

Digitizálódó társadalom

Tanulmányok az új technológiák
társadalmi-jogi hatásairól



Szerkesztette
Török Bernát – Zódi Zsolt



LUDOVIKA
EGYETEMI KIADÓ

Digitalizálódó társadalom



Digitalizálódó társadalom

Tanulmányok az új technológiák
társadalmi-jogi hatásairól

Szerkesztette

Török Bernát – Zódi Zsolt



LUDOVIKA
EGYETEMI KIADÓ

Budapest, 2023

A kötet megjelenését a Nemzeti Média- és Hírközlési Hatóság támogatta.



Szerzők

Bányász Péter
Bencsik András
Czékmann Zsolt
Czibrik Eszter
Csudai Tünde
Detrekői Zsuzsa
Domokos Márton
Kántor Ákos
Kelemen Roland
Kéring Szabolcs

Klein Tamás
Menyhárd Attila
Nogel Mónika
Nyáry Gábor
Papp János Tamás
Püskösty András
Sorbán Kinga
Szabó Endre Győző
Török Bernát
Zódi Zsolt

Szakmai lektor
Rab Árpád Szörény

Kiadja a Nemzeti Közszerzői Egyetem
Ludovika Egyetemi Kiadó
A kiadásért felel: Deli Gergely rektor

Székhely: 1083 Budapest, Ludovika tér 2.
Kapcsolat: kiadvanyok@uni-nke.hu

Felelős szerkesztő: Pordány Katalin
Olvasószerkesztő: Szabó Ilse
Korrektor: Kutas Éva
Tördelőszerkesztő: Fehér Angéla

Nyomdai kivitelezés: Pátria Nyomda Zrt.
Felelős vezető: Orgován Katalin vezérigazgató

DOI: https://doi.org/10.36250/01164_00

ISBN 978-615-6598-72-1 (nyomtatott)
ISBN 978-615-6598-73-8 (ePDF) | ISBN 978-615-6598-74-5
(ePub)

© A szerkesztők, 2023
© A szerzők, 2023
© A kiadó, 2023

Minden jog védve.

Tartalom

<i>A kötet szerzői</i>	7
<i>Bevezető Társadalmat és jogot felforgató technológiák</i>	11
I. rész Állam és digitalizáció	19
Czékmann Zsolt – Czibrik Eszter: Nagyító alatt az automatikus döntéshozatali eljárás	21
Bencsik András: A közigazgatás esete a digitalizációval	31
Kántor Ákos: Jogalkotás és digitalizáció – kihívások és dilemmák	41
Kelemen Roland: A cyberfare state alapgondolata – Az egyén és kapcsolatai átalakulásának hatása az állam működésére és biztonságára	63
II. rész Platformok és szabályok	79
Zódi Zsolt: A platformszabályozás megold(hat)atlan dilemmái	81
Detrekői Zsuzsa: Az EU szerzői jogi direktívája: segélykiáltás a hazai videómegosztó platformokért	103
Klein Tamás: Az újmédia szabályozásának új iránya? – A Digital Services Act alapjogvédelmi mechanizmusa	117
Papp János Tamás: A szűrőbuborék kipukkasztása – Gondolatok az online szűrőbuborékok és visszhangkamrák koncepciójának újraértelmezéséhez	141
Csudai Tünde: A pluralizmus érvényesülése a tömegtájékoztatás piacán	161
Kéring Szabolcs: NetzDG, avagy gyakorlati példa a platformszabályozás megvalósítására	175
III. rész Adatok és normák	197
Menyhárd Attila: Az egészségügyi adatok jogi természete	199
Pünkösty András: A nagy adathalmazok felhasználásának etikai kérdései – avagy szükség van-e adatetikára?	215
Nogel Mónika: A precíziós medicina és a demokrácia kölcsönhatásai	235
Domokos Márton: Hogyan segíthetik a mesterséges intelligenciával kapcsolatos „emberi jogi hatásvizsgálatok” a demokráciát?	245
Szabó Endre Győző: Pirkad a metaverzumban: az új virtuális világ egyes adatvédelmi és társadalmi kérdéseiről	269
IV. rész Műveletek a kibertérben	287
Sorbán Kinga: Hacktivizmus a demokráciában – bűncselekmény vagy politikai véleménynyilvánítás?	289
Bányász Péter: Lélektani műveletek az ukrán–orosz háborúban	309
Nyáry Gábor: Akindzsik a kibertérben	321

Vákát

A kötet szerzői

Bányász Péter politológus, kiberbiztonsági szakértő. Doktori értekezését a közösségi média és a védelmi szféra kapcsolatából írta. Fő kutatási területe a kiberbiztonság humán aspektusa. Jelenleg a Nemzeti Közszolgálati Egyetem Államtudományi és Nemzetközi Tanulmányok Karának adjunktusa, az Egyetem Kiberbiztonsági Kutatóintézetének kutatója. A Magyar Hadtudományi Társaság szakértője.

Bencsik András egyetemi docens, az ELTE Állam- és Jogtudományi Kar Közigazgatási Jogi Tanszékének oktatója. Kutatási területei közé tartozik: a közigazgatási hatósági eljárás, a közigazgatási bíráskodás, a közigazgatási működés törvényességének biztosítása, továbbá a gazdasági közigazgatás (versenyjog, fogyasztóvédelem) témakörei, valamint a mesterséges intelligencia alkalmazásának lehetőségei a közigazgatásban. E tárgykörökben több pályázati kutatási és szakértői projektben vett részt kutatóként. Számos hazai és külföldi (angol nyelvű) publikáció szerzője. 2015-ben jelent meg *A közigazgatás törvényességétől a technológiai innovációig* című monográfiája. 2015 januárja és 2016 januárja között az általános közigazgatási rendtartásról szóló törvényt előkészítő Kodifikációs Bizottság tagja volt. Tagja a Public Governance, Administration and Finances Law Review bírálóbizottságának. Az MTA köztestületi tagja.

Czékmann Zsolt intézeti tanszékvezető egyetemi docens a Miskolci Egyetem Állam- és Jogtudományi Kar Államtudományi Intézet Közigazgatási Jogi Tanszékén. Kutatási területei: infokommunikáció és jog, e-közzszolgáltatások, digitális állam, smart city, közigazgatási jog alapintézményei, közzszolgálati jog.

Czibrik Eszter harmadéves PhD-hallgató a Miskolci Egyetem Deák Ferenc Állam- és Jogtudományi Doktori Iskolájában. Kutatási területei: közigazgatási hatósági eljárás, közigazgatási szerződések.

Csudai Tünde jogász, 2021 óta a Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi Doktori Iskola PhD-hallgatója. A Pázmány Péter Katolikus Egyetem JÁK Deák Ferenc Továbbképző Intézet médiajogi szakjogász képzésében 2019-ben LL.M. fokozatot szerzett. Jelenleg a Szabályozott Tevékenységek Felügyeleti Hatósága Jogi Főosztályának munkatársa, korábban a Hatóság jogelődje, a Szerencsejáték Felügyelet hivatali főtanácsosa volt. A tömeg-tájékoztatáshoz kapcsolódó alkotmányjogi, médiajogi és versenyjogi kérdéskörökben kezdte meg doktori kutatását. Angol felsőfokú és német középfokú szintű nyelvismerettel rendelkezik.

Detrekői Zsuzsa TMT-jogász és részmunkaidőben egyetemi oktató. 2007-ben és 2008-ban néhány hónapig a Harvard Egyetem Berkman Center for Internet & Society OpenNet Initiative tanácsadója volt. Az origo.hu online tartalomszolgáltató főtanácsadója volt. Jelenleg egy jelentős magyarországi internetszolgáltató jogi tanácsadója, emellett jogi támogatást nyújt a Magyarországi Tartalomszolgáltatók Egyesületének. Kutatási területe az online tartalmak és az internettel kapcsolatos szabályozások, amelyből doktori disszertációját is írta, és 2016-ban PhD-fokozatot szerzett.

Domokos Márton a CMS Budapest Ügyvédi Iroda kereskedelmi jogi csoportjának szenior tanácsadója és a regionális adatvédelmi csoport koordinátora. Rendszeresen tart előadásokat (például Internet Hungary, Infotér) és publikál cikkeket (például Jogi Fórum, IAPP Privacy Perspectives, OneTrust DataGuidance, Thomson Reuters' Data Privacy Advisor), elsősorban a mesterséges intelligencia, valamint az adatvédelem témakörében. A Direkt és Interaktív Marketing Szövetség Adatvédelmi Tagozatának elnöke, továbbá a Kürt Akadémia oktatója.

Kántor Ákos a Károli Gáspár Református Egyetem Állam- és Jogtudományi Doktori Iskola doktorandusza. A Nemzeti Közzolgálati Egyetem Információs Társadalom Kutatóintézet megbízott kutatója. Jogi diplomáját a Pázmány Péter Katolikus Egyetemen szerezte 2007-ben, szabályozási (kodifikátor) szakjogász (LL.M.), matematika–fizika szakos tanár, számítógép-rendszer-programozó végzettségekkel rendelkezik. Több minisztériumban dolgozott, az Igazságügyi Minisztériumban részt vett az e-perek kodifikációjában. Az Országos Fordító és Fordításhitelesítő Iroda fejlesztési projektekért felelős vezérigazgatói tanácsadója.

Kelemen Roland 1985-ben született Győrben. A győri Széchenyi István Egyetemen szerzett állam- és jogtudományi diplomát 2015-ben, majd alma materében állam- és jogtudományi doktori fokozatot 2022-ben. 2015 óta oktat a győri Széchenyi István Egyetem Állam- és Jogtudományi Karának Jogtörténeti Tanszékén, jelenleg adjunktusként. 2017 óta kutatóként dolgozik a Nemzeti Közzolgálati Egyetem Hadtudományi és Honvédtisztképző Karának Honvédelmi Jogi és Igazgatási Tanszékén, 2022 óta tudományos munkatársként. Kutatási területei a kivételes hatalom elmélete, története és kortárs kihívásai, valamint a kiberbiztonság és a kiberhadviselés nemzetközi jogi kérdései, továbbá a kiberműveletek és a kibertér jelentősége a hibrid konfliktusokban és ezek összefüggései a védelemi joggal, illetve a kibertér kiépülésének államra, gazdaságra és társadalomra gyakorolt hatásának nemzetbiztonsági következményeit vizsgálja.

