájékoztatás, illetve megjelenítési mód (pl. pop-up ablak), amely valamely birtokba vehető forgalomképes ingó dolog – ideértve a pénzt, az értékpapírt és a pénzügyi eszközt, valamint a dolog módjára hasznosítható

természeti erőket –, szolgáltatás, ingatlan, vagyoni értékű jog értékesítésének vagy más módon történő igénybevételének előmozdítására, vagy e céllal összefüggésben a vállalkozás nevének, megjelölésének, tevékenységének népszerűsítésére vagy áru, árujelző ismertségének növelésére irányul (a továbbiakban: reklám), vagy társadalmi cél megvalósításához kapcsolódó, reklámnak nem minősülő tájékoztatás.

Az minősül elektronikus hirdetőnek, akinek érdekében az elektronikus hirdetést közzéteszik, illetve aki a saját érdekében az elektronikus hirdetés közzétételét megrendeli. Elektronikus hirdetési szolgáltató az, aki önálló gazdasági tevékenysége körében az elektronikus hirdetést elkészíti, létrehozza, illetve ezzel összefüggésben egyéb szolgáltatást nyújt (nem feltétlenül azonos a platform közvetítő szolgáltatójával, ahol a reklám megjelenik). Az elektronikus hirdetés közzétevője az a személy, aki az elektronikus hirdetés közzétételére alkalmas eszközökkel rendelkezik és ezek segítségével az elektronikus hirdetést megismerhetővé teszi. Elektronikus hirdetés közzétételéről pedig akkor beszélünk, ha az elektronikus hirdetés megismerhetővé válik, akár nagyobb nyilvánosság, akár egyedi címzett számára.

A törvény az opt-in elvet érvényesíti, azaz ahhoz, hogy a címzett elektronikus hirdetést kaphasson, előzetesen hozzá kell járulnia, ez lehet konkrét, de lehet általános hozzájárulás is. A hozzájáruló nyilatkozat bármikor korlátozás és indokolás nélkül, ingyenesen és bármilyen formában visszavonható.

A címzettel közölt reklámhoz kapcsolódóan egyértelműen és szembetűnően tájékoztatni kell a címzettet arról a címről és egyéb elérhetőségről, ahol az ilyen reklámok részére történő közléséhez való hozzájáruló nyilatkozatának visszavonása, illetve a reklám küldésének megtiltása iránti igényét bejelentheti.

Az elektronikus hirdetésre vonatkozó szabályok betartását a Nemzeti Média- és Hírközlési Hatóság ellenőrzi. Az NMHH a kéretlen elektronikus hirdetéssel összefüggő rendelkezések megsértése esetén széles szankcionálási eszköztárral rendelkezik – a körülmények mérlegelése alapján – a jogsértő állapot megszüntetésének elrendelésétől egészen az ötvenezer forinttól ötszázezer forintig terjedő összegű elektronikus kereskedelmi bírság kiszabásáig.

3.10. Magatartási kódexek alkalmazása

Az elektronikus kereskedelemben különösen fontos az állami és piaci szereplők együttes, megállapodáson nyugvó normáinak kialakítása, illetve az üzleti szereplők önszabályozása. Ez teszi lehetővé a változó körülményekhez való gyors igazodást. Az együttes/társszabályozások és önkéntes szabályozási kódexek kialakítása elsősorban a résztvevők feladata, az állam szerepe itt csak másodlagos, legfeljebb támogató jellegű lehet.

Ilyen magatartási kódex a bankok elektronikus úton történő szolgáltatásnyújtásra vonatkozó eljárási rendje, de a BDT2008.1740 szerint ilyennek minősül a Magyarországi Internet Szolgáltatók Tanácsának Tudományos Egyesülete által létrehozott domainregisztrációs szabályzat is.[35]

[35] http://www.domain.hu/domain/szabalyzat/szabalyzat.html

4. ELEKTRONIKUS HÍRKÖZLÉSJOG

A fejezet Dr. Tóth András írása.

4.1. Fogalommeghatározás

Az **elektronikus hírközlés** az erre szolgáló (pl. kábeles, műholdas, mobil és hagyományos vezetékes, mikrohullámú stb.) hálózatokon végzett jelátviteli tevékenységet jelenti. Az **elektronikus hírközlésjog** pedig az ezen tevékenységgel kapcsolatos közérdekű elvárásokat jeleníti meg, így például: a piacra lépés, versenyélénkítés, egyetemes szolgáltatás biztosítása, adatvédelem, hálózatbiztonság, fogyasztói jogok, fogyatékkal élők hozzáférésének előmozdítása, hatékony frekvenciagazdálkodás terén.

4.2. Jelentőség és főbb jellemzők

Az elektronikus hírközlés a digitális gazdaságunk **alapinfrastruktúráját** adja, ebből fakadóan **gazdasági ágazatként** is jelentős. **Globális** jellege miatt a szabályozást a nemzetek feletti karakter is meghatározza (ENSZ, WTO, EU). Az EU-ban a terület (gazdasági jelentősége okán) az **egységes belső piaccá** fejlesztés érdekében kapott uniós szintű szabályozást. Ráadásul az EU-ban ez volt az **első olyan közszolgáltatás, amelyet sikerrel liberalizáltak,** vagyis nyitottak meg a piaci verseny előtt, amely az árak csökkentéséhez és a szolgáltatások színvonalának emeléséhez vezetett szerte az EU-ban éppen ezért az EU elektronikus hírközlés-szabályozása **modellértékű** a közszolgáltatások szabályozói fejlesztése szempontjából.

Az elektronikus hírközlés egy EU-s szabályozási fogalom, amely a 2000-es évek elején lejátszódott technológiai **konvergencia** szabályozási következményeként állt elő. A konvergenciát a **digitalizáció** tette lehetővé, amely révén az átvitt jelek olyan mértékű tömörítése volt megvalósítható, melynek eredményeként a korábban elkülönült jelátviteli platformok (kábeles, műholdas, mobil és hagyományos vezetékes) közötti határvonal az átvitt tartalom (hang, adat, kép) szempontjából teljesen megszűnt. Ekként vált lehetővé, hogy a hagyományosan hangátvitelre szolgáló távközlési hálózaton adat (internet) és audiovizuális (TV) jelek is továbbíthatók, vagy az eredetileg televíziózásra szolgáló kábeltelevíziós hálózatokon immár internet- és telefonszolgáltatás is elérhető.

Az EU elektronikus hírközlés-szabályozása szerint a távközlés (hangátvitel), média (TV és rádiójelek átvitele) és informatika konvergenciája azt jelenti, hogy **minden átviteli hálózatra egységes szabályozásnak kell kiterjednie**, ugyanakkor a tartalom és átvitel szabályozását egymástól el kell választani.

4.3. Alapjogi vonatkozások

4.3.1. Hálózatsemlegesség

A digitalizáció ellenére a növekvő online tartalomfogyasztás és kínálat (pl. YouTube, Netflix) **folyamatos kapacitás bővítést** igényel az infrastruktúra szolgáltatók részéről. Rendre felmerül, hogy ezeket a költséges infrastruktúra fejlesztéseket **kinek kellene megfizetnie** és az infrastruktúra-szolgáltatók részéről nagy a csábítás, hogy ezeket a többletberuházásokat a tőkeerős tartalomfejlesztőkkel fizettessék meg. Ráadásul az átviteli szolgáltatók ennek kikényszerítéséhez hatásosan tudnak fenyegetni a jelátviteli utak blokkolásával. Erre a vitára vezethető vissza a hálózatsemlegesség elve, amely azt jelenti, hogy az internethez bármely tartalomkínáló szabadon hozzáférhet, és ez egyúttal biztosítja számára, hogy a felhasználók el is érjék. Az EU 2015/2120/EU **hálózatsemlegességi rendelete** tiltja az internetes tartalom blokkolását vagy az ezzel egyenértékű minőségrontást, ide nem értve az ésszerű forgalomszabályozást. A rendelet szerint a nyílt internet nem korlátozható, a teljes internethez biztosítani kell a hozzáférést, **nem lehet a priorizálásért** többletdíjat kérni. A rendelet megengedi azonban, hogy az infrastruktúra-szolgáltatók optimalizált hozzáférési szolgáltatásokat kínáljanak, illetve különböző sávszélességű kiskereskedelmi hozzáférési csomagokat alakítsanak ki. A fogyasztóknak pedig joguk van a nekik biztosított sávszélesség tényleges ellenőrzésére és felmondhatják az előfizetői szerződést, ha a szerződésükben vállalt minimális sávszélesség nem teljesül.

4.3.2. Az internethez való hozzáférés korlátozása

Az EU 2009/140/EK irányelve alapján az internethozzáférés alapvető az oktatási és szólásszabadság jogainak érvényesülése szempontjából, ezért az ahhoz **való hozzáférést csak az alapvető jogok tiszteletben tartásával lehet korlátozni.** A 2002/21/EK irányelv szerint az alapjogok korlátozásával járó végfelhasználói hozzáférés-korlátozásoknak szükségesnek és arányosnak kell lenniük, biztosítva a hatékony bírói jogvédelmet, a tisztességes és pártatlan eljárást, az ártatlanság vélelmét és a magánszféra védelmét.

4.4. A liberalizáció és globális háttere

Miként arról már volt szó, az elektronikus hírközlés az első olyan közszolgáltatás, amelyet az EU sikerrel nyitott meg a piaci verseny előtt, amely lehetővé tette ezen szolgáltatások árának csökkenését, minőségének növekedését és ezek által hatékony elterjedését a felhasználók körében, amely alapvető fontosságúnak bizonyult a digitális gazdaság egészének fejlődése szempontjából.

A **közszolgáltatások** (víz, gáz, áram, közlekedés, posta, hírközlés) jellemzően **hálózatos iparágak**, amely kifejezi ezen szolgáltatások infrastrukturális jellegét. Ezen jellegből fakad azonban a verseny nehézsége, miután a már létező hálózatok megkettőzése gazdaságilag nem feltétlenül ésszerű. Éppen a hírközlés mutatott azonban arra rá, hogy ez nem is lehetetlen, így a hálózatos közszolgáltatások korábban feltételezett **természetes monopólium** szerinti megítélése lassú eróziónak indult, pontosan a hírközlési ágazatban bekövetkezett fejleményeknek köszönhetően.

Az 1970-es években végbemenő technológiai fejlődés és a jelentően megnövekedett kereslet a kommunikációs szolgáltatások iránt ugyanis oda vezetett, hogy a már létező hálózatokat bizonyos szinten a versenytársak megtérülő módon duplikálni tudták. Ennek volt a következménye az a per,

amit az 1970-es években egy MCI nevű cég kezdeményezett az USA-ban a világ akkori legnagyobb távközlési vállalata, az amerikai AT&T ellen, mert az megtagadta tőle a hálózat helyi szintű összekapcsolását, ezzel korlátozva a versenytársat távolsági szolgáltatások nyújtásában, ahol ő már párhuzamos infrastruktúrát kezdett kiépíteni. Az ügyben az amerikai bíróság az 1980-as évek elején megállapította, hogy az ilyen elzárkózás törvénytelen, mert a nélkülözhetetlen eszköz feletti kontrollt átvetítheti más piacra.

Ezek a fejlemények az amerikai piacokon egybeestek a **szolgáltatáskereskedelmi általános egyezmény (GATS)** létrehozására irányuló Uruguay-i Forduló indulásával, amelynek eredményeként 1995-ben létrejött a Világkereskedelmi Szervezet (WTO). Az USA el akarta kerülni, hogy a nála megnyíló hírközlési versenyen olyan monopóliumok nyerészkedjenek, amelyek nemzeti piacai védettséget élveznek, ezért az USA a szabad szolgáltatáskereskedelmi tárgyalások részévé tetette a hírközlési ágazatot, ami oda vezetett, hogy a GATS **1998-tól előírta a nemzeti hírközlési piacok liberalizációját**, azaz a monopoljogok lebontását. Miként az *MCI v. AT&T* per is rámutatott, a versenytársak nem álltak rögtön rajtra készen teljesen párhuzamos hálózati infrastruktúrával, bizonyos mértékig rá voltak utalva a volt monopóliumok infrastruktúrájára.

Ezért a GATS előírta, hogy az államok diszkriminációmentes feltételek mellett biztosítsák a versenytársak számára a **hálózatokhoz való hozzáférést**. A GATS egyúttal elismerte a hírközlés közszolgáltatás-jellegét is az **egyetemes szolgáltatások** biztosítása formájában, amely világossá tette, hogy a hírközlési szolgáltatások elérhető árú és földrajzi elhelyezkedéstől független hozzáférhetősége nem válhat a verseny áldozatává. A versenyben ugyanis a szolgáltatók nyilván csak a jövedelmező területekre koncentrálnák erőforrásaikat, amely veszélybe sodorná a közszolgáltatási jelleg érvényesülését. Mindemellett a GATS előírja, hogy a **piacra lépés** feltételeinek megismerhetőnek kell lenniük, a szabályozó hatóságnak **el kell különülnie** a szolgáltatóktól, a **szűkös erőforrásokat** (frekvenciák) pedig objektív, transzparens, diszkriminációmentes eljárásban kell kiosztani.

4.5. Az EU elektronikus hírközlésjoga

Az EU-ban a liberalizációra, a korábbi nemzeti monopoljogok lebontására a Bizottság által az **EUMSz 106. cikk (3) bekezdése alapján kibocsátott irányelvek** alapján került sor. Miután ez az egyetlen, tagállamoktól független, Szerződésen alapuló irányelvalkotási jogosítványa a Bizottságnak, ezért a liberalizációs folyamat elején – az 1980-as évek végén – a tagállamok megrettentek attól, hogy a közszolgáltatások piacának megnyitására úgy fog sor kerülni, hogy arra nem lesz majd ráhatásuk. Ez különösen olyan stratégiai jelentőségű közszolgáltatások esetében aggasztotta a tagállamokat, mint az energetika. Emiatt került sor 1989-ben egy **politikai kompromisszum** megkötésére a tagállamok és a Bizottság között, melynek eredményeként a Bizottság elfogadta, hogy az EUMSz 106. cikken alapuló liberalizációs hatáskörét csak a hírközlési szektort illetően gyakorolja.

Miután a hírközlés gazdasági ágazatként is jelentős, ezért az **egységes belső piaccá válás** érdekében a GATS által is előírt szabályozását már a Tanács és a Parlament irányelvei teremtették meg. Az alábbi szabályozási területeket szükséges e helyen kiemelni:

Verseny megteremtése: miként arról már volt szó, a monopoljogok lebontása önmagában nem fogja a verseny megjelenést biztosítani, éppen ezért szükség van a volt monopolszolgáltató **hálózatához való hozzáférés biztosítására**. Miután a liberalizációnak köszönhetően a piaci pozíciók változhatnak, ezért olyan szabályozási megoldást kellett keresni (különösen. mert alkotmányjogilag tulajdonjoghoz való jog korlátozásáról van szó), amely rugalmasan biztosítja, hogy csak azt a vállalkozást sújtsa a hozzáférésbiztosítási (és azt támogató egyéb) kötelezettség, amely valóban megkerülhetetlen pozícióban van. Erre a célra szolgál a **jelentős piaci erő** koncepciója, melynek azonosítására tagállami szinten, a kompetens szabályozóhatóság által versenyjogi alapokon kerül sor.