Kéring Szabolcs a Pázmány Péter Katolikus Egyetem Jog- és Államtudományi Karán szerzett jogi diplomát, a szakvizsga letétele óta ügyvédkedik Budapesten. Ügyvédként éveken át dolgozott magyarországi médiaszolgáltatóknak, illetve a médiaszolgáltatási tevékenységhez kapcsolódó bizottságokban, alapítványi kuratóriumban is tag; 2019 óta pedig Magyarország Digitális Gyermekvédelmi Stratégiájának állandó szakértője. Munkája mellett a Pázmány Péter Katolikus Egyetem Jog- és Államtudományi Kar Doktori Iskolájának doktorandusza, abszolutóriumot 2022-ben szerzett, kutatási területe az internetes tartalomszolgáltatással és egyéb szolgáltatásokkal kapcsolatban felmerülő felelősségi és szabályozási kérdések.

Klein Tamás a Budapesti Metropolitan Egyetem Üzleti, Kommunikációs és Turisztikai Karának egyetemi docense. Jogi diplomáját az ELTE Állam- és Jogtudományi Karán szerezte, majd ugyanott védte meg PhD-értekezését *A sajtószabadság alkotmányos tartalmának jelentésmódosulásai, különös tekintettel a magyar Alkotmánybíróság gyakorlatára* címmel. Alkotmányjogászként fő kutatási területei a sajtószabadság alkotmányjogi és médiajogi elemzése, valamint a platformgazdaság, különösen a közösségimédia-platformok jogi szabályozásának kérdésköre. Tudományos érdeklődése az elmúlt években egészült ki a mesterséges intelligencia szabályozásának kutatásával. Több mint nyolcvan tudományos közlemény szerzője vagy szerkesztője. Monográfiája *Sajtószabadság és demokrácia* címmel 2020-ban jelent meg.

Menyhárd Attila az ELTE ÁJK Polgári Jogi Tanszékének egyetemi tanára és az NKE Eötvös József Kutatóközpont Információs Társadalom Kutatóintézetének a kutatóprofesszora. Az MTA TK Jogtudományi Intézetének külsős munkatársa. Az UNIDROIT Kormányzótanácsának, a bécsi székhelyű European Centre of Tort and Insurance Law kutatóintézetnek és több más nemzetközi szakmai szervezetnek a tagja.

Nogel Mónika jogász, európai uniós adatvédelmi szaktanácsadó. A Széchenyi István Egyetem Deák Ferenc Állam- és Jogtudományi Kar egyetemi docense, a Nemzeti Közszerződési Egyetem Eötvös József Kutatóközpont Információs Társadalom Kutatóintézet kutatója. Kutatási területe az egészségügyi jog, a genetika és jog kapcsolódási pontjai és a szakértői bizonyítás.

Nyáry Gábor történelem és portugál szakos kutatói diplomával végzett az Eötvös Loránd Tudományegyetem Bölcsészettudományi Karán 1984-ben, majd 1986-ban szerezte meg az egyetemi doktori címet. A Magyar Zoltán e-Közigazgatástudományi Egyesület elnökségi tagjaként a 2000-es évek közepétől foglalkozik az IKT-technológiák és a nemzetközi kapcsolatok egymásra hatásával. 2018 óta tanít a Milton Friedman Egyetemen diplomáciatörténetet és -gyakorlatot, digitális, illetve kulturális diplomáciát, történeti geopolitikát és nagystratégiát. Az NKE-n a Kiberbiztonsági Kutatóintézet kutatójaként vizsgálja a kibertér geopolitikájának, a kiberdiplomáciának és az emergens fenyegetéseknek a problémáit. A Magyar Diplomáciai Akadémia oktatójaként pedig az ország leendő diplomatáit vezeti be a kiberdimenzió világába: a nagystratégiától a nyílt forrású hírszerzésig megannyi témát érintve.

Papp János Tamás a Pázmány Péter Katolikus Egyetem tudományos segédmunkatársa, a Nemzeti Média- és Hírközlési Hatóság Online Platformok Főosztályának jogi szakértője. Jogi tanulmányait a Pázmány Péter Katolikus Egyetem Állam- és Jogtudományi Karán végezte, ahol 2022-ben szerzett doktori fokozatot. Fő kutatási területei a szólásszabadság és a médiajog, valamint az online platformokon való véleménynyilvánítás szabadságával kapcsolatos kérdések.

Pünkösty András 2006-ban végzett jogászként a Pázmány Péter Katolikus Egyetemen, 2010-ben elvégezte a University of Cambridge kihelyezett angol és EU-jogi képzését, majd 2014-ben doktori fokozatot szerzett a Pázmányon. 2009–2013 között ügyvédjelölt, illetve a Nemzetgazdasági Minisztériumban EU-referens. 2013-tól 2018-ig a Gazdasági Versenyhivatal munkatársa. Jelenleg adjunktus a PPKE Európai Jogi Tanszékén, valamint kutató az egyetem Versenyjogi Kutatóközpontjában és tudományos munkatárs a Nemzeti Közszerződési Egyetem Információs Társadalom Kutatóintézetében.

Sorbán Kinga a Nemzeti Közszerződési Egyetem Információs Társadalom Kutatóintézetének kutatója, fő kutatási területei a platformszabályozás, valamint a tartalommal összefüggő kiberbűncselekmények. 2018 júniusáig a Nemzeti Média- és Hírközlési Hatóság nemzetközi kapcsolattartásért felelős munkatársaként médiaszabályozással kapcsolatos ügyekben látta el a hatósági álláspont képviseletét az Európai Unióban és nemzetközi szervezetekben. Jogi diplomáját 2013-ban az Eötvös Loránd Tudományegyetemen szerezte, 2018-ban a Pécsi Tudományegyetem infokommunikációs szakjogász képzésén LL.M. címet szerzett. *Az internetes közvetítő szolgáltatók szerepe és felelőssége az informatikai bűncselekmények nyomozásában* című értekezésével 2022-ben PhD-fokozatot szerzett, ugyanebben az évben jogi szakvizsgát tett.

Szabó Endre Győző jogász, a Nemzeti Adatvédelmi és Információszabadság Hatóság elnökhelyettese, az Eötvös József Kutatóközpont Információs Társadalom Kutatóintézetének kutatója. Kutatási területe a privacy és az új technológiák, továbbá az adatvédelem szintjének elemzése.

Török Bernát 2003-ban szerezte jogi diplomáját a Pázmány Péter Katolikus Egyetemen. Előbb az Országos Rádió és Televízió Testület munkatársa, majd 2010 és 2018 között az Alkotmánybíróság főtanácsadója volt. 2016–17-ben a Yale Law School vendégkutatójaként dolgozott. Doktori fokozatát 2018-ban szerezte. Az NKE ÁNTK Alkotmányjogi és Összehasonlító Közjogi Tanszékének docense, és az Információs Társadalom Kutatóintézet vezetője. Kutatási területe a szólásszabadság és az információs társadalom alapjogi kérdései.

Zódi Zsolt jogász, az NKE tudományos főmunkatársa, diplomáját a Miskolci Egyetemen, PhD-fokozatát a Pécsi Tudományegyetemen, habilitációját az ELTE-n szerezte. Húsz éven át dolgozott az elektronikus jogi kiadás területén. Jelenlegi kutatási területei az információs társadalom szabályozási kérdései, jogi technológiák, és szövegempirikus jogi kutatások. Két monográfia és több mint száz tanulmány és könyvrészlet szerzője.

Bevezető

Társadalmat és jogot felforgató technológiák

„Felforgató technológiák” – a legújabb technológiákra már azelőtt ráaggatták ezt a hangzatos, sommás jelzőt, hogy valójában átértékeltük volna, milyen mélységben változtatják meg egyéni és társadalmi életünket. Érezhető volt azonban, hogy az egyre hőmpölygő innováció nem csupán lehatárolható részterületeken vagy egy-egy fontos kérdésben hozhat majd újítást, hanem egész struktúrákat törölhet el, vagy írhat át úgy, hogy az, ami a korábbi működési mechanizmusok helyén létrejön, radikálisan új kérdéseket vet föl. Valóban így lett, és ennek most már tanúi, résztvevői vagyunk: haszonélvezői és elszenvedői egyszerre. Nehezen vitatható, hogy az előttünk álló évek, évtizedek, sőt korszak egyik legnagyobb stratégiai kihívása a minket körülvevő technológiai fejlődés kordában tartása lesz – nem abban az értelemben, hogy miként fékezzük azt le, hanem hogy miként garantáljuk további biztonságos folyását. Elsődleges feladattá vált, hogy a mindent átszövő információs hálózatainkra, az egyre összetettebbé váló online tereinkre, valamint a folyton-folyvást újat hozó technológiákra ne az öncélú technikai haladás termékeiként tekintsünk, hanem életünk kibontakoztatásának szolgálatába állítsuk őket.

Korunk társadalmát információs társadalomnak szokás nevezni. A kifejezés abban a tekintetben mindenképpen jól ragadja meg a társadalmi-gazdasági folyamatok ismertetőjegyét, hogy egyéni és közösségi életünkben is meghatározó szerepet játszik a rendelkezésre álló információknak az a bősége, amelyet az egyre terjedő digitalizáció termel. Újabb és újabb technológiák és eszközök működésének válik lényegévé a nagyvilág, illetve személyes szféránk valamennyi részletének rögzítése digitalizált adat formájában, hogy aztán e rögzített adatokat a maguk funkciója szerint rendszerezze, felhasználják.

Kötetünknek, amely a digitalizáció társadalmi hatásainak fontos aspektusait tárgyaló írásokat fog össze, a *Digitalizálódó társadalom* címet adtuk. A cím egyrészt leíró jellegű, és nyomatékosít: bár jó pár éve benne élünk dolgaink digitalizálásának folyamatában, ez a folyamat most ért oda, hogy egy mindent átszövő digitális életről beszélhetünk. Az egyébként is feltartóztathatatlan digitalizáció a koronavírus-járvány révén még nem várt, brutális erejű ösztönzést is kapott, amelynek hatására a társadalmak olyan területeken, illetve oly mértékben tértek át az online eszközök használatára, ami korábban elképzelhetetlen volt. Olyannyira így van ez, hogy felmerül a kérdés, nem kellett volna-e már inkább „digitalizált”, nem pedig „digitalizálódó” társadalomról szólni a kötet címében. Jóllehet a technológiai folyamatok állása alapján akár már ilyen címadás is indokolt lett volna, címünk e tekintetben már nem leíró jellegű, hanem értékvalasztást jelez. Nem gondoljuk ugyanis, hogy a legújabb technológiai vívmányok kiterjedt használata egyet jelenthetne egy teljes mértékben digitalizált vagy digitalizálódó, minden elemében gépek által vezérelt

társadalommal. Fontos észben tartanunk, hogy társadalmi életünk számos eleme, sokszor éppen közös dolgaink lényege nem transzformálható digitális adattá, és még ott is, ahol a digitalizáció nagy szolgálatunkra van, szükség lehet a digitalizáció hatékonyságán túli megfontolások érvényesítésére.

A minden korábbinál szédületesebb tempóban zajló technológiai fejlődés páratlan lehetőségeket hozott, és az emberi élet megszervezésének minden eddiginél tudatosabb és hatékonyabb módszereivel kecsegtet. Mára azonban az is napnál világosabbá vált, hogy nem a Kánaán érkezett el, hanem olyan új lehetőségek nyíltak meg, amelyek új kockázatokat is jelentenek, sok esetben ráadásul az előnyökhöz képest is jelentős méretű kockázatokat. Ahhoz, hogy az emberi tudás által életre hívott potenciált biztonságosan a magunk javunkra tudjuk fordítani, a társadalom egészének odafigyelésére és erőfeszítésére van szükség.

A digitalizáció feltartóztathatatlan folyamata életünk minden szegmensét maga alá gyűri: az állam, a társadalmi élet, a gazdaság, az energiaellátás, az egészségügy, az élelmezésünk és a szórakozásunk, sőt – ahogy sajnos az elmúlt időszakban ezt is közelről szemlélhettük – a háborúzás is egyre inkább digitális formát ölt. A minket körülvevő tárgyakból, eszközökből egyre több az „Internet of Things” körébe tartozik, ami azt jelenti, hogy a kibertérbe (is) kapcsolódva szolgálja jólétünket. Ha viszont életünk egyre jelentősebb része fordul meg az ilyen-olyan internetes platformokon, akkor abból egyenesen következik, hogy értékeinket és érdekeinket is egyre nagyobb részben ott kell megvédenünk. A minket jól szolgáló körülményeket ott kell kialakítani, ahol jelen vagyunk – ha a mindennapjainkat befolyásoló információk és cselekvések a virtuális térből származnak, vagy azon keresztül jutnak el hozzánk, akkor ott kell nagyon is reális jólétet teremtenünk. A magyar kibertér szabad, demokratikus, jogállami és biztonságos berendezése éppoly alapvető feladat, mint korábbi életterünk ilyenként való megőrzése.

Ez a világos célkitűzés azonban borzasztóan összetett és nehéz feladattá vált az életünket, korábbi társadalmi struktúráinkat valóban felforgató vívmányok közepette. A felforgatás egyik eleme ugyanis éppen az, hogy a korábbi módszerek és mércék, amelyekkel kialakítottuk a követendőnek tartott társadalmi rendet, sok területen nem hatékonyak, vagy egyáltalán nem alkalmasak az új környezet kellő mértékű befolyásolására. Másképpen fogalmazva: felforgatódott a jog is. Annak demonstrálására, hogy a legújabb technológiák tényleg felforgató erejűek, elég ránéznünk a társadalmi rend alapjait lefektető alkotmányjog pillanatfelvételére. A modern alkotmányok abból a célból jöttek létre, hogy világosan meghatározott keretek közé tereljék az államhatalom működését, így biztosítva mindenekelőtt a polgári szabadságjogok gyakorlásának lehetőségét. Az alkotmánynak ebből a rendeltetéséből adódóan a szabályai az államot és annak szerveit kötelezik: megmondják, hogyan kell eljárniuk, meddig terjed a közhatalmuk, és mit kell tenniük az emberi jogok megfelelő garantálása érdekében. A magánszereplők e jogviszonyokban a jogosulti oldalon helyezkednek el: elvárhatják, hogy az állam betartsa a működésére vonatkozó előírásokat, és tiszteletben tartsa magánszférájukat és polgári jogait.

Az alkotmányjog tehát olyan vertikális hatályú normák rendszere, amelyek a közhatalom gyakorlója és az állampolgár közti viszonyt szabályozzák. Az európai jogfejlődés ezt a vegytiszta képletet az utóbbi évtizedekben már meghaladta, és – elismerve, hogy életünkre és jogaink érvényesülésére korántsem csak az államhatalom lehet meghatározó befolyással – egyes alapjogok tekintetében túllépett a jogok vertikális hatályának körén. Az alapjogok horizontális hatályán ehhez képest azt értjük, amikor a polgár az alkotmányos jogainak a védelmét nem az állammal, hanem másik magánféllel szemben igényelheti. Az európai jogrendszerek bizonyos körben már bevett gyakorlatként ismerik el az alapjogok horizontális hatályát. Mindenekelőtt a hátrányos megkülönböztetés tilalma volt az az alkotmányos előírás, amelynek a hatályát a törvényhozások a társadalom széles körében elismerték, egyes magánviszonyokban is előírva az egyenlő bánásmód kötelezettségét. Hasonló folyamat játszódott le a személyes adatok védelméhez való joggal is: az állam kötelezettségeként induló szabály ma már a legszélesebb körben kötelez mindenkit, aki mások adatait kezeli.

A digitalizáció kiteljesedése, különösen pedig az arra épülő automatizáció áttörést látszik hozni az alkotmányjog világában. Azok a szabályozások, amelyek fókuszában az algoritmusok és mesterségesintelligencia-rendszerek állnak, széles körű alapjogi követelményeket támasztanak a legújabb technológiákat fejlesztő vagy alkalmazó magánszereplőkkel szemben. A törekvés egyfelől tökéletesen érthető: ha azt akarjuk, hogy az offline világban hosszú fejlődés alatt kidolgozott alkotmányos értékeink az online életünket is meghatározzák, akkor valamilyen módon az utóbbi szférában meghatározó befolyással bíró szereplők tevékenységét is szolgálatukba kell állítanunk. Másfelől viszont az válik majd kulcskérdéssé, hogy pontosan milyen módon tesszük ezt meg. Nem lehet ugyanis szó arról, hogy az államhatalom működésére vonatkozó követelményrendszert „ráeresztjük” a tevékenységük bizonyos részében hatalmi jellegű pozícióban lévő magánfelekre. Hogy pontosan milyen formában, milyen jogi mércék alkalmazásával kell kiterjeszteni rájuk e követelményeket ahhoz, hogy meghatározott társadalmi célok elérését szolgálják, az működésük és társadalmi hatásuk megértésének és pontos leírásának függvénye. Ebben a feladatban van nélkülözhetetlen szerepe a tudományos kutatásnak. Többről van szó, mint a korábban is nyilvánvaló összefüggésről, amely szerint a társadalmi haladás nem képzelhető el a tudományos élet munkásai nélkül. A hihetetlen mértékben felpörgött, változékony információs társadalomnak ugyanis már a mindennapok vitéléhez szükséges megértése terén is rá vagyunk szorulva a folyamatokat időszérien és összetetten elemző kutatásokra és az azok eredményét feldolgozó oktatásra, ismeretterjesztésre.

A Nemzeti Közszolgálati Egyetem Információs Társadalom Kutatóintézetének újabb tanulmánykötete a társadalom digitalizálódásának néhány kiemelt területét vizsgálja. Noha a tanulmányokat négy tematikus részbe válogatva adjuk közre, valószínűleg fontosabbak azok a szempontok, amelyek összekötik őket. A szerzők ezúttal a legújabb technológiák társadalmi aspektusára fókuszálnak, és azt kutatják, milyen

hatásokkal jár az átható digitalizáció a társadalmi életünk működési mechanizmusaira, alapelveire, értékeire, szabályozási megoldásaira. Miben hoznak előrelépést, hogyan mozdítják elő például demokratikus céljainkat? Mire kell azonban vigyáznunk, és milyen új megoldásokkal kell biztosítanunk korábbi értékeink további érvényesülését egy teljesen megváltozott környezetben? Mit kell esetleg elengednünk eddigi gondolkodásunkból? Hol van szükség új szemléletmódra ahhoz, hogy eddigi társadalmi eredményeinket megtartsuk, továbbfejlesszük?

A kötet első része a digitalizációnak az állam működésére gyakorolt egyes hatásaival foglalkozik. Czékmann Zsolt és Czibrik Eszter azt elemzi, milyen viszonyban áll az automatikus döntéshozatali eljárás a meglévő törvényi alapelveinkkel: a tisztességes ügyintézéshez való joggal, a hatékonyság elvével, a hivatalbóliséggel, a jogorvoslathoz való joggal, illetve az észszerű időn belüli eljárással. Írásukban megjelennek az állami eljárások digitalizálása mögötti jogpolitikai megfontolások, érzékeltetve, hogy a rendelkezésre álló lehetőségek további kihasználásával új dimenziók nyílhatnak még meg az állami eljárások előtt. Bencsik András egyes releváns közigazgatási tevékenységfajták digitalizálásának feltérképezésével foglalkozik, külön érintve a mesterséges intelligencia lehetséges alkalmazási köreit. A szerző kifejti álláspontját abban a kérdésben, hogy a közigazgatás indokolási kötelezettsége mellett egyáltalán van-e reális lehetőség jelentős digitalizálásra, és szól arról is, hogy az eddigi folyamatok centralizációhoz vagy decentralizációhoz vezettek-e. Írásából kitűnik, az elmúlt évek kihívásai (különösen a pandémia) miként készítették a közigazgatást arra, hogy proaktív módon használja ki a digitális infrastruktúrákat. Kántor Ákos szélesebb kontextusba helyezve elemzi, milyen fejlemények figyelhetők meg a magyar jogalkotás digitalizálása terén. Egyrészt ismerteti a folyamatok társadalmi környezetét, rámutatva például arra, hogy bár a magyar internetezők uniós összehasonlításban is nagy arányban veszik igénybe az e-kormányzat szolgáltatásait, a magyar lakosság digitális készségei összességében mégis elmaradnak az uniós átlagtól. Az írás másrészt rámutat azokra a pontokra, amelyekben a digitalizáció egy mégoly humán tevékenység, mint a jogalkotás területén is nagyon jó szolgálatot tehet a társadalomnak, előmozdítva többek között a jogalkotásban való társadalmi részvétel ügyét. Kelemen Roland azzal a nagy horderejű tendenciával foglalkozik, hogy az újabb technológiai eszközök megteremtették annak lehetőségét, hogy egyes társadalmi hálózatok (például ideológiai alapú transznacionális szerveződések) már egy társadalmi totalitáson túli társadalmi struktúrához képest definiálják magukat. Ennek hatására a nem vagy kevésbé demokratikus államok a totális kontroll irányába mozdultak el, a jogállami keretek között mozgó államalakulatok viszont inkább az egyéni tudatosság erősítése mellett törtek lándzsát. Álláspontja szerint azonban a deklarációk szintjét már a nyugati demokratikus alapokon nyugvó államoknak is meg kell haladniuk, mivel a tényleges cselekvés hiányában behozhatatlan stratégiai hátrányba kerülnek.