Egyetemes szolgáltatás: A tagállamoknak gondoskodniuk kell arról, hogy területükön meghatározott szolgáltatások – a végfelhasználó **földrajzi elhelyezkedésére való tekintet nélkül** – **meghatározott minőségben és megfizethető áron minden végfelhasználó számára** rendelkezésre álljanak. Az ilyen intézkedések között szerepelhetnek a különleges szociális helyzetű fogyasztókat közvetlenül megcélzó intézkedések, amelyek meghatározott fogyasztóknak támogatást nyújtanak. Az egyetemes szolgáltatás célja, hogy a hatékony verseny és választás révén az EU egészében biztosítsa a jó minőségű, nyilvánosan elérhető szolgáltatások rendelkezésre állását, és szabályozza azokat az eseteket, amikor a végfelhasználók igényeit a piac nem elégíti ki megfelelően. A tagállamok a GATS-egyezménnyel összhangban az egyetemes szolgáltatások nyújtásának garantálása céljából egy vagy több vállalkozást jelölhetnek ki hatékony, tárgyilagos, átlátható és megkülönböztetéstől mentes kijelölési eljárás alkalmazásával, úgy, hogy az állam területének egésze lefedhető legyen. A tagállamok nem kötelesek egyetemes szolgáltatót kijelölni, ha az egyetemes szolgáltatás feltételei egyébként is teljesülnek. Amennyiben megállapítható, hogy valamely vállalkozásra tisztességtelen teher hárul az egyetemes szolgáltatás biztosításának kötelezettsége miatt, akkor az érintett tagállam a kijelölt vállalkozás kérelmére határoz a **veszteségek kompenzálásáról**, amely lehet állami támogatás vagy a költségek valamennyi szolgáltató közötti arányos megosztása.

Piacra lépés szabályozása: Az elektronikus hírközlési szolgáltatások nyújtása – bizonyos kivételekkel (pl. rádiófrekvencia-használati jogok) – csak általános felhatalmazás tárgyát képezheti, ami azt jelenti, hogy az érintett vállalkozástól megkövetelhető, hogy **bejelentést** tegyen tevékenysége megkezdése előtt, de nem írható elő számára, hogy a szabályozó hatóság kifejezett határozatát előzetesen beszerezze. A **rádiófrekvencia- és számhasználati jogokat nyílt, átlátható, megkülönböztetésmentes eljárások** keretében kell megadni. Az elektronikus hírközlési szolgáltatások nyújtói számára **igazgatási díj** fizetése írható elő, a nemzeti szabályozó hatóság felhatalmazási rendszerének fenntartásával és a használati jogok megadásával összefüggő tevékenységek finanszírozása céljából. Az ilyen díjat az említett tevékenységek tényleges igazgatási költségeinek fedezésére kell korlátozni. Az igazgatási díjak mellett a rádiófrekvenciák és számok használatára vonatkozóan **használati díj** is kivethető, az ilyen erőforrások legelőnyösebb felhasználását biztosító eszközként.

*Hatékony frekvenciagazdálkodás***:** A rádiófrekvenciák szűkös, jelentős társadalmi és piaci értékkel bíró közjavak. Közérdek a gazdasági, társadalmi és környezeti értelemben vett lehető leghatékonyabb és legcélravezetőbb spektrumgazdálkodás. A spektrummal való hatékonyabb gazdálkodást mozdítja elő az analógról a digitális földfelszíni televíziózásra történő átállás, amely növeli az értékes spektrum rendelkezésre állását (ez az ún. „**digitális hozadék**"). A tagállamok például a spektrumfelhalmozás megakadályozása érdekében szabályokat írhatnak elő, így különösen **szigorú határidőket** határoznak meg a használati jogoknak a jogosult általi tényleges kihasználására. A tagállamok biztosítják, hogy – a Bizottság vagy az általuk meghatározott sávokban − a vállalkozások egyéni rádiófrekvencia-használati jogaikat más vállalkozásokra átruházhassák, illetve más vállalkozásoknak haszonbérbe adhassák.

5. TECHNOLÓGIA ÉS ROBOTJOG

A fejezet Dr. Tóth András és Dr. Klein Tamás írása.

5.1. Jog és technológia[36]

A technológia és szabályozás gyakran **egymás ellentéteinek tűnnek**, hiszen a technológia a haladást, a szabályozás pedig éppen a haladás gátját, a bürokratizmust testesíti meg.[37] A jog ráadásul a múltban rászolgált a vele kapcsolatos előítéletekre. A múltbeli szabályozási események ugyanis gyakran az emberek változással szembeni fenntartásait, ellenállásait lovagolták meg, és sokszor arra voltak visszavezethetőek, hogy a jog és a jogalkotó nem vállalta fel az új technológiák jelentette kockázatok kezelését. Minderre jó történelmi példa Nürnberg város 1403-as rendelete, amely megtiltotta az acél huzalokat gyártó gépeket és előírta azok megsemmisítését, valamint megeskette az érintetteket, hogy a jövőben nem használnak ilyen gépet, és másokat sem tanítanak meg rá, mondván, a gépek fenyegetik a fennálló társadalmi rendet, a céhes gyártást.[38]

Ugyanakkor el kell ismerni, hogy a mai technológiák hatásait nem lehet összehasonlítani az ipari forradalom által elindított társadalmi változásokkal. Abban nincs különbség, hogy a technológiai változás akkor is és most is emberi munkahelyek tömeges megszűnésével, újak létrejöttével, kulturális értékek megváltozásával járhat (**kreatív rombolás**).[39] A mai technológiai változások ugyanakkor közvetlenül és széles körben érintik a társadalom egészségének életminőségét (pl. szintetikus biológia), életszínvonalát (pl. e-gazdaság) méltóságát (pl. robotok) valamint környezetét (pl. GMO). Ez pedig valóban fokozottabb óvatosságot követelhet meg a jogalkotótól.

A technológiai fejlődés a **joggal szemben kettős elvárást** támaszt: egyrészről a jog szabályainak megerősítésére, a jogalkotási folyamat újragondolására lehet szükség annak érdekében, hogy a technológiai fejlődés ne ássa alá az emberi szabadságjogokat. Másfelől szükséges azonban az is, hogy a jog korlátozza a technológiai fejlődést.

A technológiával kapcsolatos egyik legfőbb probléma a **bizonytalanság**, amelynek kezelésében a jognak megkerülhetetlen szerepe van. Az Európai Parlament (EP) szerint is egy robotokra vonatkozó európai szabályozás segíthet annak tudatosításában, hogy a robotok immár nem a sci-fi világába tartoznak.[40]

---

36 Az alfejezet Dr. Tóth András írása.

37 Jonathan B. Wiener: The regulation of technology, and the technology of regulation, Technology in society 26 (2004) 483.

38 Wolfgang van den Daele: Access to New Technology. In Defense of the Liberal Regime of Innovation, 85., in. Dimension of technology Regulations, eds.: Morag Goodwin, Bert-Jaap Koops, Ronald Leenes, Wolf Legal Publishers, 2010.

39 Romboló innovációnak nevezzük azon új termékeket, folyamatokat és üzleti modelleket, amelyek újradefiniálják a piacokat és felülírják a korábbi meghatározó vállalkozásokat. Gyakran ezek a változások az adott piac vertikumán kívülről érkeznek. OECD Working Party No.2 on Competition and Regulation: Protecting and Promoting Competition in Response to „Disruptive" Innovations in Legal Services, 13 June 2016, DAF/COMP/WP2(2016)1, 4.

40 European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) European Civil Law Rules in Robotics – Study, 6. http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016)571379_EN.pdf 10

A technológiai fejlődésre adott felelős jogi válasz kulcsa egy olyan alapállás, amely a kockázatokat nem pusztán feltételezi, hanem azok létéről meggyőződik (**precaution principle**).[41] Másként megfogalmazva, az új technológia blokkolható addig, amíg nem bizonyosodik be róla, hogy biztonságos.[42] Erre jó példa az az eset, amikor a Pfizer állatoknak szánt antibiotikumát az EU-ban arra való hivatkozással tiltották be, hogy nem lehetett teljes tudományos bizonyosságot nyerni arra vonatkozóan, hogy a szer emberekben nem hoz létre antibiotikum-rezisztenciát.[43] A kockázatbecslésnek tudományos alapokon és nem a közvélemény félelmén kell alapulnia.

Ugyanakkor a társadalomnak is le kell mondani arról az illúzióról, hogy mindenféle technológiai kockázat előre felmérhető és pusztán szabályozással megelőzhető. A vegyipari balesetek megelőző szabályozási doktrínája, az ún. Seveso irányelv alapján is világos, hogy pusztán a múltban bekövetkezett balesetek tanulságai nem óvhatják meg a társadalmat, önmagukban nem garantálhatják a biztonságos jövőt.[44]

A technológiai haladás és a válaszadásra késztetett jog között van egy fontos összefüggés, amely a jogot megfelelő válaszok kialakításában segítheti: a **szabályozás maga is technológia**, a kormányzás technológiája.[45] A technológiai fejlődés szabályozása így nem más, mint a szabályozás technológiájának kérdése. A szabályozásnak is számos technológiája, eszköze van. Ahhoz, hogy a jog a fentiek során a technológiával kapcsolatosan ismertetett kettős kihívásnak megfeleljen (fejlődés segítése, alapjogok védelme), **több eszközt is kombinálnia kell**: jogszabályokat, technikai szabályokat, magatartási szabályokat és a legjobb gyakorlatokat.[46] Ez tudná egyszerre garantálni a rugalmasságot és kiszámíthatóságot.

A jog egyre többször szabályoz tudományos tevékenységeket, illetve azok eredményeit, miközben a jog tényalapú megközelítést alkalmazó és a tudomány sokszor bizonytalan alapállása között feszültség lehet. A technológia és a tudomány azonban nem csak a jogi szabályozás célterületei, de egyúttal eszközei is lehetnek, például **parancsként beépülhetnek a technológiába**, ami a robotok esetében elég kézenfekvőnek is hangzik (lásd Asimov törvényeit).[47] Ez a megközelítés megjelenik például az Európai Parlament és a Tanács 2016/679 rendelet**én**ek 25. cikkében, ami előírja, hogy mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során olyan megfelelő technikai és szervezési intézkedéseket kell végrehatni, amelyek célja egyrészt az adatvédelmi elvek, például az adattakarékosság hatékony megvalósítása, másrészt az e rendeletben foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába. („**privacy by design**”)

A technológia szabályozása kapcsán az időszerűségnek kiemelt jelentősége van, amit jól szemléltet az ún. **Collingridge dilemma**, amely rámutat, hogy egy technológia korai szakaszban való szabályozása korlátozó lehet, ha viszont megvárjuk, amíg egy adott technológia kibontakozik, könnyen

41 Az EU környezetvédelmi politikája a Rio-i Nyilatkozatra való hivatkozással szentesítette ezt az elvet, eszerint amikor komoly és visszafordíthatatlan károkozás veszélye áll fenn, akkor a teljes tudományos bizonyosság hiánya nem lehet az oka a környezetszennyezést megakadályozó költséghatékony intézkedések alkalmazásának. Esther Versluis, Marjolein van Asselt, Tessa Fox, Anique Hommels: Calculable Risks? An Analysis of the European Seveso Regime, in. Dimension of technology Regulations, eds.: Morag Goodwin, Bert-Jaap Koops, Ronald Leenes, Wolf Legal Publishers, 2010., 264.

42 Wiener (2004) i.m. 495.

43 T-13/*99 Pfizer Animal Health kontra Tanács*, EBHT [1999] II-01961 389. és 369. pontok

44 Esther Versluis, Marjolein van Asselt, Tessa Fox, Anique Hommels: Calculable Risks? An Analysis of the European Seveso Regime, in. Dimension of technology Regulations, eds.: Morag Goodwin, Bert-Jaap Koops, Ronald Leenes, Wolf Legal Publishers, 2010., 34.

45 Wiener (2004) i.m. 484.

46 Collaborative project (CP), FP7-SiS-Challenge 1-3: Regulating Emerging Robotic Technologies in Europe: Robotics facing Law and Ethics (Robolaw), www.robolaw.eu, 11

47 Uo.

elveszíthetjük felette a szabályozói kontrollt.[48] Egyébként a technológiai fejlődés irama önmagában gyakran megakadályozza a szabályozót abban, hogy időben beavatkozzon. Másfelől a „**regulatory connection**" elmélet fényében ez nem biztos, hogy probléma: a technológia elhúzódó szabályozása, nyomon követése ad lehetőséget a megfontolt jogi válaszok megtalálásra, főleg, hogy sokszor a technológia csak későbbi fejlődési szakaszában bontakozik ki a szabályozás szempontjából is releváns módon.[49]

5.2. A sharing economy jogi vonatkozásai[50]

Jelen fejezet az olyan online alkalmazások által felvetett jogi problémákat és lehetséges megoldásaikat veszi számba, amelyek összekapcsolják a magántulajdonukat üzleti, kereskedelmi célokra hasznosítókat a lehetséges fogyasztókkal.

Már abban sincs egyetértés a témával foglalkozók között, hogy miként kell nevezni az ilyen online alkalmazásokat. A legismertebb elnevezés – a közösségi gazdaság (sharing economy) – a szolgáltatás jellemzői közül azt emeli ki, hogy az új generáció fogyasztói már **nem a tulajdon mindenhatóságát hirdetik** és nem akarnak mindenre szert tenni, amire szükségük van, megelégszenek a használati eszközökhöz való **hozzáféréssel**, amelyhez viszont hatékony eljárásokra van szükségük.[51] Ezzel szemben többen arra hívják fel a figyelmet, hogy ezen alkalmazások kapcsán nem beszélhetünk klasszikus közösségi használatról. Először is nem a használati eszközök egy időben, többek általi közös használatáról van szó.[52] Másodszor, a felhasználás nem ingyenes: az emberek nem valamiféle közösségi küldetéstudattól vezérelve adják közösségi használatba a magántulajdonukat. Sokkal inkább arról van szó, hogy a magántulajdont üzleti célokra is felhasználják, ezzel megadva a lehetőséget, hogy bárkiből taxisofőr, szakács vagy szálláskiadó legyen.[53] Mindezekre tekintettel közösségi gazdaság helyett (sharing economy) helyesebb a magántulajdon üzleti célú felhasználását elősegítő on-line platformokról beszélni, amelyek összekapcsolják a keresletet és kínálatot.[54] Ezek közös jellemzői az Európai Bizottság szerint:[55]

- új piacokat hoznak létre a régiek kikezdésével, jellemzően **személyes adatok** gyűjtése és felhasználása révén
- **többoldalú** piacok hálózati hatással
- újfajta lehetőséget kínálnak a **vállalkozásra**
- növelik a **választékot** és a fogyasztói jólétet.