A kötet második része a társadalom digitális átalakulásának kulcsszereplőire, az online platformokra fókuszál. Zódi Zsolt három dilemmát elemez, amelyek

minden bizonnyal az új platformszabályozások mellett is velünk maradnak. Egyrészt az uralkodó szabályozási megoldások közül érinti az *ex ante* jellegű szabályok túlburjánzásának hátulütőit, és kérdéseket vet föl az általános monitorozási kötelezettséghez való szabályozó viszonytal kapcsolatban. Másrészt megvizsgálja az adatokhoz való hagyományos jogi hozzáállás fenntarthatóságát, harmadrészt pedig kulcsfontosságú tisztázó gondolatokat fogalmaz meg a platformok és az államok viszonyával kapcsolatban. Detrekői Zsuzsa az Európai Unió szerzői jogi irányelve 2019-es implementációjának következményeit elemzi a videómegosztó platformok vonatkozásában, kiemelve, hogy az új szabályok nemcsak a nagy nemzetközi platformok, hanem a helyi kis szolgáltatók életét is jelentősen befolyásolják. A tanulmány annak lehetséges gyakorlati problémáit tárja fel, hogy az irányelv megszünteti a felhasználói tartalmak esetén a felelősségkorlátozás intézményét, és közvetlenül felelőssé teszi a szolgáltatókat a felhasználók cselekedeteiért. Klein Tamás azt a fentebb említett európai alkotmányjogi fejlődést vizsgálja a digitális szolgáltatásokat szabályozó uniós rendelet (DSA) példáján keresztül, amely a meghatározó piaci szereplőket alapjogi szemlélettel szabályozza. Tanulmányában amellet érvel, hogy a DSA sajátos, az európai alkotmányos hagyományokra építő megoldást talált, és olyan szabályozást alkotott, amely azon túl, hogy figyelembe veszi a belső piac működési elveit, az alapvető jogok védelmét is előtérbe helyezi. A szerző mindamellet hangsúlyozza: azt, hogy a DSA alapvető jogok érvényesülését biztosítani hivatott megoldásai mennyire lesznek hatékonyak, a rendelet alkalmazhatóságának a kezdete előtt nem lehet megjósolni. Papp János Tamás tanulmánya az online szűrőbuborékok és visszhangkamrák koncepcióival és azok empirikus alátámasztásának hiányával foglalkozik. A szerző szerint a buborékok vagy visszhangkamrák léteznek, társadalmi jelentőségük és az általuk okozott lehetséges társadalmi károk valódiak, azonban az a gondolat, amely az online platformokat hibáztatja ezek kialakulásáért, nem igazolható tudományos kutatásokkal. A napjainkban is egyre inkább tapasztalható társadalmi polarizálódás a hagyományos és az online média kölcsönös együtthatásaként jött létre, és az ellene való küzdelemben a legalkalmasabb eszköz talán a minőségi, objektív újságírói tartalmak előállításának támogatása lehet, amely által nehezebbé válik a párhuzamos nyilvánosságok elkülönítésének fenntartása. Csudai Tünde szintén a társadalmi kommunikáció körében azt vizsgálja, hogy a tájékoztatási piac struktúrája az internet térhódításával és az ott alkalmazott új technológiákkal radikálisan megváltozott, és folyamatosan változik. A tanulmány rámutat arra, hogy a jogalkotó számára jelenleg nagy kihívást jelent egy hatékonyan működő demokratikus médiarendszer kialakítása, hiszen az eddig már ismert médiapiacot és sajtót illető általános fogalmak jelentéstartalmai sem egyértelműek. A szerző álláspontja szerint a tájékoztatási piacon jelentkező változásokra tekintettel újfent meg kell vizsgálni, hogy az Alaptörvényben deklarált demokratikus közvélemény kialakulásához szükséges pluralizmus mint alapfeltétel milyen mértékben, milyen feltételekkel érvényesülhet a tartalomterjesztés innovációja következtében. Kéringer Szabolcs arra irányítja figyelmünket, hogy míg az Európai Unió az egységes online

piac szabályozási kereteinek megalkotásán dolgozik, addig a tagállamok is szolgáltatnak példákat a platformszabályozás megvalósítására, és szabályozásaik iránya és tartalma jelentősen különbözhetnek is egymástól. A tanulmány a NetzDG elmúlt öt éve alapján vizsgálja meg, hogy ugyanarra a problémára Németország és közvetlen szomszédai mennyire eltérő módon reagálnak.

A kötet harmadik része a digitalizáció kulcselemét és a szabályozási erőfeszítések egyik központi tárgyát: az adatot állítja a középpontba. Azt a kérdést, hogy az adatokhoz való jogi hozzáállásunk kiegészítésekre (vagy akár reformra is) szorulhat, a kötet korábbi írásai is (különösen Zódié) felvetik, a harmadik rész tanulmányai kifejezetten olyan témákat érintenek, amelyek az adatokat érintő szabályozások legaktuálisabb problémái közé tartoznak. Menyhárd Attila az egészségügyi adatok jogi természetének nagy jelentőségű, egyre sürgetőbb kérdését elemzi. Felhívja a figyelmet arra, hogy bár az egészségügyi adatok kapcsán szinte természetesen adódik a közvélekedés számára, hogy érzékenységük miatt feltétlen védelmet kell kapniuk, az egészségügyi adatok sajátossága az is, hogy a felhasználásukkal mások életének vagy egészségének a védelmét lehet hatékonyabbá tenni. A felhasználás viszont olyan piaci szereplők közvetítésével valósul meg, akiknek a számára ez haszonszerzéssel járó üzleti tevékenység, miközben a felhasználás közérdek is. Ezért már önmagában annak a kérdésnek a megválaszolása is jogpolitikai döntést igényel, hogy az adatjogosult megtagadhatja-e az adatainak a továbbításához és feldolgozásához való hozzájárulást akkor, ha ezek másokat, vagy esetleg a társadalom szélesebb körét segítik a gyógyulásban vagy abban, hogy csökkentsék a megbetegedés kockázatát. Pünkösty András a nagy adathalmazokkal kapcsolatos etikai dilemmákat rendszerezi, aminek során kitér az üzleti etika, alkalmazott etika szempontjai mellett az akadémiai adatetika megalapozásának igényére is. A szerző amellet érvel, hogy az adatetika művelése hozzájárulhat a technológiával kapcsolatos helyes bizalom kialakításához, egyúttal fontos hozzájárulást jelent a megfelelő technológiai szabályozás megalkotásához. A tanulmány azzal az alapvető kérdéssel szembesít minket, hogy vajon a technológia és a tudomány fejlődésével együtt halad-e az etikai gondolkodás fejlődése? Nogel Mónika az egészséghez való jog és egyéb emberi jogok és a demokrácia közötti nyilvánvaló összefüggésekre irányítja a figyelmünket. Az egészségegyenlőtlenségek növekedése súlyosan veszélyezteti az ország gazdasági teljesítményét, hosszú távú társadalmi fejlődését, ezért ezeknek az egyenlőtlenségeknek a csökkentése a társadalom számára elengedhetetlen fontosságú. A tanulmány szerint ebbe a szoros kölcsönhatásokkal átszőtt rendszerbe kell az orvostudomány egyik legígéretesebb vívmányát, a precíziós medicinát beilleszteni úgy, hogy az állami források költséghatékony, népegészségügyi prioritásokat szem előtt tartó, méltányos felhasználásával a precíziós medicina ne szélesítse tovább az egészségügyi egyenlőtlenségeket. Domokos Márton ismét az alapjogok horizontális hatályú megjelenésének világába kalauzol minket akkor, amikor a mesterséges intelligenciával kapcsolatos emberi jogi hatásvizsgálatokról ír. A tanulmányban elemzett európa tanácsi ajánlás értelmében ugyanis a magánszektor szereplőinek is

be kell tartaniuk az állami szereplők számára az algoritmikus rendszerek folyamatos felülvizsgálatára, a demokratikus részvételre és tudatosságra, az információs önrendelkezésre, a számítási kísérletekre, a tesztelésre és az algoritmikus döntéshozatal azonosíthatóságára meghatározott előírásokat. Szabó Endre Győző az adatvédelem kérdéseit vizsgálja a metaverzum sok tekintetben futurisztikus és lenyűgöző virtuális világában, amelyben a felhasználó újszerű módon lesz képes feloldódni a digitális környezetben. Elemzésében arra jut, hogy az új technológia csak részben vet fel újszerű adatvédelmi kérdéseket.

A kötet negyedik része végül három olyan tanulmányt fog össze, amelyek a kibertér világában végzett speciális műveletekkel foglalkoznak. Sorbán Kinga arra vállalkozik, hogy jogtudományi szempontból értelmezze a hackerek tevékenységét. Tanulmányában arra jut, hogy a növekvő társadalmi támogatottság ellenére hiba lenne úgy tekinteni a hacktivistákra, mint a kibertér Robin Hoodjaira, szemben ugyanis az ártalmatlan kiberaktivisták eszköztárával, a hacktivisták eszközei jogsértőek. A szerző ugyanakkor arra is rámutat, hogy noha e cselekmények jogsértő jellege nem kérdéses, a hacktivistáknak mégsem kell különösebben tartaniuk a felelősségre vonástól, hiszen a hackercsoportokhoz köthető személyek felderítése nem egyszerű és igencsak erőforrás-igényes feladat. Bányász Péter arra a jelenségre hívja fel a figyelmünket, hogy az Ukrajna által végzett sikeres lélektani műveletek hatására fiatalok százai tettek szert támadó képességekre, megtanulták, hogyan lehet következmények nélkül behatolni védett rendszerekbe, beleértve kritikus infrastruktúrákat. Ez számos kockázatot rejt magában, amelyek közül az egyik legfontosabb szempont a „kiberönkéntesek” „pacifikálása” a háború befejezése után. A kiemelt kérdés az, hogyan lehet biztosítani, hogy ne kiberbűnözőkként folytassák, hanem etikusan használják fel képességeiket. Nyáry Gábor a kibertérben zajló, egyre intenzívebb, egyre nagyobb károkat okozó akciók kapcsán azt hangsúlyozza, hogy a kibertér, a látszat ellenére, nem valamiféle „technológiai Vadnyugat”. Léteznek normák, jól kigondolt, világos szabályok az itt zajló konfliktusokra, a követendő vagy tiltott magatartásokra, ezek azonban jórészt kényszerítő erővel nem bíró megállapodások. A digitális terekben elmérgesedő helyzet ugyanakkor a megegyezés kényszerét is magában hordozza.

Összegzésképpen elmondható, hogy kötetünk tanulmányai nagy témagazdagsággal ugyanabba az irányba igyekeznek terelni az olvasó gondolkodását: társadalmunk digitalizálódása nagy lehetőségeket hordozó adottság, az azonban már korántsem adódik magától, hogy ezeket a lehetőségeket valóban a közös javunkra aknázzuk-e ki. Örülünk a technológia vívmányainak, de ne veszítsük szem elől azokat az alkotmányos értékeket és demokratikus társadalmi érdekeket, amelyeket közös ügyeink alakítására – legyen szó analóg vagy digitális környezetről – érvényesnek tartunk.

Török Bernát

Vákát

I. rész
Állam és digitalizáció



Vákát

Nagyító alatt az automatikus döntéshozatali eljárás



Az automatikus döntéshozatali eljárás szabályozásával kapcsolatos kérdések gyakran kerültek fókusz-pontba az elmúlt években, sokan talán már „lerágott csontként” említik a témát. Ennek megcáfolására egy új szemüveget felvéve foglalkozunk az említett kérdéskörrel. Vajon ténylegesen – még kimondatlanul – mikortól beszélhetünk az automatikus döntéshozatali eljárásról, milyen szabályrendszerben érvényesül ez az eljárási típus, illetve érint-e valamilyen alapelvet vagy alapelveket a jogintézmény? Milyen jogpolitikai szándékok húzódtak meg az automatikus döntéshozatali eljárás bevezetése mögött? Ezen kérdések megválaszolása képezi a következő tanulmányunk központi elemeit.

Bevezetés

A közigazgatás digitalizációjában aktív szerepet játszik a döntéshozatal is,¹ ennek mi sem jobb példája hazánkban, mint az automatikus döntéshozatali eljárás, amely a hatályos szabályozás értelmében a leggyorsabb hatósági eljárási típusként nevesíthető. *Az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény* (a továbbiakban: Ákr.) hatálybalépésével hozott novumokkal szokták egy körben kiemelni – többek között – az automatikus döntéshozatali eljárás térnyerését is. Azonban annak szabályozása már *a közigazgatási és hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény* (a továbbiakban: Ket.) utolsó nagy módosításakor napvilágot látott. *A közigazgatási bürokráciacsökkentést érintő egyes törvények módosításáról szóló 2016. évi CXXVII. törvény* 46. § (1d) bekezdése rögzítette, hogy 2017. január 1-jét követően mely ügyekben lehet alkalmazni az automatikus döntéshozatali eljárást. A törvény összhangban *az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény* (a továbbiakban: Eüsztv.) rendelkezéseivel egy olyan emberi közbeavatkozás nélküli eljárás kereteit fektette le, amelynek technikai feltételeit az Eüsztv., a felhatalmazó rendelkezéseket a Ket., az eljárás tényleges formáit pedig az egyes szakigazgatások eljárásjogi szabályai jelentették. De vajon ténylegesen újdonságnak hatott ez az eljárás? Kérdésünkre egy „igen, de...” válasz adható, és hogy miért, ezzel foglalkozunk a következőkben.

¹ Elin Wihlborg – Hannu Larsson – Karin Hedström: “The Computer Says No!”: A Case Study on Automated Decision-Making in Public Authorities. In *2016 49th Hawaii International Conference on System Sciences*. IEEE conference proceedings, 2016. 2903–2913.

Az automatikus döntéshozatali eljárásról

Az automatikus döntéshozatali eljárás a Ket.-ben történő bevezetését követően még egy évig volt hatályban, így ebből kifolyólag a három eljárási fajtát a Ket., mintegy pilot üzemmódban csupán rövid ideig tartalmazta,² majd az Ákr. 2018. január 1-jei hatálybalépésével azonos szövegtartalommal fenntartotta az automatikus döntéshozatali eljárásra irányadó eljárási szabályokat. A bevezetőben azonban feltettünk egy kérdést, hogy mikorra is datálható ténylegesen az automatikus döntéshozatali eljárás gyökereinek a megjelenése. Ehhez – úgy gondoljuk – érdemes elsőként az automatikus döntéshozatali eljárás jellemzőit röviden bemutatni.

Az Ákr. teremti meg az eljárási keretet, eszerint „automatikus döntéshozatalnak van helye, ha azt törvény vagy kormányrendelet megengedi, a hatóság részére a kérelem benyújtásakor minden adat rendelkezésére áll, vagy azokat automatikus információátvitel útján meg tudja szerezni, a döntés meghozatala mérlegelést nem igényel, és nincs ellenérdekű ügyfél”.³ 2022. január 1-jével bővült az automatikus döntéshozatallal intézhető ügyek száma azokkal az ügyekkel, amelyeknél a hatóság ugyan nem rendelkezik az ügy eldöntéséhez szükséges adatokkal, azonban azokat közvetlenül, automatikus információátadással, rendszer-rendszer kapcsolatban be tudja szerezni.⁴ Az ügyintézési határidő tekintetében egy huszonnégy órás időtartamot jelöl meg az Ákr.,⁵ amely egyértelműen a hatékonyság és az ügyfélközpontság irányába mutató rendelkezés. Mindez lehetővé teszi, hogy nagyszámú ügyben jelentősen gyorsuljon a hatósági eljárás döntéshozatali mechanizmusa, így a döntések könnyen ellenőrizhetők, és ezáltal abszolút nullára csökkenthető a döntésekben a korrupciós kockázat, emellett pedig az automatizációval érintett ügytípusokban eljáró ügyintézők tehermentesíthetők és átcsoportosíthatók más eljárások intézésére.⁶ A hatályos szabályozás értelmében az eljárás a kérelem beérkezését követő napon indul. Azonban számos esetben a hatóság már a kérelem benyújtásakor dönt, például a kormányablakokban azonnal intézhető ügyek esetében, ami kizárja, hogy az eljárás csak a kérelem benyújtását követő napon induljon, valamint az elektronikus ügyintézés terjedésével egyre inkább nő az azonnali döntéshozatallal intézhető ügyek száma.⁷ Erre tekintettel zárójeles megjegyzésként érdemes megjelölni, hogy 2023. január 1-jétől módosul akként az eljárási törvény, hogy az eljárás a kérelemnek

² Baranyi Bertold: Az automatikus döntéshozatali eljárás. In Barabás Gergely – Baranyi Bertold – Fazekas Marianna (szerk.): *Nagykommentár az általános közigazgatási rendtartásról szóló 2016. évi CL. törvényhez*. Budapest, Wolters Kluwer, 2022.

³ 2016. évi CL. törvény az általános közigazgatási rendtartásról (Ákr.) 40. §.

⁴ Ákr. Részletes Indokolása a 40. §-hoz.

⁵ Ákr. 50. § (2) bekezdés a) pont.

⁶ Pilz Tamás: Fenntarthatóság és alkalmazkodóképesség – avagy mi várhat a magyar közigazgatásra a következő években? *Pro Publico Bono*, 10. (2022), 1. 20.

⁷ Az egyes igazságügyi tárgyú, valamint kapcsolódó törvények módosításáról szóló 2021. évi CXXII. törvény végső előterjesztői indokolása a 110. §-hoz.

az eljáró hatósághoz történő megérkezésének időpontjában indul,⁸ bár ezzel a rendelkezéssel mondhatni ellentétes az a jogszabályhely, amely rögzíti, hogy az órákban megállapított határidő az okot adó cselekményt követő óra első percében kezdődik.⁹ Amennyiben nem ellentétes rendelkezésként, hanem a határozatlan jogfogalom pontosításaként értelmezzük, akkor arra a következtetésre juthatunk, hogy az ügyintézési határidő kezdete – hasonlóképp, mint a hatályos szabályozás – a kérelemnek a hatósághoz történő megérkezését követő óra első percére tehető.

Az automatikus döntéshozatali eljárás kiegészítő, garanciális szabályaként rögzíti a törvény, egyfajta „jogorvoslatként”, hogy a döntés közlését követő öt napon belül az ügyfél kérheti, hogy a hatóság a kérelmét ismételten, teljes eljárásban bírálja el.¹⁰ Bár az Ákr. kifejezetten nem rendelkezik róla, mint a Ket. korábban, azonban továbbra is csak az alapeljárásban lehet helye automatikus döntéshozatal keretében lefolytatni az eljárást, kérelemre vagy hivatalból induló jogorvoslati eljárásban nem.¹¹

A döntéshozatal módját, menetét, valamint technikáját az Eüsztv. rögzíti, eszerint „jogszabályban meghatározott feltételek fennállása esetén az elektronikus ügyintézészt biztosító szerv az eljárást automatikus döntéshozatal útján folytatja le. Az elektronikus ügyintézészt biztosító szerv automatikus döntéshozatal esetén a rendelkezésére álló, valamint az automatikus információátvitel útján megszerzett adatok alapján, emberi közbeavatkozás nélkül hozza meg a döntését és közli az ügyféllel.” A törvény lehetőséget ad arra, hogy mind kérelemre, mind pedig hivatalból lefolytassák az automatikus döntéshozatali eljárást.¹² Mindazonáltal nem lehet az általánosság szintjén meghatározni az automatikus döntéshozatali eljárás konkrét esetköreit, hiszen azok rögzítése minden esetben az egyes ágazati jogszabályok feladata.¹³ Álláspontunk szerint érdemes egy-egy példával szemléltetni a hivatalból lefolytatandó, valamint a kérelemre induló automatikus döntéshozatali eljárásokat.

Hivatalból lefolytatandó automatikus döntéshozatalra példaként hozható a *közúti közlekedésről szóló 1988. évi I. törvény* (a továbbiakban: Kkt.) és végrehajtási rendeletében rögzített eljárás. A Kkt. 21. §-a¹⁴ felsorolja, hogy a gépjármű üzembentartója

⁸ Ákr. 37. § (2) bekezdés (időállapot: 2023. január 1.). Megállapította: 2021. évi CXXII. törvény egyes igazságügyi tárgyú, valamint kapcsolódó törvények módosításáról 110. § c) pont.

⁹ Ákr. 52. § (3) bekezdés.

¹⁰ Ákr. 42. §.

¹¹ Barabás Gergely: Ákr. 39–42. §. In Barabás Gergely – Baranyi Bertold – Fazekas Marianna (szerk.): *Kommentár az általános közigazgatási rendtartásról szóló törvényhez*. Budapest, Wolters Kluwer, 2018. 313.

¹² 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól (Eüsztv.) Részletes Indokolása a 11. §-hoz.

¹³ Mátyás Ferenc: Átalakul a közigazgatási eljárás. *Jogászvilág*, 2016. szeptember 29.