---

48 Bert-Jaap Koops: Ten dimensions of technology regulation. Finding your bearings in the research space of an emerging discipline, in. Dimension of technology Regulations, eds.: Morag Goodwin, Bert-Jaap Koops, Ronald Leenes, Wolf Legal Publishers,2010., 317.

49 R. Brownsword and M. Goodwin, Law and the Technologies of the Twenty-First Century. Texts and Materials, Cambridge-New York: Cambridge University Press, 2012

50 Az alfejezet Dr. Tóth András írása.

51 lásd részletesen: Hannah A. Posen (2016): Ridesharing in the Sharing Economy: should Regultarors Impose Über Regulations on Uber? Iowa Law Review, Vol.101:405

52 Damien Geradin: Should Uber be Allowed to Compete in Europe; And if so How? Competition Policy International, June 2015, 3. és Hannah A. Posen, (2016) i. m. 414.

53 Sofia Ranchordás: Does Sharing Mean Caring? Regulating Innovation in the Sharing Economy, Tilburg Law School Legal Studies Research Paper Series No.06/2015, Minnesota Journal of Law Science & Technology, Vol. 16:1, 2015., 43.

54 Benjamin G. Edelman & Damien Geradin: Efficiencies and Regulatory shortcuts: How should we regulate companies like Airbnb and Uber? November 24, 2015., Forthcoming, Stanford Technology Law Review , 1.

55 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Online Platforms and the Digital Single Market, Oppurtunities and Challenges for Europe, COM(2016) 288/2, 2.

A magántulajdon üzleti célú felhasználását elősegítő on-line platformok elterjedését segíti az is, hogy megkönnyítik a vállalkozóvá válást. Az Európai Parlament jelentéstervezete is hangsúlyozza, hogy *„a közösségi gazdaság következtében növekszik a verseny és a fogyasztók **választása**, valamint az **erőforrások**, a készségek és az egyéb eszközök **hatékonyabb felhasználása*** révén lehetőségek nyílnak a munkahelyteremtésre, a gazdasági növekedésre, a versenyképességre, a befogadóbb munkaerőpiacra és a körforgásos uniós gazdaság kialakítására; sürgeti a Bizottságot és a tagállamokat, hogy támogassák a közösségi gazdaság továbbfejlesztését azzal, hogy beazonosítják az ennek útjában álló mesterséges akadályokat és a növekedését gátló vonatkozó jogszabályokat."[56]

A sharing economy vállalatai (pl. Uber, Airbnbn) kapcsán felmerülő szabályozói kihívások valójában nem új keletűek. Ugyanazok, mint amelyekkel az új technológiák úttörői a történelemben korábban bármikor szembesültek, nevezetesen, hogy miként lehet egyszerre biztosítani a technológiai fejlődést és azt, hogy az ne ássa alá a közérdeket, miközben meg kell küzdeni a fennálló rend védelmezőivel, akik gyakran érthetően az állásukat féltik.

Az Európai Parlament jelentéstervezete is ösztönzi a Bizottságot, hogy *„a közösségi gazdaság keretében elemezze, hogy miként lehet **egyensúlyt teremteni** a fogyasztók szerepének növelése és védelme között, valamint – ahol pontosításra van szükség – biztosítsa a digitális szféra fogyasztói vonatkozású jogi keretének megfelelőségét, beleértve az esetleges visszaélésekkel kapcsolatos eseteket is, valamint határozza meg, hogy megfelelőek vagy hatékonyabbak-e az utólagos jogorvoslatok."*[57]

Stigler negyven évvel ezelőtt már leírta a szabályozói foglyulejtettség jellemzőit, amikor a szabályozás előnyeit nem a köz, hanem a szabályozott élvezi, aki megpróbálja a szabályozót a saját érdekei mentén befolyásolni.[58] Így lesznek az egykor fogyasztókat védő szabályokból a status quo védelmi bástyái.[59]

Az, hogy egy technológia új, nem jelenti, hogy nem kell szabályozni, vagy engedni kell, hogy társadalmi veszteségek forrása legyen.[60] Új technológiákra általában új szabályozás kell. Nincs ok arra, hogy a sharing economy vállalatai élvezzék a **szabályozatlanság jelentette versenyelőnyöket**, de arra sincs szükség, hogy a szabályozó csak azért büntesse őket, mert újszerűek és ezáltal kihívásokat támasztanak.[61] Ha új, megfelelő szabályozás hiányában a régi szabályokat alkalmazzuk az új technológiákra, akkor az könnyen az új technológia jelentette előnyök kiiktatásához vezethet.[62] Másfelől viszont vannak horizontális jogi szabályok, amelyeket minden körülmények között tiszteletben kell tartani, ilyenek a személyes adatok kezelésére, adófizetésre, munkajogra, műszaki, biztonsági, közegészségügyi, környezetvédelmi megfelelőségre, a fogyasztóvédelemre vonatkozó előírások. Léteznek aztán a speciális, adott tevékenységre vonatkozó szabályok is, mint például az árszabályozás vagy a taxik számának korlátozása a városi dugók elkerülése érdekében. A szabályozási feszültségek abból fakadhatnak, ha a horizontális jogi elvárásokat az új technológia nem tartja be, a speciális szabályokat pedig a jogalkotó nem szabja az új – egyébként társadalmi előnyökkel járó – technológiára. Például az Uber-sofőröknek és autóknak nem szabad kevésbé biztonságosnak lenniük, mint a hagyományos taxiknak.[63] Szükségesek tehát a speciális, sofőrökre vonatkozó megfelelési szabályok, az autókra vonatkozó biztonsági előírások betartása, a biztosítás megléte.[64]

---

56 Jelentés a digitális egységes piaci intézkedéscsomag megvalósításáról (2015/2147(INI)) 77. pont

57 Uo. 78. pont

58 Georges Stigler: The Theory of Economic Regulation, 2 BELL J. ECON. REG. 3 (1971), and Sam Peltzman, Toward a More General Theory of Regulation, 19 J. L. & ECON. 211 (1976).

59 Posen, Hannah A. (2016), i. m. 425.

60 Geradin, Damien (2015), i. m. 3.

61 Uo.

62 Ranchordás, Sofia (2015) i. m. 59.

63 Geradin, Damien (2015) i. m. 10.

64 Posen, Hannah A. (2016), i. m. 428.

5.3. Fogyasztóvédelem a digitális korban[65]

5.3.1. Szabályozási háttér: a tisztességtelen kereskedelmi gyakorlat tilalma

Mind közgazdaságilag, mint pedig jogilag kiemelt jelentősége van a valós kereskedelmi kommunikációnak. Közgazdaságtanilag a **valós kereskedelmi kommunikáció** lehetővé teszi a fogyasztóknak, hogy a legjobban használják ki erőforrásaikat a számukra árban és minőségben is legmegfelelőbb kínálat megtalálásában. Mindez azt jelenti, hogy a valótlan kereskedelmi kommunikáció csökkenti a fogyasztói jólétet és tisztességtelen versenyelőnyt biztosít a valósan kommunikáló vállalkozásokkal szemben.

Az EU belső piacán az üzleti vállalkozások fogyasztókkal szemben folytatott tisztességtelen kereskedelmi gyakorlatairól szóló irányelv (a továbbiakban: UCP-irányelv)[66] közvetlenül védi a fogyasztó gazdasági érdekeit az üzleti vállalkozásoknak a fogyasztókkal szemben folytatott tisztességtelen kereskedelmi gyakorlataitól. Ezáltal közvetetten védi a jogszerűen eljáró üzleti vállalkozásokat is az ezen irányelvet be nem tartó versenytársaiktól, így biztosítva a tisztességes versenyt az általa összehangolt területeken.

Az online értékesítés aránya az elmúlt időszakban a teljes kereskedelmet meghaladóan jobban nőtt az EU-ban még a 2008-2012 közötti időszakban is, márpedig az interneten vásárlók aránya meghaladja az 50%-ot.[67] Mindezen körülmények között a **torzítatlan fogyasztói döntéshozatal jelentősége az online térben felértékelődik,** miközben a tisztességtelen kereskedelmi gyakorlat tilalmára vonatkozó szabályozást az elektronikus kereskedelemben is megfelelően alkalmazni kell.[68]

A UCP-irányelvet Magyarországon a fogyasztókkal szembeni tisztességtelen kereskedelmi gyakorlat tilalmáról szóló 2008. évi XLVII. törvény (a továbbiakban: Fttv.) implementálja. Az Fttv. tiltja a tisztességtelen kereskedelmi gyakorlatot, különösen a megtévesztéssel vagy elhallgatással megvalósulókat.

5.3.2. Adatvédelem és tájékozott döntéshozatal

Az internet a „minden ingyenes" kultúráját ajánlja.[69] Az interneten működő szolgáltatásplatformok pedig ezen modellt jellemzően a hirdetési piacról tartják fenn. Olyan kétoldalú piac ez, ahol a platform szolgáltatója egyre vonzóbb ingyenes szolgáltatásokat fejleszt annak érdekében, hogy az őket igénybe vevő felhasználók egyre növekvő tábora miatt az ingyenes szolgáltatásokat kínáló platform a reklámozóknak aztán minél vonzóbb legyen (a növekvő felhasználói figyelem miatt). Ebben a közegben a szolgáltatást ingyenesen igénybe vevő felhasználók személyes adata és az adott felületen történő felhasználói aktivitása (amely pl. sütik révén monitorozható) komoly üzleti érték, hiszen az idejükkel és figyelmükkel fizetnek a reklámozóknak, ezt tekintetbe véve beszélhetünk figyelmi piacokról is.[70]

---

65 Az alfejezet Dr. Tóth András írása.

66 Az Európai Parlament és a Tanács 2005/29/EK irányelve (2005. május 11.) a belső piacon az üzleti vállalkozások fogyasztókkal szemben folytatott tisztességtelen kereskedelmi gyakorlatairól, HL L 149.,.2005.6.11., 22. o., 8. preambulum-bekezdés

67 Preliminary Report on the E-commerce Sector Inquiry, Brussels, 15.9.2016 SWD(2016) 312 final, 7. és 9. pontok http://ec.europa.eu/competition/antitrust/sector_inquiry_preliminary_report_en.pdf

68 Federal Trade Commission: .com Disclosures, How to Make Effective Disclosures in digital Advertising, March 2013,

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

70 Lsd. Colangelo, Giuseppe and Maggiolino, Mariateresa, Data Protection in Attention Markets: Protecting Privacy Through Competition? (April 2, 2017). Forthcoming, Journal of European Competition Law & Practice. Available at SSRN: https://ssrn.com/abstract=2945085 or http://dx.doi.org/10.2139/ssrn.2945085

A kereskedő és a fogyasztó közti **információs aszimmetria egyik forrása az online szolgáltatások látszólagos ingyenessége.** Az online szolgáltatások igénybevételekor a felhasználók ritkán vannak azzal tisztában, hogy pontosan milyen adatokat adnak át (viselkedési, helyszín stb.), illetve, hogy azokat mire is használják fel, és milyen további harmadik felekkel osztják meg. Az információs aszimmetriát ugyan csökkenti, hogy az adatalapú online szolgáltatások igénybevételekor a felhasználónak el kell fogadni az adatvédelmi szabályzatot és az általános szerződési feltételeket, ezek azonban gyakran olyan hosszúak és bonyolultan vannak megfogalmazva, hogy a legtöbb fogyasztó számára nehézséget okoz a megértésük vagy sajnálják az időt az elolvasásukra. A fogyasztóvédelemnek (a valóban tájékozott döntéshozatal feltételeinek megteremtése mellett) ki kellene arra is terjednie, hogy korlátok közé szorítsa, hogy a szolgáltatók piaci erejüket kihasználva szabadon gyűjthessenek mindenféle adatokat bármilyen célra.[71] Az OECD szerint ezt az biztosítaná, ha a fogyasztó tisztában lenne azzal, milyen szintű adatátadás pontosan milyen szolgáltatás igénybevételhez szükséges, és ennek fényében ő maga dönthetne az igényeihez igazodva.[72]

Az **adatvédelem szintje a verseny nem árjellegű paramétere lehet**.[73] Miként a termék minősége is.[74] Erre utalnak azok az online vállalkozások, amelyek kifejezetten a magas adatvédelmi szinttel kívánnak versenyelőnyre szert tenni (pl. Snapchat, DuckDuckgo). Bár a Snapchat kapcsán az amerikai Federal Trade Commission (FTC) megállapította, hogy az tévesen állította, hogy az alkalmazásán keresztül küldött video- és képüzenetek a beállított időlimitet követően „örökre eltűnnek", mert ez számos technikai megoldással kijátszható volt.[75] Szintén elmarasztalásra került az Uber, mert megtévesztő módon állította egyrészt, hogy megelőző intézkedésekkel biztosítja, hogy alkalmazottai ne férjenek hozzá az Uber-sofőrök személyes adataihoz, miközben ezt egyáltalán nem monitorozta, másrészt a felhasználók személyes adatait pedig biztonságosan kezeli, amivel kapcsolatban pedig megállapítható volt, hogy az Uber a személyes adatokat felhőben és emelt szintű titkosítási védelem nélkül tárolta.[76] Emiatt 2014 májusában több mint százezer felhasználó adatát szerezték meg hekkerek.

5.3.3. Az információs zaj csökkentésének eszközei

Az online térben már nem az információ hiányával, hanem annak áradatával kell megküzdeni. Ebben az információs zajban segítenek a mindenféle értékelések és vélemények.

A European Consumer Centres' Network által 2013-ban készített webes felmérés eredményei szerint a válaszadók 82%-a olvas online értékeléseket vásárlás előtt.[77] Az online interakciók során ugyanis jellemzően ismeretlen felhasználók és szolgáltatásnyújtók kerülnek egymással kapcsolatba, mely esetben megkönnyíti a tranzakció létrejöttét, ha tudható, hogy a múltban a kiadásra kínált szoba mennyire volt tiszta állapotban (pl. Airbnb), vagy a szolgáltatás/termék kínálója valóban leszállította-e az árut az általa hirdetett minőségben (pl. eBay). A termék- és szolgáltatásértékelések növekvő jelentősége miatt nagy a kísértés, hogy a szolgáltatók ezeket befolyásolják.

---

71 OECD: Big Data: Bringing Competition Policy to the Digital Era DAF/COMP/M(2016)14, 27-Oct-2016, 89. pont https://one.oecd.org/document/DAF/COMP(2016)14/en/pdf

72 Uo., 95. pont

73 Eleonora Ocello, Cristina Sjödin, Anatoly Subočs: What's Up with Merger Control int he Digital Sector? Lessons from the Facebook/whatsApp EU merger case, Competition merger brief, Issue 1/2015 – February, 6.