¹⁴ 1988. évi I. törvény a közúti közlekedésről (Kkt.) 21. § (1) „A gépjármű üzemben tartója, illetve a 21/A. § (2) bekezdésében meghatározott esetben a gépjárművet használatra átvevő személy felel azért, hogy az általa üzemeltetett, illetve használt gépjárművel

a) a megengedett legnagyobb sebességre,

b) a vasúti átjárón való áthaladásra,

az általa üzemeltetett gépjárművel milyen szabályokat köteles betartani. Amennyiben a rendelkezéseket megszegik, közigazgatási bírság kiszabásának van helye.¹⁵ A hatályos jogszabályok nem teszik lehetővé, hogy a közigazgatási hatósági eljárásokban méltányosságot gyakoroljanak – emberileg méltányolható körülmények fennállása esetén sem –, így a kiszabott bírság redukálására vagy annak esetleges elengedésére sincs alapvetően lehetőség.¹⁶ További – témánk szempontjából releváns – rendelkezése a törvénynek, hogy a közigazgatási bírságot kiszabó, elsőfokú határozat meghozatala a törvény végrehajtási rendeletében meghatározott feltételek esetén hivatalból, automatikus döntéshozatal útján történik.¹⁷

Kérelemre induló automatikus döntéshozatali eljárásról beszélhetünk például abban az esetben, amikor az állampolgár bejelenti a személyazonossága igazolására alkalmas hatósági igazolványa elvesztését, eltulajdonítását vagy megsemmisülését, ezt követően pedig kérheti a vezetői engedélye, magánútlevele, második magánútlevele, szolgálati útlevele vagy hajós szolgálati útlevele pótlását, ha és amennyiben nem következett be az adataiban változás. Az állampolgár az elektronikus azonosítást követően elektronikus kapcsolattartás útján kezdeményezheti az elveszett, eltulajdonított vagy megsemmisült állandó személyazonosító igazolványának pótlását annak érvényességi idején belül azzal megegyező adattartalommal.¹⁸ Az állandó személyazonosító igazolvány kiadására irányuló eljárást a nyilvántartást kezelő szerv automatikus döntéshozatali eljárás útján folytatja le.¹⁹ Mind a két példánál láthattuk, hogy a felhatalmazó rendelkezéseket az Ákr. fogalmazta meg, az automatikus döntéshozatal konkrét esetkörét az ágazati törvény, valamint annak végrehajtási rendelete, a döntéshozatal technikai feltételeinek, illetve módjának tárgyában a szakigazgatási jogszabály kiutal az Eüsztv. vonatkozó rendelkezéseire. Az automatikus döntéshozatali eljárás kapcsán nem mehetünk el *az ingatlan-nyilvántartásról szóló*

- c) a járműforgalom irányítására szolgáló fényjelző készülék jelzéseire,
- d) a megengedett legnagyobb össztömeget vagy tengelyterhelést meghaladó járművek közötti közlekedésére,
- e) a gyorsforgalmi út leálló sávjának, leállóöblének igénybevételére,
- f) a behajtási tilalomra, a korlátozott övezetre (zóna), a kötelező haladási irányra,
- g) a természet védelmére,
- h) a díjköteles útszakaszok használatáért fizetendő, megtett úttal arányos útdíjra,
- i) a Nemzeti Tengelysúlymérő Rendszer keretében végzett mérés eredménye befolyásolásának tilalmára

vonatkozó – külön jogszabályban meghatározott – egyes előírások betartásra kerüljenek.”

¹⁵ Kkt. 21. § (2) bekezdés.

¹⁶ Ritó Evelin – Czékmann Zsolt: Okos megoldás a közlekedésszervezésben – avagy az automatikus döntéshozatali eljárás egy példán keresztül. *Miskolci Jogi Szemle*, 13. (2018), 2. 109.

¹⁷ Kkt. 21. § (4) bekezdés.

¹⁸ 1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról 29. § (16), (16a) bekezdés.

¹⁹ 414/2015. (XII. 23.) Korm. rendelet a személyazonosító igazolvány kiadása és az egységes arc-képmás- és aláírás-felvételzés szabályairól 17/D. §.

2021. évi C. törvény új szabályozása mellett, hiszen a jövő év februárjában hatályba lépő törvény széles körben kívánja biztosítani az automatikus döntéshozatali eljárás alkalmazásának lehetőségét. A törvény felhatalmazza a végrehajtási rendeletét, hogy meghatározott esetekben és feltételekkel automatikus döntéshozatalnak legyen helye.²⁰ A hatályos ingatlanügyi eljárásokban csak a tulajdoni lapról elektronikus dokumentumként szolgáltatott hiteles és nem hiteles tulajdonilapmásolat-szolgáltatás teljesítése során járt el az automatikus döntéshozatali eljárás szabályai szerint a földhivatal, jövő évtől kezdve azonban ezen a helyzeten változtatott a jogalkotó.²¹ Mindazonáltal hangsúlyoznunk kell, hogy a tanulmányunk készítésekor a törvény végrehajtási rendelete nem látott napvilágot, így a konkrét esetkörökről nem tudunk még beszámolni.

Egyfajta változásként lehet rögzíteni, hogy míg a Ket. a sommás eljárás speciális típusaként tartotta számon az automatikus döntéshozatali eljárást,²² addig az Ákr.-ben úgymond kinőtte magát, és külön eljárási módozatként nevesíti a hatósági eljárási törvény. Az Ákr. az automatikus döntéshozatali eljárást, a sommás eljárást, valamint a teljes eljárást nevesíti eljárási módozatokként. A sommás, valamint az automatikus döntéshozatali eljárás egy hatékony, gyors, illetve észszerű határidőn belüli eljárásként jellemezhető. A teljes eljárás ehhez képest klasszikus közigazgatási eljárási formaként említhető, amelyben minden eljárási részcsелеkmény elvégezhető.²³ Alapvetően egyszerű megítélésű, tömegesen előforduló, a hatóság részéről különösebb beavatkozást nem igénylő, azaz egyfajta „önműködő” ügytípusokról beszélhetünk.²⁴ Kiemelhető ennek vonatkozásában, hogy a közigazgatási hatósági eljárásjog szabályozásának kialakításakor mindig is törekedtek olyan jogintézmények bevezetésére, amelyekkel a hatósági ügyeket gyorsan és tömegesen lehet lefolytatni, ezt az is lehetővé teszi emellett, hogy számos olyan ügytípus van, ahol nincs szükséges mérlegelésre, bizonyítási eljárás lefolytatására, vagy nincsenek ellenérdekű ügyfelek, és az eljárás nemcsak gyorsan befejezhető, hanem befejezendő is.²⁵

Hasonló jogpolitikai szándékok fedezhetők fel álláspontunk szerint az egyszerűsített döntéshozatal bevezetése mögött is. A hatályos szabályozás szerint jogorvoslatról való tájékoztatást mellőző, az indokolásban pedig csak az azt megalapozó jogszabályhelyek megjelölését tartalmazó egyszerűsített döntés hozható, ha a hatóság a kérelemnek teljes egészében helyt ad, és az ügyben nincs ellenérdekű ügyfél,

²⁰ 2021. évi C. törvény az ingatlan-nyilvántartásról 52. § (1) bekezdés.

²¹ Czékmann Zsolt – Czibrik Eszter: Az új ingatlan-nyilvántartási törvény és az Ákr. viszonya. *KözigazgatásTudomány*, 2. (2022), 1. 51.

²² Hajas Barnabás: Gondolatok az általános közigazgatási rendtartás jegyzői munkára gyakorolt várható hatásairól. *Jegyző és Közigazgatás*, 18. (2016), 5.

²³ Hajas Barnabás: Általános közigazgatási rendtartás – Ket. kontra Ákr. *Új Magyar Közigazgatás*, 9. (2016), 4. 20.

²⁴ Boros Anita: A magyar közigazgatási eljárásjog harmadik generációs törvénye: az Ákr. (II.). *Új Magyar Közigazgatás*, 11. (2018), 2. 32.

²⁵ Barabás (2018): i. m. 311.

vagy a döntés az ellenérdekű ügyfél jogát vagy jogos érdekét nem érinti, vagy ha a döntés az egyezség jóváhagyásáról rendelkezik.²⁶ Az egyszerűsített döntéshozatal bevezetése korábbra datálható, mint az automatikus döntéshozatal megjelenése, ezzel megalapozva az eljárásrendben olyan megoldásokat, ahol garanciális elemek észszerű redukálására van lehetőség. A szabályozás már az *államigazgatási eljárás általános szabályairól szóló 1957. évi IV. törvény módosításáról és egységes szövegről szóló 1981. évi I. törvény* (a továbbiakban: Áe.) rendelkezései között helyet kapott, eszerint „ellenérdekű ügyfél hiányában a kérelemnek helyt adó első fokú határozat, továbbá az egyezséget tartalmazó vagy jóváhagyó határozat indokolása és a kérelemnek helyt adó első fokú határozatban a jogorvoslatról való tájékoztatás is mellőzhető” volt.²⁷ Az Áe. vezette be ezt a nem alakszerű határozattípust. A Ket. fenntartotta az egyszerűsített döntéshozatal lehetőségét, illetve a bírói gyakorlat is formálta az érintett szabályozást, például kiemelhető a Kúria, az akkori Legfelsőbb Bíróság ehhez kapcsolódó döntése, amely szerint az egyszerűsített döntéshozatalra vonatkozó szabályokat nem lehet kiterjesztően értelmezni.²⁸

Az egyszerűsített döntéshozatal és az automatikus döntéshozatal visszavezethetők egészen a hatékonyság alapelveiben megfogalmazottakig. Az elv alapvetően egy hármas pilléren nyugszik, magában foglalja a költség-, időbeli hatékonyságot, valamint a technológiai fejlettséget. Vizsgáljuk meg, hogy mennyiben feleltethetők meg ezeknek részleteiben. A technológiai fejlettség megkérdőjelezhetetlen az automatikus döntéshozatali eljárással összefüggésben, hiszen az emberi tényező kiiktatásával születik döntés.²⁹ A költség-, illetve időbeli hatékonyság vonatkozásában a gyors ügyintézési határidő emelhető ki, illetve az a passzus, miszerint, amennyiben a hatóság nem rendelkezik minden adattal a döntés meghozatalához, azt saját hatáskörében eljárva automatikus információátvétel útján is be tudja szerezni. Mindazonáltal nemcsak a hatékonyság elve emelhető ki az automatikus döntéshozatali eljárásra vonatkozó szabályozással összefüggésben. Az ügyintézési határidő rövidségére tekintettel a jogszerűség elemeként is fémjelzett észszerű időben való eljárás elve is kimutatható a jogintézményben. A hivatalbóliság (officialitás) elve kapcsán rögzíthető – a korábbi példánkra is visszautalva –, hogy az automatikus döntéshozatali eljárást nemcsak kérelemre, hanem hivatalból is lefolytathatják.

Végül, de nem utolsósorban érdekes kérdést vet fel a jogorvoslathoz való jog kérdése. Amennyiben az automatikus döntéshozatali eljárás eredményeként hozott határozatot a képviselő-testület kivételével, helyi önkormányzat szerve vagy

²⁶ Ákr. 81. § (2) bekezdés.

²⁷ 1981. évi I. törvény az államigazgatási eljárás általános szabályairól szóló 1957. évi IV. törvény módosításáról és egységes szövegről (Áe.) 43. § (2) bekezdés.

²⁸ A Legfelsőbb Bíróság Kfv.I.35.298/2006/5. számú ítélete.

²⁹ Részletesen lásd Czékmann Zsolt – Cseh-Zelina Gergely – Ritó Evelin: Az automatikus döntéshozatal helye és szerepe a hatósági eljárásban. *KözigazgatásTudomány*, 2. (2022), 2. 40. (Az automatikus döntéshozatal folyamatábrája).

rendvédelmi szerv helyi szerve bocsátotta ki, akkor fellebbezéssel támadható, ezen esetkörökön kívül pedig a döntés véglegessé válását követően közigazgatási per indítható. Másrészt pedig álláspontunk szerint további „jogorvoslatként” értelmezhető az Ákr. azon rendelkezése, amely az ügyfélnek biztosítja azt a lehetőséget, hogy a döntés közlését követően öt napon belül kérheti, hogy kérelmét ismételten teljes eljárásban bírálja el a hatóság, amennyiben a határozat fellebbezéssel nem támadható.³⁰

Az alapelvek által érintetteket az 1. táblázat foglalja össze.

1. táblázat: Az Ákr. alapelvei az automatikus döntéshozatali eljárásban

	Ésszerű időben való eljárás elve	Tisztességes ügy- intézéshez való jog	Hatékonyság elve	Hivatalból- lóság elve	Jogorvoslatához való jog
Ákr.	24 óra	rendelkezésre álló adatok alapján történő döntés	az adatokat automatikus infor- mációátvitel útján is beszerezheti	hivatalból is lefolytatható	teljes eljárásra való áttérés
Érvényesül?	✓	✓	✓	✓	?

Forrás: az Ákr. rendelkezése (40. §) alapján a szerzők szerkesztése

Összegzőképpen rögzíthető közös ismérvként mind a két jogintézmény kapcsán, hogy esetükben a hatóság „kényszerpályára” kerül, és pusztán a jogszabályi feltételek taxatív fennállása esetén hozzák meg a döntést. Emellett hasonló szabályozási kérdésként említhető, hogy a hatóság mérlegelési jogköre is háttérbe szorul, az automatikus döntéshozatali eljárásra vonatkozó szabályozás pedig *ipso iure* ki is mondja, hogy esetében a döntés meghozatala mérlegelést nem igényelhet. Mindazonáltal a közigazgatási hatósági eljárásban egyebekben a mérlegelés kiemelt jelentőségű. Az érdemi mérlegelés folytán többféle egyaránt jogszerű, azonban célszerűségi fokában eltérő döntés születhet, aminek oka abban áll, hogy vagy a hipotézis többféleképpen értelmezhető, vagy a jogkövetkezmény ad lehetőséget többféle döntésre.³¹ A mérlegelés jogi természetéből adódóan azonban az nem értelmezhető az automatikus döntéshozatali eljárással, valamint az egyszerűsített döntéssel összefüggésben.

A következőkben egy táblázat keretében foglaljuk össze az automatikus döntéshozatali eljárásra, illetve az egyszerűsített döntéshozatalra vonatkozó szabályozást, valamint összehasonlítjuk a két jogintézmény sajátosságait, megvizsgálva azt, hogy az egyes jellemzők miképp jelennek meg egyiknél, s a másiknál.

³⁰ Ákr. 42. §.

³¹ Patyi András: *A közigazgatási működés jogi alapjai. A magyar közigazgatás és közigazgatási jog általános tanai*. II. kötet. Budapest, Dialóg Campus Kiadó, 2017. 168–169.

2. táblázat: Az automatikus döntéshozatali eljárásra és az egyszerűsített döntéshozatalra vonatkozó szabályozás összehasonlítása

Automatikus döntéshozatali eljárás	Egyszerűsített döntéshozatal
<i>Törvény vagy kormányrendelet megengedi</i>	→ Ágazati jogszabály kizárhatja az egyszerűsített döntéshozatalt (például: 2013. évi CCXII. tv. 37. § (2) bekezdés: „A mezőgazdasági igazgatási szerv egyszerűsített döntést nem hozhat.”)
<i>A hatóság részére a kérelem benyújtásakor minden adat rendelkezésre áll, vagy azokat automatikus információátvitel útján meg tudja szerezni</i>	→ Amennyiben a kérelemnek a hatóság egy az egyben helyt ad, akkor az egyszerűsített döntéshozatalhoz a hatóságnak szintén rendelkezésre áll minden adat
<i>A döntés meghozatala mérlegelést nem igényel</i>	→ Egyszerűsített döntéshozatalnál sincs helye mérlegelésnek
<i>Nincs ellenérdekű ügyfél</i>	→ Részben megfeleltethető (lásd később)
Tartalmaznia kell jogorvoslatot; az automatikus döntéshozatali eljárás eredményeként született határozattal szemben öt napon belül az ügyfél kérheti, hogy kérelmét ismételten teljes eljárásban bírálják el, valamint a döntés véglegessé válását követően közigazgatási pert indíthat (esetleg fellebbezéssel támadhatja, ha a határozatot a képviselő-testület kivételével helyi önkormányzat szerve vagy rendvédelmi szerv helyi szerve hozta például: korábbi példánkban említett közigazgatási bírság megállapításával szemben)	← <i>Jogorvoslatról való tájékoztatást mellőző</i>
A döntést indokolni kell	← <i>Az indokolásban csak az azt megalapozó jogszabályhelyek megjelölése</i>
Egyes esetkörökben az automatikus döntéshozatalnál is egy az egyben helyt ad a kérelemnek a hatóság, és bocsátja ki az alapján döntését, azonban az egyszerűsített döntéshozatalra vonatkozó ezen rendelkezés nem értelmezhető a hivatalból lefolytatandó automatikus döntéshozatal esetében	← <i>Ha a hatóság a kérelemnek teljes egészében helyt ad</i>
Ipso iure ne legyen ellenérdekű ügyfél	← <i>Az ügyben nincs ellenérdekű ügyfél, vagy a döntés az ellenérdekű ügyfél jogát vagy jogos érdekét nem érinti</i>
Automatikus döntéshozatali eljárás eredményeként hozott határozatba nem foglalhatnak egyezséget	← <i>Az egyezség jóváhagyásáról rendelkezik</i>
Automatikus döntéshozatali eljárás lefolytatásának eredményeként csak érdemi döntés, azaz határozat hozható	← <i>Az önálló jogorvoslattal nem támadható végzésről az indokolásban csak az azt megalapozó jogszabályhelyek megjelölését tartalmazó egyszerűsített döntés hozható</i>
Σ Mindkét jogintézmény szabályozása kapcsán megállapítható, hogy a hatékonyság figyelhető meg mögötte, azonban tartalmilag nem fedik teljes egészében egymást, de találunk közös szabályozási pontokat.	

Forrás: az Ákr. rendelkezései [40. §; 81. § (2) bekezdés] alapján a szerzők szerkesztése

Az egyszerűsített döntéshozatal már kiállta az idők próbáját, ezért releváns az összevetés, és az automatikus döntéshozatal alapvető megfeleléséhez kiindulási alapként tekintünk rá.

Az automatikus döntéshozatal esetében szükséges még rögzítenünk, hogy habár a technológiai fejlődéshez és digitalizációhoz közvetlenül kapcsolódó jogfejlesztési megoldás álláspontunk szerint nem érvényesül maradéktalanul ebben az esetben az e-kormányzati megoldásokra jellemző transzformatív jelleg.³² Az alapjogviszonyban szigorúan technikai megoldásról van szó infokommunikációs eszközökkel, nem minőségi változásról például a felek jogaiban és kötelezettségeiben.³³

Zárásgondolatok

Tanulmányunkban az automatikus döntéshozatali eljárás mibenlétét és az alapelvekhez való viszonyának körbejárását céloztuk meg, ennek keretében feltártuk az automatikus döntéshozatali eljárás, valamint az egyszerűsített döntéshozatal szabályozása mögött meghúzódó jogpolitikai okokat, kiemeltük a közös, illetve egymásba nem illeszkedő jellemzőket. Megvizsgáltuk a gyakran nem méltóképp emlegetett alapelveket is, hogy azok miképp érvényesülnek az automatikus döntéshozatal során. Összegzésképpen elmondható, hogy az automatikus döntéshozatallal kapcsolatos szabályozás a 21. század elvárásainak megfelelő tartalommal rendelkezik, de számos olyan lehetőséget tartogat még, amelyek új dimenziót nyithatnak az eljárási rendszerünkben például az okosszerződések terjedésével.

Felhasznált irodalom

- Boros Anita: A magyar közigazgatási eljárásjog harmadik generációs törvénye: az Ákr. (II.). *Új Magyar Közigazgatás*, 11. (2018), 2. 31–40.
- Czékmann Zsolt – Czibrik Eszter: Az új ingatlan-nyilvántartási törvény és az Ákr. viszonya. *KözigazgatásTudomány*, 2. (2022), 1. 42–53. Online: <https://doi.org/10.54200/kt.v2i1.33>
- Czékmann Zsolt – Cseh-Zelina Gergely – Ritó Evelin: Az automatikus döntéshozatal helye és szerepe a hatósági eljárásban. *KözigazgatásTudomány*, 2. (2022), 2. 35–47. Online: <https://doi.org/10.54200/kt.v2i2.34>
- Hajas Barnabás: Általános közigazgatási rendtartás – Ket. kontra Ákr. *Új Magyar Közigazgatás*, 9. (2016), 4. 18–25.
- Hajas Barnabás: Gondolatok az általános közigazgatási rendtartás jegyzői munkára gyakorolt várható hatásairól. *Jegyző és Közigazgatás*, 18. (2016), 5. Online: <https://jegyzo.hu/gondolatok-az-altalanos-kozigazgatasi-rendtartas-jegyzoi-munkara-gyakorolt-varhato-hatasairol-i-resz/>

³² Lásd Ugrin Emese – Varga Csaba: *Új állam- és demokrácielmélet*. Budapest, Századvég Kiadó, 2007. 222.

³³ Az ugyanakkor érdekes kérdés, hogy a gyakorlatban hogyan változik a jogalkalmazó helyzete, illetve ki egyáltalán a jogalkalmazó. Erről részletesen lásd Czékmann–Cseh-Zelina–Ritó (2022): i. m.