74 Autorité de la Concurrence – Bundeskartellamt: Competition Law and Data, 10th May, 2016. 3. http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf. 24.

75 https://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were

76 https://www.ftc.gov/news-events/press-releases/2017/08/uber-settles-ftc-allegations-it-made-deceptive-privacy-data

77 Trust marks report 2013, 51. o. http://ec.europa.eu/dgs/health_food-safety/information_sources/docs/trust_mark_report_2013_en.pdf

A UCP-iránymutatás[78] kiemeli, hogy a belső piacon a UCP-irányelv 6. cikk (1) bek. b) pontja és 7. cikk (4) bek. a) pontja értelmében **a felhasználói értékelések** publikálásakor a platform üzemeltetője köteles **valós** információt közölni a szolgáltatásainak lényeges tulajdonságairól. Az értékelések eredete tekintetében a platform nem téveszthetti meg a fogyasztót. A platformnak különösen el kell kerülnie azt, hogy olyan benyomást keltsen, mintha a közzétett értékelések valódi felhasználóktól származnának, amikor annak megfelelő biztosítására nincs lehetősége. Az ausztrál versenyhatóság (ACCC) 2011 novemberében a Citymove nevű vállalkozást azért bírságolta meg, mert a vállalkozás hamis fogyasztói véleményeket tett közzé.[79] Az olasz versenyhatóság pedig azért marasztalta el a TripAdvisor-t, mert bár úgy hirdette magát, mint ahol valós fogyasztói értékelések érhetők el, valójában azokat nem ellenőrizte.[80]

A fogyasztói döntési folyamatra a reklámok és a reklámnak nem minősülő tartalmak eltérő módon képesek hatást gyakorolni, így például adott esetben az elfogulatlannak tűnő, egy adott áru vagy szolgáltatás kedvező tulajdonságait közvetlenül vagy közvetetten ismertető szerkesztői tartalom nagyobb meggyőző erővel bírhat, mint az értékesítésében érdekelt vállalkozás reklámja.[81] Főleg a fiatalok esetében meghatározók a **közösségi média véleményvezérei**, akik esetében különösen fontos, hogy világossá tegyék követőik felé, ha egy véleménynek látszó posztjuk **valójában fizetett tartalom**. Az Fttv. rendelkezéseinek értelmében ezért tilalmazott az olyan, valamely áru értékesítésének vagy más módon történő igénybevételének előmozdítását célzó kereskedelmi gyakorlat, amely annak révén alkalmas a fogyasztói döntési folyamat torzítására, hogy az áru értékesítésében érdekelt vállalkozás által nyújtott ellenszolgáltatásért cserébe az írott vagy elektronikus médiában megjelenő tájékoztatás a vállalkozás által ellenszolgáltatással nem befolyásolt szerkesztői tartalom formáját ölti.[82] A GVH szerint a véleményvezérnek a fennálló üzleti kapcsolattal, közvetlen gazdasági érdekeltséggel összefüggésben *„jól észlelhetően és hangsúlyosan, szembetűnően és egyszerűen, egyértelműen és közérthetően"* szükséges feltüntetnie, hogy a közzétett tartalom fizetett, támogatott tartalom és/vagy annak közzétételéért ellenszolgáltatásban részesült.[83]

5.4. Mesterséges intelligencia és robotjog[84]

5.4.1. Az ember teremtette lényekről alkotott társadalmi felfogások

A robotokról szóló gondolkodás szinte egyidős az emberiséggel, hiszen már az ókori ember is álmodott a neki szolgáló gépekről. A robotokkal kapcsolatos társadalmi felfogás ugyanakkor nem egységes a földgolyó egészét szemlélve. Kulturálisan – mutat rá Tóth András – igen jelentős különbség érzékelhető a nyugati és a keleti társadalmak robotokról vallott értékítélete között. A nyugati világban kulturálisan és történelmileg vitathatatlanul léteznek azok a széles körben ismert negatív **előítéletek**, amelyek abból táplálkoznak, hogy az ember által teremtett lények feletti humán kontrollelvesztését követően a teremtmények alkotójuk és az emberiség ellen fordulnak. Az európai és amerikai társadalmi közegben ezek az előítéletek napjainkban is érzékelhetően jelen

78 http://ec.europa.eu/justice/consumer-marketing/files/ucp_guidance_en.pdf

79 http://www.accc.gov.au/media-release/accc-removalist-admits-publishing-false-testimonials

80 http://www.agcm.it/component/joomdoc/allegati-news/ps9345-eng.pdf/download.html

81 Big data and innovation: Implications for Competition Policy in Canada, draft discussion Paper, 35. o http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/vwapj/Big-Data-e.pdf/$file/Big-Data-e.pdf , 41. o

82 Vj-47/2011

83 #GVH#Megfeleles#Velemenyvezer, 3. pont; http://www.gvh.hu//data/cms1037278/aktualis_hirek_gvh_megfeleles_velemenyvezer_2017_11_20.pdf

84 Az alfejezet Dr. Klein Tamás írása.

vannak. Az elmúlt években többek között Stephen Hawking, Elon Musk, és Bill Gates is felhívták arra figyelmet,[85] hogy a mesterséges intelligenciával rendelkező robotok a nukleáris fegyverkezésnél is nagyobb veszélyeket rejtenek, és komoly fenyegetést jelentenek az emberiségre.[86] Hawking legnagyobb félelme, hogy a mesterséges intelligenciával rendelkező robotok képesek lesznek újratervezni magukat, és behozhatatlan előnyre tehetnek szert az emberrel szemben. Moore törvénye szerint a számítógépek minden másfél évben megduplázzák a sebességüket és memóriájukat. A veszély az, hogy a számítógépek intelligenciát fejlesztenek ki és átveszik az uralmat, mivel az embert fékezi a lassú biológiai evolúció és nem tud versenyezni a mesterséges intelligencia növekedési ütemével. Ehhez képest a keleti társadalmakban, különösen a távol-keleti kultúrákban a robotokkal kapcsolatban ilyen előítéletekkel, félelmekkel nem lehet találkozni. Ennek egyik, szociokulturálisan meghatározott oka az ősi japán vallási tradícióban, a sintoista hagyományban (a szellemek útja) keresendő. A sintoista vallási tanok szerint minden létezőnek, így a robotnak is van lelke. Így a robotokra a keleti társadalmak nem fenyegető veszélyforrásként, hanem mint metafizikai adottságra tekintenek. A távol-keleti jogi szabályozás is ilyen alapon viszonyul a robotikához. A keleti társadalmak rendkívüli innovációvezéreltségén túl ennek az attitűdnek is betudható, hogy Dél-Koreában már 2008-ban jogszabályt fogadtak el a robotok társadalomban betöltött szerepével és működésével kapcsolatos etikai standardokról.[87]

5.4.2. A jogi szabályozás keretei

A negyedik ipari forradalom korában tapasztalt technológiai fejlődés olyan mértékben globális jellegű, hogy nemzetállami szabályozás nem lehet hatékony, ezért a robotokra vonatkozó **jogalkotást szükségszerűen az államoknál magasabb, államközi együttműködésben kell megvalósítani.** Az Európai Unió intézményrendszerét az elmúlt néhány évben intenzíven foglalkoztatja a robotok jogi szabályozásának a kérdése. Az Európai Parlament 2017. február 16-án elfogadott egy állásfoglalást a robotikára vonatkozó polgári jogi szabályokról,[88] amelyben ajánlásokat is megfogalmazott az Európai Bizottság részére, az utóbbi által kidolgozandó uniós irányelv vonatkozásában. Az EP egy jövendő, robotokra vonatkozó európai szabályozás hatásától azt várja, hogy legyen képes tudatosítani, hogy az intelligens robot már nem a sci-fi világába tartozó absztrakt kérdés, másfelől elismeri, hogy már a szabályozás ténye is megerősítheti a nyugati előítéletekből származó félelmeket.[89]

A szabályozásnak szembe kell néznie a robotika összetettségével és szerteágazó társadalmi, gyógyászati és bioetikai hatásaival összhangban lévő, irányadó etikai elvekkel is. Mivel az **utánkövető szabályozás**sal szembeni elvárások jelentősek, így a jogalkotónak rendkívül adaptív módon, gyors reakcióidővel kell reagálnia a technológiai fejleményekből fakadó társadalmi szabályozási szükségletekre.

---

85 Michael Sainato, "Stephen Hawking, Elon Musk, and Bill Gates Warn About Artificial Intelligence", Observer [online], 19 August 2015, http://observer.com/2015/08/stephen-hawking-elon-musk-and-bill-gates-warn- about-artificial-intelligence/

86 vö. An Open Letter to the UnitedNations Convention on Certain Conventional Weapons, https://www.dropbox.com/s/g4ijcaqq6ivq19d/2017%20Open%20Letter%20to%20the%20United%20Nations%20Convention%20on%20Certain%20Conventional%20Weapons.pdf?dl=0

87 vö. Klein Tamás – Tóth András: A robotika egyes szabályozási kérdései, In. Egyes modern technológiák etikai, jogi és szabályozási kihívásai, KRE ÁJK, Budapest, 2018.

88 P8_TA(2017)0051 A robotikára vonatkozó polgári jogi szabályok, Az Európai Parlament 2017. február 16-i állásfoglalása a Bizottságnak szóló ajánlásokkal a robotikára vonatkozó polgári jogi szabályokról (2015/2103(INL)) [továbbiakban EP Állásfoglalás].

89 European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) European Civil Law Rules in Robotics – Study, 6. [továbbiakban: EP Study] 10. http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016)571379_EN.pdf

A jogi szabályozáson túl, de bizonyos esetekben annak részeként, a robotok fejlesztéséhez, tervezéséhez, gyártásához, használatához és módosításához egyértelmű, szigorú etikai keretre is szükség lesz. Az etikai elvek és parancsok jogiasítása különösen azért bír nagy jelentőséggel, mivel az egyes morális alapú etikai előírásoknak hézagpótló szerepük lehet.

5.4.3. A szabályozás alapvető elvei

A robotokra vonatkozó jogi szabályzás legalapvetőbb elveit, a robotika alapvető törvényeit Isaac Asimov fektetett le 1943-ban, a *Runaround* (Körbe-körbe) című novellájában. Asimov törvényei olyan tételeket, parancsokat állapítanak meg, amelyek garantálják, hogy a robotok mindenkor az emberiség érdekében működjenek. A **robotika alapvető** törvényei az alábbi pontokban foglalhatók össze:

1. A robotnak nem szabad kárt okoznia emberi lényben, vagy tétlenül tűrnie, hogy emberi lény bármilyen kárt szenvedjen.

2. A robot engedelmeskedni tartozik az emberi lények utasításainak, kivéve, ha ezek az utasítások az első törvény előírásaiba ütköznének.

3. A robot tartozik saját védelméről gondoskodni, amennyiben ez nem ütközik az első vagy második törvény bármelyikének előírásaiba.

Később Asimov a három törvényt még kiegészítette egy nulladik paranccsal, amelynek értelmében a robotnak minden áron meg kell védenie az emberiséget (akár az első törvény megszegésének árán is).

Asimov törvényei alapján (is) – hívja fel a figyelmet Tóth András - **meg kell különböztetni a robotetikát a gépek etikájától vagy másként robotjogtól:** előbbi a robotok tervezőire, gyártóira, működtetőire vonatkozik, utóbbi pedig magukra a robotokra.[90] Miután még az autonóm robotok sem képesek egyelőre morális döntésekre, így a gépi etika (robotjog) egyelőre hipotetikus kérdés. Asimov törvényei a robotokra vonatkoznak, de tekintettel erre azokat a robotok tervezőire, gyártóira kell adaptálni.[91] Az Európai Parlament is ezt a felfogást erősíti ajánlásában, amikor a szabályozás általános elvei között rögzíti, hogy Asimov törvényeit úgy kell tekinteni, hogy címzettjeik a robotok – többek között az önrendelkezéssel és az autodidakta tanulás lehetőségével felruházott robotok – tervezői, gyártói és üzemeltetői, mivel ezek a törvények nem alakíthatók át gépi kóddá.[92]

5.4.4. A robotfogalom meghatározásának fontossága

A *robot* kifejezést modern értelemben először Karel Čapek cseh író használta az 1920-ban megjelent R. U. R. (*Rossumovi univerzální roboti* vagy angolul *Rossum's Universal Robots*) című science fiction drámájában. A nyugati előítéletes felfogást tükröző műben a tömeggyártásban megalkotott, modern kori rabszolgaként foglalkoztatott robotok öntudatra ébrednek, fellázadnak rabszolgatartóik ellen, és kipusztítják az emberiséget.

A robot fogalmának meghatározása, hogy mi a robot *jogi értelemben*, a jogi gondolkodás és szabályozás egyik legelemibb feladata, hiszen a szabályozás tárgyi hatályának meghatározása so-

90 Klein – Tóth (2018), i. m.
91 vö. Klein – Tóth (2018) i. m.
92 EP Állásfoglalás T. pont.

rán elengedhetetlen a pontos fogalmi lehatárolás elvégzése, a fogalmi elemek egzakt azonosítása. Ugyanakkor mind a mai napig nem született meg egy egységes, nemzetközi szinten elfogadott, jogilag releváns robotfogalom. A különböző fogalomalkotások közös metszete, hogy a robot egy olyan felépített rendszer, amely mind fizikai, mind „szellemi" tevékenységet mutat, de biológiai értelemben nem él.[93]

Az Európai Unió vonatkozó állásfoglalásában felszólítja a Bizottságot, hogy tegyen javaslatot az intelligens autonóm robotok közös uniós fogalommeghatározásaira, oly módon, hogy a fogalomban az intelligens robotok alábbi jellemzői szerepeljenek:

- **autonómia elérése** érzékelők révén és/vagy a környezettel folytatott adatcsere (összekapcsolhatóság), illetve ezen adatok cseréje és elemzése révén;
- önálló tanulás tapasztalás és interakció útján (opcionális kritérium);
- legalább kisméretű **fizikai megjelenés**;
- magatartásának és cselekedeteinek környezethez történő igazítása (**adaptációs képesség külső ingerek alapján**);
- a **biológiai értelemben vett élet hiánya**.[94]

5.4.5. A robot-jogalanyiság problematikája – a „Robo Sapiens" jogállásának kérdőjelei

A robotok döntéshozatalának egyre fokozódó autonómiája aktuálissá teszi a robot-jogalanyiság kérdésének felvetését, vagyis azt a jogilag lényeges problémát, hogy lehet-e robot jogviszonyok (jogilag releváns társadalmi viszonyok) alanya, **lehetnek-e jogai, terhelhetik-e kötelezettségek**?

Amíg a robot csupán emberi parancsok végrehajtásának technikai eszköze, a jogalanyiság kérdése nem időszerű, ám ha a robotok képesek lesznek autonóm döntések meghozatalára, az instrumentalitás érve nem lesz tartható, és a jogilag releváns státusz problematikája sem kerülhető meg. A valódi kérdés tehát a robot által meghozható döntésnek a minősége, az tudniillik, hogy egy előre meghatározott (programozott) szabályrendszer alapján hozza meg a döntését, vagy azt a mesterséges intelligenciára támaszkodva újraértelmezheti.

5.4.5.1. A jogalanyiság tartalmi összetevőinek bizonytalansága

A zsidó-keresztény etikai megalapozású nyugati társadalmak antropológiai felfogásával, világképével nehezen békíthető össze a robotoktermészetes személyhez, az emberhez hasonló *személyiségének* az elismerése. Ugyanakkor az sem problémamentes, ha analógiaként a jogi személyek jogalanyiságát alkalmazzuk a robotok jogi státuszára. Az embertől különböző, jog által elismert jogalanyiság emberek által létrehozott és **az ember tevőleges közreműködésével működni képes szervezeteket** illet meg, ezzel szemben a robot, amennyiben **emberi közrehatás nélkül** „cselekszik," és jogi személyiséggel ruházzuk fel, a jog támogatásával mintegy **az ember konkurensévé válhat**.

A progresszív felfogás[95] olyan *dolognak* kíván jogalanyiságot kölcsönözni, amelynek elismerése a technológiai fejlődés pillanatnyi szintjét tekintve a *közeljövőben* még **nem időszerű**. A jogalanyi-

[93] vö. Neil M. Richards – William D. Smart: How should the law think about robots?, In. Ryan Calo – A. Michael Froomkin – Ian Kerr Robot Law, Edward Elgar Publishing, Cheltenham, UK – Northampton (USA), 2016. 6.

[94] EP Állásfoglalás 1. pont.

[95] vö. Zara Orsolya: Robo Sapiens, avagy személy lesz-e a robot? Aktuális jogi és szabályozási kérdések az Európai Parlamentben, In. Európai Jog, 2016/3, 48-51.

ságot a modern, római jogi gyökerű magánjogi elmélet két jogképességgel felruházott alakzat részére tartja fenn: a jogképességgel felruházott személyegyesülések és vagyontömegek részére, amelyek érvényes jognyilatkozatokat kizárólag (cselekvőképes) törvényes képviselőik útján tehetnek. Ezeknek a jogalanyoknak a „személyisége" fikciós alapú ugyan, mégis a valóságban működésük során mögöttük egy emberi szándék, akarat áll, és ez az akarat, ami végső soron – Moór Gyula elméletét kölcsönözve[96] – betudható a jogi személynek.[97] Egy számítógépes program által vezérelt mesterséges intelligencia azonban sem személyösszességnek, sem vagyontömegnek nem tekinthető.

A jogalanyiság hatályos felfogásában a robot leginkább a vagyonösszeghez, mint jogi személy formához áll a legközelebb. A vagyonösszesség azonban végső soron az ember(ek egy csoportjának) akaratelhatározása, döntései alapján jár el, vagyis jognyilatkozatai beszámíthatók egy embernek, vagy embereknek. A dogmatikai tradíció mögött tehát minden esetben egy emberi cselekvés áll, a jog által létrehozott jogalany mindig emberi ellenőrzés, kontroll alatt áll (ami természetesen nem jelenti azt, hogy ez az emberi közrehatás mögöttes felelősséget is létrehoz). Mindez egy autonóm döntés meghozatalára képes robot esetében már közel sincs így.

A robot, még akkor is, ha önálló döntés(ek) meghozatalára képes, lényegében az általa megismert, a működését biztosító programban megírt szabályoknak megfelelő döntést hoz. A robot alapvetően *contra legem* döntést nem hoz(hat). Nincsen érzelmi viszonyulása a külső valósághoz, az algoritmusában meghatározottak szerint ad egyes konkrét szituációkra releváns választ.[98]

Az intelligens robotok jogalanyiságának elismerése esetén, mint jogilag releváns entitásnak jogai és kötelezettségei lehetnek, azzal a feltétlen megszorítással, hogy csak olyanok, amelyek természetüknél fogva nem kizárólag az embert illethetik meg, vagy terhelhetik. A jogalanyiság terjedelmének további megszorítása pedig a jogalkotó belátásán alapul, azzal, hogy e jogalanyiságnak nincsen érinthetetlen, mindenki más rendelkezése alól kivont magja.

5.4.5.2. Az Európai Parlament jogalanyisággal kapcsolatos felfogása

Egy jövőben megalkotandó *robot-személyiség* jogi konstrukciójának kidolgozását az Európai Parlament szükségesnek tartja és annak csak módját teszi mérlegelés tárgyává.[99] A jogalanyiság konkrétumai kapcsán olyan szabályozás megalkotását sürgeti, amelyben „a robotok specifikus jogalanyiságának létrehozatala hosszú távon, oly módon [valósul meg], hogy **legalább a legkifinomultabb autonóm robotokat sajátos jogokkal és kötelezettségekkel** – többek között az általuk esetlegesen okozott kár jóvátételére vonatkozó kötelezettségekkel – **rendelkező elektronikus személynek lehessen minősíteni**, lehetőleg az elektronikus személyiséget azokban az esetekben alkalmazva, amikor a robotok önálló döntéseket hoznak, vagy más módon, önállóan kerülnek kölcsönös kapcsolatba harmadik felekkel."[100]

A jogalanyiság kérdését tehát az Európai Parlament helyesen azokra az esetekre szűkítené, amelyekben a robot valóban önálló, humán inputtól nem befolyásolt, független döntést hoz. Ezzel együtt

---

96 „A jogi személy nem más, mint meghatározott emberi cselekvések jog által kijelölt beszámítási pontja" vö. Moór Gyula, A jogi személyek elmélete, Budapest, 1931. 317, 320, 341, 351.

97 Anélkül, hogy a jogelmélet mély elemzéseit részletesen bemutatnánk, megjegyezzük, hogy a jogi személyek jogalanyiságát elméletileg megalapozó elméletek (fikciós elmélet, realitáselmélet stb.) egyöntetűen megjelenítik a jogi személyek mögötti emberi cselekvést, akaratot.

98 Az EP tanulmánya is foglalkozik a robot érzelemnyilvánításának problémájával, és felhívja a figyelmet a robotok jelentette érzelmi manipuláció veszélyeire, amire a robotok tervezői rá is játszhatnak, például, amikor gyermekarcot készítenek az emberi kinézetű robotoknak. Lényeges azonban annak tudatosítása, hogy a robotok által emberekből kiváltott érzelmek a robot részéről mesterséges empátiából indulnak ki, vagyis nem valódi emóciókon alapulnak. vö. EP Study 23.

99 Megjegyezzük, hogy valamilyen jogilag releváns státusz kidolgozását mi sem tartjuk lehetetlennek, ám azt – fentebb röviden összefoglalt érvelésünkre tekintettel – robot-személyiségnek hívni elhibázottnak tartjuk. A szigorú keretek között tartott, elsősorban kárfelelősségi alapon megfogalmazott sajátságos, korlátozott és célhoz kötött jogalanyiság megfontolását azonban nem utasítjuk el.

100 EP Állásfoglalás 59. f.) pont.

is a jogalanyiság tartalmi meghatározásán túl jelentősége van a robot-jogalanyiság etikai megfontolásokat sem nélkülöző, jogi megnevezésének is. Az EP egy új jogalanytípus, az *elektronikus személy* bevezetését javasolja.

5.4.6. A robot cselekvőképességének kérdése

A cselekvőképesség a jogtudomány érvényes paradigmája szerint az embernek (és csakis az embernek) az a(z absztrakt) képessége, hogy saját jognyilatkozatai által jogokat és kötelezettségeket tud szerezni magának vagy másoknak. A cselekvőképesség jogi kategóriájában szó szerint szerepel, hogy az a cselekvésre való képesség, amelynek mozgatója az emberi tudat és a tudati cselekvés révén kialakuló akarat.

A robot bármilyen mesterséges tudattal is rendelkezzen, alternatívák közüli választása, döntése során nem (szabad akaraton alapuló) akaratelhatározást valósít meg, hanem egy előre meghatározott algoritmusnak megfelelően konkrét szituációra ad (kötött, előre determinált) választ. A robot, amely önálló döntés meghozatalára képes, lényegében az általa megismert szabályoknak megfelelő döntést hozza meg, és mivel működésének alapja a programozott szabály, ezért alapvetően *contra legem* döntés meghozatalára nem képes (és a szabályozásnak garantálnia kell, hogy ilyen döntést nem is hozhat!). Nincsen érzelmi viszonyulása a külső valósághoz, az algoritmusában meghatározottak szerint ad egyes konkrét szituációkra racionális és nem emocionális választ.

A robot nem magatartást tanúsít, hiszen annak legelemibb jellegzetessége az akaratelhatározás képessége. A jogi szabályozásnak olyan imperatív parancsot kell alkotni, és azt a programozónak kötelessége a robot programjába vésni, amely a tudományos haladás eredményeinek ellenére is megtiltja az előre szabott magatartási szabályoktól való autonóm eltérés lehetőségét, vagyis, hogy a robot felülírja a számára programban meghatározott parancsokat. A jog – az emberiség érdekében – kizárólag ebben a rendszerben képes ellenőrzése alatt tartani a technológiát.

5.4.7. A robotjogi deliktuális felelősség dilemmái

A robotokkal és a robotok által okozott károkért való felelősség szabályozása talán a legsürgetőbb, megoldásra váró szabályozási kérdés. A robotokkal okozott kár esetében a robot csupán a károkozás eszköze, és nem megvalósítója (még akkor sem, ha a kárt közvetlenül a robot tevékenysége okozza), szemben a robotok által okozott károkkal, amelyek a robot saját autonóm döntésének, döntései sorozatának folyományaként következnek be.

A robotokkal, a robotok felhasználásával okozott károkért való felelősség érdemben nem különbözik egy állat, vagy tárgyi eszköz, esetleg cselekvőképtelen ember segítségével megvalósított károkozásért viselt felelősségtől, hiszen ebben az esetben is az a személy felelős, aki saját érdekében a robotot, mint eszközt felhasználta, akinek „gondozása” alatt áll, tkp. akinek az utasítását végrehajtotta.

Abban az esetben azonban, amikor a robot már nem egy ember közvetlen utasítását hajtja végre, hanem önálló döntést hoz, a kérdés már nem ennyire egyszerű. A felelősség megállapíthatósága, a felelős személy azonosítása annál összetettebb, minél nagyobb autonómiával rendelkezik a robot: minél szélesebb körben rendelkezik autonóm döntési szabadsággal, vagyis azzal a képességgel, hogy maga hozzon saját döntéseket, annál kevésbé tekinthető egyszerű eszköznek.

A robot döntéseinek megítélése szempontjából a jognak arra kell választ kínálni, hogy a robot tevékenységének eredményeként bekövetkező kárért kinek kell viselni a jogi felelősséget.

Az Európai Parlament állásfoglalásában kiemelten foglalkozik a felelősség kérdésével, hiszen „úgy véli, hogy a robotok által okozott károk iránti polgári jogi felelősség fontos kérdés, amelyet uni-

ós szinten kell kezelni a hatékonyság, az átláthatóság, a következetesség, a megvalósítás és a jogbiztonság azonos mértékének biztosítása érdekében az egész Európai Unióban, a polgárok, a fogyasztók és a vállalkozások javát egyaránt szolgálva."[101] Ezért az Európai Parlament kifejezetten sürgette a felelősségi szabályok megalkotását. A szabályozásnak két alapvető, kölcsönös függőségen alapuló feltételt szükségszerűen érvényesítenie kell: nevezetesen a kiszámíthatóságot és az irányíthatóságot, vagyis a kontroll alatt tartás feltétlen megvalósulását.

Az EP, habár nem határoz meg ajánlásában konkrét felelősségi alakzatokat, szabályokat, néhány elvi jelentőségű megállapítást megfogalmaz. Talán a legfontosabb követelményként rögzíti a dokumentum a felelősség limitálásának a tilalmát, vagyis azt a szabályozási elvárást, miszerint „bármilyen jogi megoldást [választ a jogalkotó] a robotok által okozott károk iránti felelősségre vonatkozóan a vagyoni károktól eltérő esetekben, a jövőbeni jogalkotási aktus semmilyen körülmények között nem korlátozhatja a megtéríthető károk típusát és mértékét, illetve nem korlátozhatja a károsultnak felkínálható kártérítés formáit pusztán azon az alapon, hogy a kárt nem emberi lény okozta."[102]

Miután a felek azonosítása megtörtént, a következő eldöntendő kérdés a felelősség telepítésének módja és mértéke. Az EP elvi éllel rögzítette azt az elvárást, hogy „a felelősségüknek arányosnak kell lennie a robotnak adott utasítások tényleges szintjével és a robot önállóságával, így minél nagyobb a robot tanulási képessége vagy önállósága, annál kisebbnek kell lennie a többi fél felelősségének, és minél hosszabb ideig tartott a robot „oktatása", annál nagyobb az „oktató" felelőssége." Ezzel összefüggésben az EP hangsúlyozta, hogy „amikor azonosítani kívánjuk azt a személyt, akinek a robot károkozó magatartása ténylegesen tulajdonítható, a robot „betanításból" származó készségei nem keverendők össze a szigorúan az önálló tanulási képességeitől függő készségekkel."[103]

A jelenlegi átmeneti időszakban, amíg a szabályozás nem lesz megnyugtató, az Európai Parlament szükségesnek látja egy temporális kikötés alkalmazását, amelynek értelmében legalább a jelenlegi szakaszban az embereknek és nem a robotoknak kell a felelősséget viselniük.

A bonyolult felelősségi viszonyok egy esetleges megoldásaként tekint az Európai Parlament állásfoglalása egy sajátságos, a robotok által okozott károk megtérítésére létrehozott kötelező biztosítási rendszer intézményesítésére. Egy ilyen kötelező felelősségbiztosítási rendszernek reflektálnia kellene a robotika sajátosságaira, vagyis a gépjárművek esetében alkalmazott rendszerrel szemben, „ahol a biztosítás az emberi cselekedetekre és hibákra terjed ki, a robotikára vonatkozó biztosítási rendszernek a láncolat összes lehetséges felelősségi körét figyelembe kell vennie."[104] Ezt a kötelező robot-felelősségbiztosítást az EP állásfoglalása szerint ajánlatos lenne megtámogatni egy „kockázati" pénzalappal, amely azt a célt szolgálná, hogy az olyan káreseményeknél is legyen lehetőség a kár megtérítésére, amelyeknél nem áll rendelkezésre a szükséges mértékű biztosítási fedezet. Ennek érdekében az EP felszólította a biztosítási szektort, hogy alakítsanak ki olyan biztosítási termékeket, amelyek kifejezetten tekintettel vannak a robotika jelentette kihívásokra.[105]

Mivel a robotok gyártói, üzembentartói által kötött felelősségbiztosítás fedezné a robot által okozott károkat, így felelősségük korlátozott lehet, amennyiben befizetnek egy kompenzációs alapba.[106] Az EP a robotok károkozása esetére kialakítandó felelősségi rendszer tartalmának vizsgálata során a Bizottság mélyreható elemzésére bízza annak megállapítását, hogy az objektív felelősséggel vagy a kockázatkezeléssel kapcsolatos megközelítést kell-e alkalmazni.[107] Az objektív felelősség csak annak bizonyítását teszi szükségessé, hogy kár keletkezett, és hogy kauzalitás áll fenn a robot károkozó

[101] EP Állásfoglalás 49. pont.
[102] EP Állásfoglalás 52. pont.
[103] EP Állásfoglalás 56. pont.
[104] EP Állásfoglalás 57. pont.
[105] uo.
[106] vö. az EP törekvésével: „lehetővé tenni, hogy a gyártó, a programozó, a tulajdonos vagy a felhasználó a korlátolt felelősség előnyeit élvezhesse, amennyiben befizetnek egy kompenzációs alapba, illetve közös biztosítást kötnek a robotok okozta károk esetében nyújtandó kártérítés garantálás érdekében" – EP Állásfoglalás 59. c.) pont.
[107] EP Állásfoglalás 53. pont.

működése, illetve a károsult által elszenvedett kár között.[108] Ugyanakkor a kockázatkezeléssel kapcsolatos felelősségi koncepcióval összefüggésben arra is rá kell mutatni, hogy az nem a „gondatlanul eljáró" személyre, mint egyéni felelősre összpontosít, hanem arra a személyre, aki bizonyos körülmények között képes a kockázatokat minimálisra csökkenteni és kezelni a negatív hatásokat.[109]

A minden szempontból megfelelő, a terheket ideálisan telepítő felelősségi rendszer megalkotása rendkívüli felelősséget ró a jogalkotóra. A boldog, békés egyensúlyi állapotot, az érdekek összebékítését megvalósítani képes felelősségi modell megalkotása a robotokat érintő jogi szabályozás egyik legfontosabb feladata. Első lépésben azonban úgy véljük – az EP álláspontját osztva –, a napjainkban már fenyegető károk megfelelő kezelése érdekében átmenetileg még az embereknek és nem a robotoknak kell a felelősséget viselniük, azzal, hogy ez nem járhat szükségtelenül dermesztő hatással a technológiai fejlődésre.

5.4.8. Robotikai Charta – Az EP javaslata a robotika etikai magatartási kódexére

Az Európai Parlament egy olyan etikai kódex elfogadására tesz javaslatot, amely rögzítené az azonosítás, a felügyelet és az alapvető etikai elveknek való megfelelés alapjait. Ezeket az elveket a robotokra irányuló valamennyi emberi magatartásra kiterjesztené, a tervezési és fejlesztési fázistól kezdve.

A kódex nem helyettesítheti a robotika területén szükséges jogi szabályozást, csupán kiegészítő funkcióval kell rendelkeznie. Elsősorban a robotika etikai minősítését segítené elő, és megerősíti a felelős innovációs erőfeszítéseket ezen a területen. Egy ilyen etikai kódex további, jogon túli funkciója lehet a nyilvánosság aggodalmaira való válaszadás.

A magatartási kódex felszólít minden kutatót és tervezőt, hogy felelős módon cselekedjen, és teljes mértékben vegye figyelembe az emberi méltóság, magánélet és biztonság tiszteletben tartásának szükségességét. A magatartási kódex minden tudományág szoros együttműködését kéri annak biztosítása érdekében, hogy az Európai Unióban a robotikai kutatás biztonságos, etikus és hatékony módon valósuljon meg.[110]

5.4.9. Egyes robotizált technológiák kihívásai

A robotok alkalmazása a legkülönbözőbb társadalmi szektorokban ígér jelentékeny átalakulást. Tanulmányunkban csupán röviden utalunk két olyan felhasználási területre, ahol a robotok széleskörű alkalmazása már napjainkban is megvalósult. Az önvezető gépjárművek első generációi már a közutakon közlekednek, igaz, még nem használhatják valamennyi rendelkezésükre álló automatizált rendszerüket. Hasonlóan intenzív robotizációnak lehetünk tanúi, ha az egészségügyi szolgáltatások modern technológiáit vesszük szemügyre, mind a beteggondozás, mind pedig az emberi testbe épített intelligens eszközök területén.

5.4.9.1. Az önvezető járművek egyes felelősségi kérdései

Talán nem tévedés, hogy az autóiparnak van a legnagyobb szüksége hatékony uniós és globális szabályokra az automatizált és önjáró járművek határokon átnyúló fejlesztésének biztosítása érdekében. Fontos a bennük rejlő gazdasági lehetőségek teljes körű kiaknázása és a technológiai trendek pozitív

[108] EP Állásfoglalás 54 pont.
[109] EP Állásfoglalás 55 pont.
[110] EP Állásfoglalás, Etikai magatartási kódex robotikai mérnökök számára, Preambulum.

hatásainak kihasználása; hangsúlyozva, hogy a széttagolt szabályozási megközelítések akadályoznák az autonóm szállítási rendszerek létrehozását és veszélyeztetnék Európa versenyképességét.[111] Ugyanakkor az autonóm közlekedési eszközök tekintetében a polgári jogi felelősségi kérdéseken túl már most azonosíthatóak újabb szabályozandó, várhatóan nagy társadalmi fontosságú jogterületek: pl. közúti biztonság, környezeti hatás, adatvédelmi kockázatok, IKT-infrastruktúra fejlesztése, foglalkoztatási, munkaerőpiaci kihívások.

Az autonóm közlekedési eszközök, amelyek kiváltják az emberi közreműködést a közlekedési folyamatokban, forradalmasítani fogják az egyéni és a tömegközlekedést egyaránt. A rendszer számos előnye mellett, amely hatalmas gazdasági potenciált rejt, még komoly nehézségekkel kell megküzdeniük az innovátoroknak, hogy piacképessé és tömegesen alkalmazottá tegyék a technológiát. A technológia tömeges alkalmazásáig még alapvető, és napjainkban még meg nem válaszolt kérdéseknek kell eldőlnie, mint például, hogy a több technológiai fejlesztés közül végül melyik lesz általánosan alkalmazott.

A légiforgalomban működtetett robotok előképei a napjainkban is reptetett drónok, amelyek még nem autonóm közlekedési eszközök, hiszen mindig szigorúan emberi irányítás alatt állnak. A jövőben azonban a közúti közlekedéshez hasonlóan meg fog jelenni az igény a drónokkal végzett önműködő légi szállítmányozás iránt is.

5.4.9.2. Robotok a beteggondozásban és a gyógyításban

Az időskorúak, a fogyatékkal élők és a demenciában, kognitív zavarokban vagy az emlékezet hanyatlásában szenvedők gondozásában, ápolásában az utóbbi évtizedben a személygondozó robotokkal jelentős áttörést értek el, különösen a megelőzés, segítségnyújtás, nyomon követés, stimuláció és társaságot biztosító technológiák széles körű alkalmazása révén.

Az **emberi gondozás** egyik alapvető szempontja az emberi kapcsolat. Az emberi tényező robotokkal történő teljes körű helyettesítése személytelenné teheti a gondozási feladatok ellátását, ugyanakkor a robotok képesek lehetnek segíteni az automatizálható gondozási feladatok ellátásában, és megkönnyíthetik a gondozók munkáját, miközben a felszabaduló humán erőforrás révén az emberi törődés fokozható, a rehabilitációs folyamat pedig célirányosabbá tehető lenne. Az orvosok és gondozók diagnosztizálásra, illetve jobban megtervezett gyógyítási opciókra fordítható ideje nőne. Noha a robotika potenciállal bír a fogyatékossággal élő személyek és az időskorúak mobilitásának és integrációjának növelésére, mindig szükség lesz emberi gondozókra, akik továbbra is a szociális érintkezés fontos, nem helyettesíthető forrását biztosítják ügyfeleik számára.

A gondozáson túl az **orvoslás**ban is nagy szerepe lehet a gyógyító robotoknak, amelyek a nagy pontossággal végzett sebészeti beavatkozások és az ismétlődő eljárások végrehajtása terén juthatnak szerephez.

Az emberi test „megjavítására” is egyre több módon használhatók a robotika eredményei, különös tekintettel a sérült emberi szervek, elveszett fizikai funkciók javítása és pótlása terén. Azt azonban hangsúlyoznunk kell, hogy az orvoslásnak ez a területe veti fel a legtöbb bioetikai kérdést, mint például az „embertökéletesítés” kínálkozó lehetőségét.

A kiberfizikai rendszerek (CPS) alkalmazása alapvetően változtatja meg az egészséges emberi testről alkotott fogalmainkat, az „elromlott”, funkcióját vesztő emberi szervek, testrészek reparálását, működésük stimulálását szolgálják, ám egyúttal rendkívül bonyolult (bio)etikai kérdéseket hoznak felszínre. Az emberi testbe beépített CPS-ek különleges, az emberi egészségre, a testi integritásra kiterjedő kockázatokat generálnak, például, ha rendszerüket feltörik, kikapcsolják vagy memóriájukat törlik. Mivel ez veszélyeztetheti az emberi egészséget, rendkívüli esetben az emberi életet is, ennélfogva hangsúlyozzuk, hogy e rendszerek védelmét kiemelten kell kezelni.[112] Ezekhez az új eljárások-

[111] EP Állásfoglalás 25. pont.

[112] vö. EP Állásfoglalás 36-40. pontok.

hoz továbbá egyenlő hozzáférési esélyt kell biztosítani. Természetesen ez a követelmény mind a hét és félmilliárd ember vonatkozásában nem lenne reális, ám úgy véljük, az uniós alapvető értékekből parancsolóan következik, hogy az Európai Unióban való megvalósítás érdekében hatékony intézkedéseket kell tenni.

6. CYBERJOG

Dr. Klein Tamás és Dr. Tóth András írása.

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.[113] A kibertér (mint kiemelt gazdasági és társadalmi folyamat) **fejlődésének és működésnek kulcsa a bizalom** fenntartása, amelynek kulcsa a biztonság. A kibertér biztonságára három egymást kiegészítő szabályrendszer vonatkozik: (i) **bűncselekményi** tilalmak, (ii) a hálózati vagy információs rendszerek **ellenállási képességének** a fejlesztésére vonatkozó előírások, valamint (iii) az **adatbiztonsági**, adatvédelmi előírások.

6.1. Cybercrime (cyberbűnözés)[114]

Az internet technológiája két vonatkozásban is hatással van a büntetőjog fejlődésére. Nem csupán új bűncselekmények jelentek meg, hanem új teret adott a már létező és a büntetőjog által fenyegetett cselekményeknek is. Az online térben számos új(szerű) deviáns magatartás jelent meg, olyanok is, amelyek a társadalom egy korábbi technológiai fejlettségi szintjén a szükséges informatikai háttér hiányában nem létezhettek, és olyanok is, amelyek más formában, de jelen voltak a társadalomban. 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, az önkéntes jogkövetés esetleges, a felhasználói tudatosság miatt pedig a sértetté válás esélye igen nagy. Napjaink cyberbűnözéssel kapcsolatos diskurzusát alapvetően meghatározzák ezek a szempontok.

6.1.1. Egyes cyberbűncselekmény-típusok

6.1.1.1. Cyberbullying (elektronikus v. internetes zaklatás, megfélemlítés)

A kiberbűncselekmények meghatározó része a közösségi hálózatokon valósul meg, 2008-ban a Biztonságosabb Internetért Fórum keretében az Európai Bizottság által végeztetett **felmérésből kiderül, hogy a közösségi oldalak használatakor a kiskorúakat a magánélet megsértése és a szexuális célú megkörnyékezés (grooming) veszélye mellett leginkább az internetes zaklatás**

[113] 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. Lásd: Magyarország Nemzeti Kiberbiztonsági Stratégiája 1139/2013. (III.21.) Korm. határozat 3. pont

[114] Az alfejezet Dr. Klein Tamás írása. Részletes kifejtését lásd: Klein Tamás – Szabó Aliz (2018): A cybercrime, mint infokommunikációs jogi probléma, In Klein Tamás (szerk.): Tanulmányok a technológia- és cyberjog néhány aktuális kérdéséről, 144–153 o.

(cyberbullying) fenyegeti. A zaklatás mindennapossá vált az internetes világban. A *cyberbullying* egy új típusa az elsősorban tinédzserkorúak közt tapasztalható iskolai kiközösítésnek. Megvalósulhat fenyegető üzenetek formájában, *grooming*[115] során, az áldozat nevében vagy akár személyes adataival való visszaéléssel is. Az internetes zaklatások helyszínei többnyire a közösségi oldalak és az azonnali üzenetküldők. A *cyberbullying* egyes formái:

Flaming[116] (leégetés) során a fórumokon trágár hozzászólások kerülnek a nyilvánosság elé, a vita gyakran vallási, ideológiai vagy politikai kérdésen alapszik.

Az identitáslopás gyakran jár az áldozat e-mail fiókjának vagy közösségi oldalának feltörésével; leggyakoribb célja, hogy kompromittáló üzenetet továbbítsanak a sértett nevében ismerősei számára.

A ***cyber-stalking****ot* elszenvedettek 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 utolsó sorban a *sexting* provokatív, szexuális tartalmú fényképek, videók készítését és infokommunikációs hálózaton (elsősorban közösségi hálózaton) keresztüli terjesztését jelenti, melyek megosztása akár hosszú ideig üldözheti a szégyenbe hozott személyt. Az is előfordulhat, hogy évek múltán, pl. álláskeresés alkalmával okoz érdeksérelmet a megszégyenített személynek. Az erotikus felvételeket az esetek egy részében önmagukról vagy közös megegyezéssel más(ok) ról készítették, de a képek, videók internetes megosztást követően kikerülnek ellenőrzésük alól. Az önkéntes, néha felelőtlen megosztás mellett a közzététel másik indítéka sok esetben a bosszúvágy. Általában egy párkapcsolat megszakadása után az egyik fél a párjáról készített felvételeket (automatikusan, vagy zsarolást követően, pl. ha a kapcsolat folytatására irányuló követelését a másik fél megtagadja) nyilvánosságra hozza.

A fenti cselekmények számos jogellenes cselekményt, büntető törvénykönyvi tényállást is megvalósítanak, a Btk. számos tényállása ugyanis nem csak offline, de online környezetben is megvalósítható, mint pl. zaklatás (Btk. 222. §), gyermekpornográfia (Btk. 204. §), személyes adattal való visszaélés (Btk. 219. §) stb.

6.1.1.2. Adathalászat: phishing, pharming

A kiberbűncselekmény elkövetésének egy másik lehetséges esete az adathalászat.

A *phishing*-támadások során potenciális áldozatok milliói kapnak levelet, amelyekkel megtévesztik vagy támadják őket. Az üzenetek látszólag megbízható forrásból érkeznek, gyakran sürgető határidővel, és az online felhasználók személyes adatainak, különösen banki azonosítóinak, jelszavainak megszerzését célozzák.

A *pharming* annyival több az előzőnél, hogy a levelek rendszerint egy káros kódot tartalmazó, támadó honlapra mutatnak, és megpróbálják rosszindulatú szoftverrel (*malware*) megfertőzni a látogatók számítógépét: különösen személyes adatok eltulajdonítására, levélszemét küldésére, a hardware, különösen a meghajtók megfertőzésére, illetve további hasonló szoftverek terjesztésére használják. Az adathalász levél tartalmazhat olyan fertőzött mellékletet is, mely megpróbálja megfertőzni a számítógépet és átvenni felette az irányítást.

A *spear phishing*, (célzott adathalász-támadás) sokkal célirányosabb, a kiszemelt áldozatok köre sokkal szűkebb, általában 5-10 tagból áll. Ennek célja a 'célpontok', felhasználók online szokásainak tanulmányozása, például Google- vagy Facebook-fiókjaik átolvasásával, fórumokon közölt üzeneteik vizsgálatával. Ezt követően a támadók egy személyre szabott, relevánsnak tűnő levelet készítenek a

[115] Bár a grooming, azaz az online behálózás önmagában nem bűncselekmény, alkalmas a gyermekek személyes adatainak kicsalására, „szexuális játékokba" való bevonására, az áldozatok szégyenérzetének erősítésére.

[116] A flaming vagy másnéven flame war során szándékosan jogsértő, ellenséges, témához nem kapcsolódó hozzászólásokat küld az elkövető az internetes fórumra. A kifejezés mára bizonyos fokig elavult, pontosabb definíció lehet a problémakörre a trolling, mely azonban valamivel tágabb, a teljes provokatív, vitagerjesztő magatartást leírja.

kiszemelt személy számára, így az még nagyobb valószínűséggel válhat áldozattá.

Minél több személyes információt osztunk meg magunkról az online térben, annál kiismerhetőbbek, egyúttal annál kiszolgáltatottabbak leszünk. A tudatos online felhasználói attitűd ezért is jut igen jelentékeny szerephez az ilyen támadásokkal szemben.

A cyberbullying és sexting jelenségei, de az adathalász tevékenység fokozódása is jól példázza, hogy a magánszférához való viszonyulás társadalmi szinten rendkívül negatív irányba változott, hiszen ugyan ellenkező szempontból, de a magánélet sérülékenységét mutatja: a cyberbullying más magánszférájának a semmibe vétele, a sexting pedig a felhasználó saját magánszférájának a teljes megnyitását, az annak védelméről való önkéntes lemondást jelenti.

6.1.2. Az egyes jogellenes tartalmak differenciálása, különös tekintettel a gyermekek érdekére

Az internetes tartalmakat természetesen nem lehet homogén módon kezelni, azok differenciált megközelítése szükséges. Az Európai Bizottság[117] a korlátozhatóság intenzitásának mértéke alapján differenciált a *jogellenes* és a *káros* tartalmak között. Egyes jogellenes tartalmak magánjogi, mások a szigorúbb, büntetőjogi szabályozás alá esnek. A felelősségre vonás és az alkalmazható joghátrány tekintetében ennek igen nagy jelentősége van.

A jogellenes tartalmak nem csak az offline világban, de az online környezetben is általánosan tiltottak, ellenben azon káros tartalmak hozzáférhetőségét, amelyek nem jogellenesek, de a gyermekek fejlődésére kedvezőtlenül hathatnak, korlátozni szükséges. A jogellenes tartalmak nem élvezik a véleménynyilvánítás szabadságának védelmét, azok a szabad véleménynyilvánítás alkotmányos jogának védelmi zónáján kívül esnek. A káros (ártalmas) tartalmakra azonban kiterjed a véleménynyilvánítás szabadsága, eszerint szabadon tehetők közzé. Az ilyen tartalmak a felnőttek számára szabadon 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 online tartalomszolgáltatók adekvát technikai eszközökkel korlátozzák.

Olyan eszközök alkalmazása szükséges, amelyek biztosítják a kiskorúak hatékony védelmét a káros tartalmakkal szemben, ám egyúttal nem korlátozzák a felnőttek további hozzáférését. Kiskorúakra ártalmasak lehetnek az erőszakos és a szexuális tartalmak, a kábítószer- és alkoholfogyasztás megjelenése, valamint a trágár nyelvhasználat. A kiskorúak védelme érdekében az internetes szolgáltatók önszabályozásának és az állami szabályozásnak az együttes alkalmazása szükséges, és ennek érdekében célszerű a kiskorúak közötti, korosztályonként való különbségtétel, hogy a védelem minél differenciáltabb lehessen.

A káros tartalmak körének meghatározását több tényező befolyásolja, így pl. az államok társadalmi, kulturális hagyományai, vagy éppen a közerkölcs.

Az NMHH Médiatanácsa ajánlást tett közzé[118] a lekérhető és lineáris médiaszolgáltatások esetén alkalmazott hatékony műszaki megoldások fejlesztése érdekében. Az ajánlás a felhasználók végberendezéseire egy gyerekszűrő program (gyerekzár) telepítését javasolja a kiskorúak számára káros tartalom elérése előtti figyelmeztetés mellett.

---

[117] 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.

[118] A Médiatanács ajánlása a kiskorúak védelmében a lineáris és lekérhető, médiaszolgáltatók által alkalmazandó hatékony műszaki megoldásokra (aktuális változat), nmhh.hu/cikk/184785/ A_Mediatanacs_ajanlasa_a_kiskoruak_vedelmeben_ a_linearis_es_lekerheto_mediaszolgaltatok_altal_alkalmazando_hatekony_muszaki_megoldasokra_aktualis_valtozat.

6.1.3. A hiperlink (hiperhivatkozás), mint a jogsértés eszköze

A hiperhivatkozás egy olyan informatikai eszköz, amely egy adott (szöveges) tartalomban kerül elhelyezésre úgy, hogy egy másik tartalomra mutat. A felhasználót választása esetén (kattintást követően) a jól azonosítható, színében eltérő *hiperlink* átvezeti a javasolt oldalra, amelynek következtében az ott található tartalom megismerhetővé válik.

A phishinget elkövető bűnözők 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 megállapíthatóbb. 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.

6.1.4. A jogellenes tartalmak blokkolása

Az állami hatóságok által alkalmazott internetes tartalomblokkolási lehetőségek (honlapok, vagy egyes tartalmak: pl. képek, videók, szöveges tartalmak) kiemelten fontosak a jogellenes tartalmak elleni fellépésben. A blokkolással lehetséges az elérhető tartalom korlátozása, a tartalomközvetítő IP-címek hozzáférhetetlenné tétele, a weboldalak eltávolítása, valamint szűrőprogramok használata is, amelyek szintén a tartalom elérhetetlenné tételét szolgálják.

Az alapvető jogok, különösen a véleménynyilvánítás védelme érdekében a blokkolás módját minden esetben körültekintően kell megválasztani. Az illegális tartalom három módon szűrhető ki: önszabályozással[119], 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 a bűncselekményt megvalósító 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 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)[120] helyezi előtérbe. Magyarországon az N&TD eljárás átlagos ideje belföldi és az EU tagállamokban található szolgáltató esetén 12-36 óra, az Egyesült Államokban *hostolt* tartalom esetén, 24-48 óra[121]. A gyermekpornográfia az

[119] A felhasználó saját elvei alapján, saját internethasználatához telepíti a megfelelő védelmi mechanizmust.

[120] Az illegális tartalom eltávolítására szolgáló eljárás. Érdekesség, hogy az INHOPE, a legnagyobb nemzetközi forródróthálózat (mára 33 országban van nemzetközi forródrótja) azzal a feltétellel veszi fel a tagjait, hogy azok helyi és országos szinten egyaránt a nyomozóhatóság támogatását élvezzék. Magyarország 2005 óta INHOPE-tag.

[121] INHOPE Annual Report 2010. www.inhope.org/Libraries/Annual_reports/2010_Annual_report.sflb.ashx

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.

Hangsúlyozni szükséges, hogy a tartalmak blokkolása a véleménynyilvánítás szabadságának súlyos korlátozását okozza, ezért alkalmazása szigorú alkotmányos mércék alapján történhet, különösen súlyos bűncselekmények esetén. A magánszolgáltatók blokkolási tevékenysége, bár néhány esetben vitathatatlanul hasznos, különösen aggályos, hiszen az állami beavatkozással szemben az intézkedés alapjául szolgáló norma és a döntés indokai sok esetben nem egyértelműek, és a jogorvoslat lehetősége is kizárt, vagy esetleges.

A cybercrime jelensége és a felhasználók fenyegetettsége vitathatatlan. A megelőzés kizárólag több szereplő együttes fellépése esetén lehet hatékony. Ennek az együttműködésben szerepe van az internetszolgáltatóknak, a felhasználóknak és a hatóságoknak is.

6.2. Cyberbiztonság[122]

6.2.1. Bevezetés

A hálózatbiztonság kérdésének felértékelődése egyenes következménye a gazdasági, politikai, személyes élettér online világba való növekvő arányú áthelyeződésének. Az információk nagy tömegű online előfordulása jelentősen növeli az azokkal való visszaélés kockázatát is. Természetesen a hálózatok és informatikai rendszerek biztonságát nem csak a rosszindulatú támadások, de a vétlen 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 vétlen behatások súlyos következményekkel járhatnak (lsd. 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 és az információs és kommunikációs technológiák széles körű alkalmazásában rejlő lehetőségeket.[123]

A kibertér biztonsága nem képzelhető el a kiberteret alkotó elektronikus információs rendszerek, valamint az 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.[124]

A kiberbiztonság fenntartásának egyik eszköze az elektronikus hálózati és információs rendszerek (HIR) biztonsága, amely az adatok és az információs rendszerelemek olyan állapota, amelyben azok *védelme* az összes számításba vehető fenyegetésre nézve teljes körűen, folyamatosan, a

[122] Az alfejezet Dr. Tóth András írása. Részletes kifejtését lásd: Tóth András (2018): Hálózati és információs rendszerek biztonsága európai szabályozásának alapjai, In Klein Tamás (szerk.): Tanulmányok a technológia- és cyberjog néhány aktuális kérdéséről, 67–87.

[123] 526/2013/EU rendelet az Európai Uniós Hálózat- és Információbiztonsági Ügynökségről (ENISA) HL L 165/41., 2. preambulum-bekezdés

[124] Lásd az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 1. § 26. pontját

kockázatokkal arányosan (tehát a védelem költségei arányosak a fenyegetéssel okozható károkkal) megvalósul.[125] A HIR biztonsága az arra való **képességet** jelenti, hogy **ellenálljon** mindazon fenyegetéseknek, amelyek veszélyeztetik annak rendelkezésre állását, hitelességét, sértetlenségét, bizalmasságát[126], amelyek a legfőbb érték – a kibertér fejlődéséhez szükséges társadalmi bizalom – kialakításának zálogai.[127]

A HIR-szabályozás célja tehát a kibertér fejlődéséhez szükséges társadalmi **bizalom**[128] **elfogadható kockázati szinten tartása**.

6.2.2. A HIR ellenálló képességére vonatkozó EU szabályozás

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 észrevehetők és az elkövetők felderítése a technikai és globális jelleg 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 az *EU oldaláról* tekintjük át.

	Alapvető szolgáltatást nyújtó szolgáltató szereplők	**Digitális szolgáltatók**	**Elektronikus hírközlő hálózatok**
Jogforrás	**2016/1148/EU Irányelv**		**2002/21/EK irányelv és 2002/58/EK irányelv**
Fogalom	**ágazatok: energetika, pénzügyi, egészségügyi, vízszolgáltatási, közlekedési, és internet-infrastruktúra (domainszolgáltatók, adatcsereközpontok)** **ágazattól független szempontok: kritikus társadalmi/gazdasági szempontból és a biztonsági esemény jelentős zavart okozna**	**csak jogi személy lehet; online piactér, kereső-program és felhőalapú szolgáltatásokat nyújtó digitális szolgáltatók (hardver- és szoftvertermékekre a termékfelelősségre vonatkozó hatályos szabályok vonatkoznak, nem ez az irányelv)**	**olyan, általában díjazás ellenében nyújtott szolgáltatás, amely teljes egészében vagy nagyrészt elektronikus hírközlő hálózaton történő jelátvitelből áll**
Biztonsági esemény fogalma	**ténylegesen kedvezőtlen hatás a hálózati és információs rendszerek biztonságára**		**jelentős hatás a hálózatok, illetve a szolgáltatások működésére**

[125] Uo.

[126] Európai Parlament és a Tanács Irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről, 2016/1148/EU irányelv, HL L 194/1 2016. július 6., 4. cikk (2) bekezdés

[127] 2016/1148/EU irányelv 2. preambulum-bekezdése

[128] 2016/1148/EU irányelv 2. preambulum-bekezdése

	Alapvető szolgáltatást nyújtó szolgáltató szereplők	Digitális szolgáltatók	Elektronikus hírközlő hálózatok
Biztonsági esemény bejelentése	**illetékes hatóságnak**		**nemzeti hatóságnak, aki szükség esetén értesíti a többi tagállam nemzeti szabályozó hatóságát és az Európai Hálózat- és Információbiztonsági Ügynökséget;** **hálózati biztonság megsértésének konkrét kockázata esetén az előfizetőket is**
Intézkedések	**megfelelő műszaki és szervezeti intézkedések**		

A 2016/1148/EU irányelv értelmében 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*.”[129] Minden tagállam – legalább az alapvető szolgáltatásokat nyújtó szervezetekre és az irányelv által lefedett digitális szolgáltatásokra vonatkozóan – kijelöl egy vagy több CSIRT-et (**Computer security incident response teams**), amelyek a kockázatoknak és a biztonsági eseményeknek egy jól meghatározott eljárással összhangban történő kezeléséért felelősek.[130] A CSIRT-ek feladatai: a biztonsági események nemzeti szintű monitoringja, a kockázatokkal és biztonsági eseményekkel kapcsolatos korai előrejelzés, riasztás, bejelentéstétel és információterjesztés a releváns érdekeltek számára; reagálás a biztonsági eseményekre; a CSIRT-ek hálózatában való részvétel.[131]

Külön meg kell emlékezni az európai **kritikus infrastruktúrákról** (European Critical Infrastructure – a továbbiakban: ECI), amelyek védelme meghaladja a kiberteret, de természetesen arra is kiterjed. A 2008/114/EK irányelv[132] szerint a kritikus infrastruktúra körébe tartoznak a tagállamokban található azon eszközök, rendszerek vagy ezek részei, 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.[133] Az „európai kritikus infrastruktúra” vagy „ECI” a tagállamokban található olyan kritikus infrastruktúra, amelynek megzavarása vagy megsemmisítése jelentős hatással lenne legalább két tagállamra. Az irányelv végrehajtásában érintett ágazatok az **energiaágazat és a közlekedési ágazat**.[134] Valamennyi kijelölt ECI tekintetében gondoskodni kell arról, hogy létezzen egy üzemeltetői biztonsági terv (Operator Security Plan – a továbbiakban: OSP), amelyek magukban foglalják a jelentős eszközök meghatározását, a kockázatértékelést, valamint az ellenintézkedések és -eljárások meghatározását, kiválasztását és rangsorolását.[135] Valamennyi kijelölt ECI tekintetében gondoskodni kell egy **biztonsági összekötő** tisztviselő kijelöléséről és biztonsági átvilágításáról.[136]

Az ECI-k tulajdonosai/üzemeltetői számára hozzáférést kell biztosítani a kritikus infrastruktúrák

129 2016/1148/EU irányelv II. Fejezet, 7. cikk (1)
130 2016/1148/EU irányelv 9. cikk (1) bekezdés
131 2016/1148/EU irányelv I. Melléklet (2) bekezdés
132 2008/114/EK irányelv az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről HL L 345/75 2008. december 8., 2. preambulum-bekezdés
133 2008/114/EK irányelv 2. cikk a) pont
134 2008/114/EK irányelv 3. cikk (3) bekezdés
135 2008/114/EK irányelv 11. preambulum-bekezdés
136 2008/114/EK irányelv 13. preambulum-bekezdés

védelmével kapcsolatos **legjobb gyakorlatokhoz** és módszerekhez.[137] 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: ECIP kapcsolattartó pont).[138]

6.2.3. Adatbiztonság

A GDPR[139] 32. cikk (1) bekezdése szerint az adatkezelő és az adatfeldolgozó a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével **megfelelő technikai és szervezési intézkedéseket** hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja. A GDPR 33. cikk (1) bekezdése értelmében az adatvédelmi incidenst[140] az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, **bejelenti** az illetékes felügyeleti **hatóságnak**. 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 Bizottság **ePrivacy javaslata** az elektronikus hírközlés során a magánélet tiszteletben tartásáról és a személyes adatok védelméről, valamint a 2002/58/EK irányelv hatályon kívül helyezéséről **kiegészítené** 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.[141] A Javaslat továbbá kiegészíti a GDPR-t abban az értelemben is, hogy a személyes adatnak minősülő elektronikus hírközlési adatok kezelésére vonatkozik.[142]

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.

---

137 2008/114/EK irányelv 16. preambulum-bekezdés

138 2008/114/EK irányelv 10. cikk

139 Az Európai Parlament és a 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, a továbbiakban: GDPR) OJ L 119, 4.5.2016, p. 1–88

140 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

141 Javaslat 3. preambulum-bekezdése

142 Javaslat 5. preambulum-bekezdése

7. JOGSZABÁLYTÁR

1. Az Európai Parlament és a 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, a továbbiakban: GDPR) OJ L 119, 4.5.2016
2. 526/2013/EU rendelet az Európai Uniós Hálózat- és Információbiztonsági Ügynökségről (ENISA) HL L 165/41.
3. Az Európai Parlament és a Tanács 2002/21/EK irányelve (2002. március 7.) az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások közös keretszabályozásáról (Keretirányelv) OJ L 108, 24.4.2002, 33–50. o.
4. Az Európai Parlament és a Tanács 2005/29/EK irányelve (2005. május 11.) a belső piacon az üzleti vállalkozások fogyasztókkal szemben folytatott tisztességtelen kereskedelmi gyakorlatairól, HL L 149.,. 2005.6.11., 22. o.
5. 2008/114/EK irányelv az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről HL L 345/75 2008. december 8.
6. Az Európai Parlament és a Tanács 2009/140/EK irányelve (2009. november 25.) az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások közös keretszabályozásáról szóló 2002/21/EK irányelv, az elektronikus hírközlő hálózatokhoz és kapcsolódó eszközökhöz való hozzáférésről, valamint azok összekapcsolásáról szóló 2002/19/EK irányelv és az elektronikus hírközlő hálózatok és az elektronikus hírközlési szolgáltatások engedélyezéséről szóló 2002/20/EK irányelv módosításáról (EGT-vonatkozású szöveg) OJ L 337, 18.12.2009, 37–69. o.
7. Európai Parlament és a Tanács Irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről, 2016/1148/EU irányelv, HL L 194/1 2016. július 6.A fegyveres biztonsági őrségről, a természetvédelmi és mezei őrszolgálatról szóló 1997. évi CLIX. törvény
8. Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény
9. 2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről
10. A személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény
11. Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.),
12. 2012. évi I. törvény a Munka Törvénykönyvéről
13. A Büntető Törvénykönyvről szóló 2012. C. törvény
14. A Polgári Törvénykönyvről szóló 2013. évi V. törvény
15. Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény Magyarország Nemzeti Kiberbiztonsági Stratégiája 1139/2013. (III.21.) Korm. határozat

8. IRODALOMJEGYZÉK

1. Christián László (szerk.) (2013): Az információs társadalom jogi vetületei, Pázmány Press, Budapest
2. Daele, Wolfgang van den (2010): Access to New Technology. In Defense of the Liberal Regime of Innovation, in. Dimension of technology Regulations, eds.: Goodwin, Morag, Koops, Bert-Jaap, Leenes, Ronald, Wolf Legal Publishers
3. Dobrocsi Szilvia – Domokos Andrea (2018): Kiberbűnözés, In. Homicskó Árpád Olivér (szerk.): Egyes modern technológiák etikai, jogi és szabályozási kihívásai. Acta Caroliensia Conventorum Scientiarum Iuridico-Politicarum XXII. Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, Budapest
4. Edelman, Benjamin G., Geradin, Damien: Efficiencies and Regulatory shortcuts: How should we regulate companies like Airbnb and Uber? November 24, 2015., Forthcoming, Stanford Technology Law Review , 1.
5. Geradin, Damien (2015): Should Uber be Allowed to Compete in Europe; And if so How? Competition Policy International, June 2015
6. Klein Tamás – Szabó Aliz (2018): A cybercrime, mint infokommunikációs jogi probléma, In. Tanulmányok a technológia- és cyberjog néhány aktuális kérdéséről, Budapest: Médiatudományi Intézet,
7. Klein Tamás – Tóth András (2018): A robotika egyes szabályozási kérdései, In. Homicskó Árpád Olivér (szerk.): Egyes modern technológiák etikai, jogi és szabályozási kihívásai, Budapest, Károli Gáspár Református Egyetem, Állam- és Jogtudományi Kar
8. Koops, Bert-Jaap (2010): Ten dimensions of technology regulation. Finding your bearings in the research space of an emerging discipline, in. Dimension of technology Regulations, eds.: Morag Goodwin, Bert-Jaap Koops, Ronald Leenes, Wolf Legal Publishers
9. Moór Gyula (1931): A jogi személyek elmélete, Az MTA jogtudományi Bizottság kiadványsorozata, Budapest
10. Ocello, Eleonora, Sjödin, Cristina, Subočs, Anatoly: What's Up with Merger Control int he Digital Sector? Lessons from the Facebook/whatsApp EU merger case, Competition merger brief, Issue 1/2015 – February, 6.
11. Péterfalvi Attila (szerk.) (2012): Adatvédelem és Információszabadság a mindennapokban, HVG-ORAC, Budapest
12. Posen, Hannah A. (2016): Ridesharing in the Sharing Economy: should Regultarors Impose Über Regulations on Uber? Iowa Law Review, Vol.101:405
13. Brownsword, R. – Goodwin, M. (2012): Law and the Technologies of the Twenty-First Century. Texts and Materials (Cambridge-New York: Cambridge University Press
14. Ranchordás, Sofia (2015): Does Sharing Mean Caring? Regulating Innovation in the Sharing Economy, Tilburg Law School Legal Studies Research Paper Series No.06/2015, Minnesota Journal of Law Science & Technology, Vol. 16:1
15. Richards, Neil M. – Smart, William D. (2016): How should the law think about robots?, In. Ryan Calo – A. Michael Froomkin – Ian Kerr Robot Law, Edward Elgar Publishing, Cheltenham, UK – Northampton (USA)

16. Peltzman, Sam (1976), Toward a More General Theory of Regulation, The Journal of Law and Economics. Vol 19., No. 2., 211-240.

17. Sorbán Kinga (2015): 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

18. Sorbán Kinga (2016): Az informatikai bűncselekmények elleni fellépés az Egyesült Államokban. In Themis, 2016. június, 150-170. (www.ajk.elte.hu/file/THEMIS_2016_jun.pdf.)

19. Sorbán Kinga (2010): Informatikai bűncselekmények és nyomozásuk az Egyesült Királyságban. Belügyi Szemle, 63. évf. 9. sz., 48-68.

20. SORBÁN Kinga (2015): Az informatikai bűncselekmények elleni fellépés nemzetközi dimenziói. Themis, 2015. június, 343-375.

21. Stigler, Georges (1971): The Theory of Economic Regulation, 2 Bell Journal of Economics. Vol. 2, issue 1, 3-21

22. Szabó Endre Győző (2016a): A kétoldalú piacok elméletének kapcsolata a személyes adatok védelméhez fűződő jog érvényesítésével a Google ítélet fényében, Pázmány Law Working Papers, 2016/7

23. Szabó Endre Győző (2016b): Az Európai Unió általános adatvédelmi rendeletének egyes kérdéseiről II. Beépített és alapértelmezett adatvédelem - Adatvédelmi incidensek bejelentése, Pázmány Law Working Papers, 2016/27

24. Tóth András (szerk.) (2016): Technológia jog – Új globális technológiák jogi kihívásai, Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, Budapest

25. Udvary Sándor (2017a): Az önvezető gépjárművek egyes technikafüggő szabályozási kérdései. In. Gellén Klára (szerk.): Jog, innováció, versenyképesség, Wolters Kluwer, Budapest

26. Udvary Sándor (2017b): Az önvezető gépjárművek egyes technikafüggő szabályozási kérdései, In. Gellén Klára (szerk.): Jog, Innováció, versenyképesség, Wolters Kluwer, Budapest,

27. Udvary Sándor (2016a): Sofőr nélkül biztonságosabb? Az önvezető gépjárművel formálódó jogi háttere, In. Ügyvédvilág, X. évf. 4. sz., 16-17.

28. Udvary Sándor (2016b): Vehere necesse est – az önvezető gépjárművekhez kapcsolódó jogi kérdések körvonalazása, In. Lege et fidei, Ünnepi tanulmányok Szabó Imre 65. születésnapjára, Iurisprudentius Kiadó, Szeged, 644-653.

29. Versluis, Esther, Van Asselt, Marjolein, Fox, Tessa, Hommels, Anique (2010): Calculable Risks? An Analysis of the European Seveso Regime, in. Dimension of technology Regulations, eds.: Goodwin, Morag, Koops, Bert-Jaap, Leenes, Ronald, Wolf Legal Publishers,

30. Zara Orsolya (2016): Robo Sapiens, avagy személy lesz-e a robot? Aktuális jogi és szabályozási kérdések az Európai Parlamentben, In. Európai Jog, 16. évf. 3. sz., 48-51.

9. ELEKTRONIKUS FORRÁSOK

1. Autorité de la Concurrence – Bundeskartellamt: Competition Law and Data, 10th May, 2016., (http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf, (letöltés ideje: 2018.03.08.)
2. Big data and innovation: Implications for Competition Policy in Canada, draft discussion Paper, (http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/vwapj/Big-Data-e.pdf/$file/Big-Data-e.pdf, letöltés ideje: 2018.03.08.)
3. BKartA, B6-113/15, Working Paper – Market Power of Platforms and Networks, June 2016 (https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Berichte/Think-Tank-Bericht-Langfassung.pdf?__blob=publicationFile&v=2)
4. Colangelo, Giuseppe – Maggiolino, Mariateresa, Data Protection in Attention Markets: Protecting Privacy Through Competition? (April 2, 2017). Forthcoming, Journal of European Competition Law & Practice. (https://ssrn.com/abstract=2945085 vagy http://dx.doi.org/10.2139/ssrn.2945085, letöltés ideje: 2018.03.08.)
5. Collaborative project (CP), FP7-SiS-Challenge 1-3: Regulating Emerging Robotic Technologies in Europe: Robotics facing Law and Ethics (Robolaw), www.robolaw.eu, [letöltés ideje: 2018.03.08.]
6. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Online Platforms and the Digital Single Market, Opportunities and Challenges for Europe, COM(2016) 288/2, 2. (https://ec.europa.eu/digital-single-market/en/news/communication-online-platforms-and-digital-single-market-opportunities-and-challenges-europe)
7. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) European Civil Law Rules in Robotics – Study, ,(http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016)571379_EN.pdf, letöltés ideje: 2018.03.08.)
8. Federal Trade Commission: .com Disclosures, How to Make Effective Disclosures in digital Advertising, March 2013, (https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-revises-online-advertising-disclosure-guidelines/130312dotcomdisclosures.pdf)
9. Jelentés a digitális egységes piaci intézkedéscsomag megvalósításáról (2015/2147(INI)), (http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2015-0371+0+DOC+XML+V0//HU)
10. OECD: Big Data: Bringing Competition Policy to the Digital Era DAF/COMP/M(2016)14, 27-Oct-2016, (https://one.oecd.org/document/DAF/COMP(2016)14/en/pdf, letöltés ideje: 2018.03.08.)
11. OECD Working Party No.2 on Competition and Regulation: Protecting and Promoting Competition in Response to „Disruptive" Innovations in Legal Services, 13 June 2016, DAF/COMP/WP2(2016)1, (http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/COMP/WP2(2016)1&docLanguage=En)
12. P8_TA(2017)0051 A robotikára vonatkozó polgári jogi szabályok, Az Európai Parlament 2017. február 16-i állásfoglalása a Bizottságnak szóló ajánlásokkal a robotikára vonatkozó polgári jogi szabályokról (2015/2103(INL)), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0051+0+DOC+XML+V0//HU

13. Preliminary Report on the E-commerce Sector Inquiry, Brussels, 15.9.2016 SWD(2016) 312 final, (http://ec.europa.eu/competition/antitrust/sector_inquiry_preliminary_report_en.pdf, letöltés ideje: 2018.03.08.)
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.

A Nemzeti Közszolgálati Egyetem kiadványa.

Nemzeti Közszolgálati Egyetem;
Államtudományi és Közigazgatási Kar
www.uni-nke.hu

Felelős Kiadó:
Prof. Dr. Kis Norbert Dékán
Címe:
1083 Budapest, Üllői út 82.
Kiadói szerkesztő:
Vörös Ferenc
Tördelőszerkesztő:
Bödecs László

978-615-5870-30-9 (PDF)

A kiadvány
a KÖFOP-2.1.1-VEKOP-15-2016-00001
„A közszolgáltatás komplex kompetencia,
életpálya-program és oktatás technológiai
fejlesztése” című projekt keretében készült
el és jelent meg.