- Mátyás Ferenc: Átalakul a közigazgatási eljárás. *Jogászvilág*, 2016. szeptember 29. Online: <https://jogaszvilag.hu/szakma/atalakul-a-kozigazgatasi-eljaras/>
- Patyi András: *A közigazgatási működés jogi alapjai. A magyar közigazgatás és közigazgatási jog általános tanai*. II. kötet. Budapest, Dialóg Campus Kiadó, 2017.
- Pilz Tamás: Fenntarthatóság és alkalmazkodóképesség – avagy mi várhat a magyar közigazgatásra a következő években? *Pro Publico Bono*, 10. (2022), 1. 8–29. Online: <http://doi.org/10.32575/ppb.2022.1.1>
- Ritó Evelin – Czékmann Zsolt: Okos megoldás a közlekedésszervezésben – avagy az automatikus döntéshozatali eljárás egy példán keresztül. *Miskolci Jogi Szemle*, 13. (2018), 2. 104–118.
- Ugrin Emese – Varga Csaba: *Új állam- és demokrácielmélet*. Budapest, Századvég Kiadó, 2007.
- Wihlborg, Elin – Hannu Larsson – Karin Hedström: “The Computer Says No!”: A Case Study on Automated Decision-Making in Public Authorities. In *2016 49th Hawaii International Conference on System Sciences*. IEEE conference proceedings, 2016. 2903–2913. Online: <http://dx.doi.org/10.1109/HICSS.2016.364>

Felhasznált jogszabályok, jogi dokumentumok

1981. évi I. törvény az államigazgatási eljárás általános szabályairól szóló 1957. évi IV. törvény módosításáról és egységes szövegéről
1988. évi I. törvény a közúti közlekedésről
1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról
2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól
2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól
2016. évi CXXVII. törvény a közigazgatási bürokráciacsökkentést érintő egyes törvények módosításáról
2016. évi CL. törvény az általános közigazgatási rendtartásról és Indokolása
2021. évi C. törvény az ingatlan-nyilvántartásról
2021. évi CXXII. törvény egyes igazságügyi tárgyú, valamint kapcsolódó törvények módosításáról
- Az egyes igazságügyi tárgyú, valamint kapcsolódó törvények módosításáról szóló 2021. évi CXXII. törvény végső előterjesztői indokolása
- 414/2015. (XII. 23.) Korm. rendelet a személyazonosító igazolvány kiadása és az egységes arcképmás- és aláírás-felvételezés szabályairól
- Barabás Gergely – Baranyi Bertold – Fazekas Marianna (szerk.): *Kommentár az általános közigazgatási rendtartásról szóló törvényhez*. Budapest, Wolters Kluwer, 2018.
- Barabás Gergely – Baranyi Bertold – Fazekas Marianna (szerk.): *Nagykommentár az általános közigazgatási rendtartásról szóló 2016. évi CL. törvényhez*. Budapest, Wolters Kluwer, 2022.
- Legfelsőbb Bíróság Kfv.I.35.298/2006/5.

A közigazgatás esete a digitalizációval



A közigazgatás (ideértve annak szervezeti felépítését, működési mechanizmusait, valamint személyzeti kereteit egyaránt) nem marad(hat) változatlan, nem függetlenítheti magát korszakunk világának tendenciáitól, így megállapítható, hogy a közigazgatás folyamatosan mozgásban van. Korunk egyik legnagyobb kihívása a legtágabb értelemben megfogalmazott digitalizáció, amely mind a közigazgatás polgárokhoz kapcsolódó hozzáállásában, mind az infrastruktúra tekintetében újratervezést tett szükségessé a világ összes államában.

Indokolt kiemelni azt is, hogy akármennyire megkerülhetetlen a digitális robbanás megjelenése a közsférában, az eddigi tapasztalatok alapján – különösen a kelet-közép-európai térségben – nem feltétlenül beszélhetünk befejezett sikertörténetről. Ennek okai között említhető a szervezeti és eljárási szempontok egyidejű figyelembevételének nehézsége, az infrastruktúra kiépítésének lassú és költséges folyamata, valamint a változásokkal (különösen a humán erőforrást érintően) szemben megjelenő általános ellenállás, amely szintén az innováció klasszikus akadályaként említhető.

A teljesség kedvéért jelen munka szerzője azonban nem teheti meg azt, hogy ne emelje ki a közigazgatás optimális digitalizálásának vitathatatlan eredményeit, amelyek a tanulmány szempontjából is relevánsak. Abban az irányadó külföldi szakirodalom egységesnek tekinthető, hogy a bevált digitális eszközök alkalmazásának egyrészt tulajdonítható egyfajta húzóhatás, amely újabb – korábban a digitalizáció által nem érintett – ágazatokban is legitimálhatja az új technológiai eszközök alkalmazását. Ezt a hatást erősíti az az adottság, hogy a versenyszférában működő standardizált platformok és más digitális megoldások – bizonyos körben és feltételek mellett – könnyen átültethetők a közigazgatásba. Voltaképpen arról van szó, hogy ez a közvetítő jellegű, interaktivitást biztosító online értékteremtő tevékenység a „tradicionális”, offline gazdaságban is ismert jelenség, amely főszabály szerint valamely vállalkozás technológiáján és infrastruktúráján működik. Másrészt kiemelendő az is, hogy a nemzetállami és uniós közigazgatás-politika által elérendő célként deklarált célkitűzések (például ügyfélközpontúság, hatékonyság, szubszidiaritás stb.) megvalósítására és erősítésére fokozottan alkalmasakká tehetők a technológiai eszközök, különös tekintettel a közigazgatási hatósági tevékenységre és a közszolgáltatások szervezésére.

Mindezek alapján a tanulmány kísérletet tesz a közigazgatás digitalizálásának feltérképezésére, ennek keretében érinti a releváns közigazgatási tevékenységfajtákat,

sorra veszi továbbá – ezekhez kapcsolódóan – a mesterséges intelligencia lehetséges alkalmazási köreit. Jelen írás a vizsgált témakört a centralizáció és a decentralizáció elvének alakulása szempontjából is értékeli.

Kiindulópontok

A közigazgatás (ideértve annak szervezeti felépítését, működési mechanizmusait, valamint személyzeti kereteit egyaránt) nem marad(hat) változatlan, nem függetlenítheti magát korszakunk világának tendenciáitól, így megállapítható, hogy a közigazgatás folyamatosan mozgásban van. Korunk egyik legnagyobb kihívása a legtágabb értelemben megfogalmazott digitalizáció, amely mind a közigazgatás polgárokhoz kapcsolódó hozzáállásában, mind az infrastruktúra tekintetében újratervezést tett szükségessé a világ összes államában.

Indokolt kiemelni azt is, hogy akármennyire megkerülhetetlen a digitális robbanás megjelenése a közzsférában, az eddigi tapasztalatok alapján – különösen a kelet-közép-európai térségben – nem feltétlenül beszélhetünk befejezett sikertörténetről. Ennek okai között említhető a szervezeti és eljárási szempontok egyidejű figyelembevételének nehézsége, az infrastruktúra kiépítésének lassú és költséges folyamata, valamint a változásokkal (különösen a humán erőforrást érintőekkel) szemben megjelenő általános ellenállás, amely szintén az innováció klasszikus akadályaként említhető.¹

A teljesség kedvéért jelen munka szerzője azonban nem teheti meg azt, hogy ne emelje ki a közigazgatás optimális digitalizálásának vitathatatlan eredményeit, amelyek a tanulmány szempontjából is relevánsak. Abban az irányadó külföldi szakirodalom egységesnek tekinthető, hogy a bevált digitális eszközök alkalmazásának egyrészt tulajdonítható egyfajta húzóhatás, amely újabb – korábban a digitalizáció által nem érintett – ágazatokban is legitimálhatja az új technológiai eszközök alkalmazását. Ezt a hatást erősíti az az adottság, hogy a versenyszférában működő standardizált platformok és más digitális megoldások – bizonyos körben és feltételek mellett – könnyen átültethetők a közigazgatásba. Voltaképpen arról van szó, hogy ez a közvetítő jellegű, interaktivitást biztosító online értékteremtő tevékenység a „tradicionális”, offline gazdaságban is ismert jelenség, amely főszabály szerint valamely vállalkozás technológiáján és infrastruktúráján működik.² Másrészt

¹ Sajnálatos további fejlemény az is, hogy Magyarországon az utóbbi időben több olyan szakcikk is megjelent, amelyek – az elért eredmények bemutatása mellett – azt hangsúlyozzák, hogy miért nincs szükség vagy lehetőség további digitalizációra a közigazgatásban. Ebben a körben említhető – egyebek mellett – Fejes Erzsébet és Futó Iván később hivatkozott tanulmánya.

² Ennek versenyjogi aspektusairól lásd Firniksz Judit: Rangsorolás – új szabályozási igény a platformok és az információs túlerheltség korában. In Valentiny Pál et al. (szerk.): *Verseny és szabályozás*. Budapest, KRTK Közgazdaság-tudományi Intézet, 2021. 165–199.

kiemelendő az is, hogy a nemzetállami és uniós közigazgatás-politika által elérendő célként deklarált célkitűzések (például ügyfélközpontúság, hatékonyság, szubszidiaritás stb.) megvalósítására és erősítésére fokozottan alkalmasakká tehetők a technológiai eszközök, különös tekintettel a közigazgatási hatósági tevékenységre és a közszolgáltatások szervezésére. Ezzel összefüggésben szeretnék utalni az úgynevezett DESI-indexre (Digital Economy and Society Index), amely a közép-kelet-európai uniós államokat a skála utolsó harmadába sorolja különösen a közszolgáltatások hatékonyságának mutatói alapján.³

A közigazgatás tevékenységfajtái és a mesterséges intelligencia alkalmazásának lehetőségei

A közigazgatás alaptevékenységeivel összefüggésben az irányadó szervezeti jogi dogmatika különbséget tesz a közhatalmi jellegű tevékenységfajták, a szervezeti vagy tulajdonosi hatalmi pozícióból fakadó tevékenységek, valamint az úgynevezett nem hatalmi tevékenységek között.⁴ Jelen tanulmányban kizárólag a mesterséges intelligencia szempontjából releváns alaptevékenységeket (így a stratégiaalkotást, a belső folyamatok szervezését, az ügyfeleknek nyújtott tájékoztatást, valamint az érdemi ügyintézés) említem, ezekkel kapcsolom össze az MI-technológiák alkalmazási köreit.

Kiindulópontként rögzítendő, hogy a stratégiaalkotás (policy-making) inkább a kormányzati tevékenység részeként értelmezhető annak ellenére, hogy önmagában a tervezésnek megvannak a tételes jogi alapjai a közigazgatási jogban, az ügyviteli tevékenység pedig szerven belül (így nem közhatalmi aspektusban) értelmezhető. Mindezek alapján megállapítható, hogy vannak olyan mesterséges intelligencián alapuló eszközök, amelyek alkalmasak e tevékenységek támogatására (például hatásvizsgálat digitalizálása, chatbot alkalmazása, gépi látás vagy beszédértés alkalmazása), ezekre nem fordítok hangsúlyt a tanulmányban, így a következőkben az ügyfelek (állampolgárok) és a közigazgatás közötti interakciókban bevezethető technológiákra fogok kitérni.

Az érdemi ügyintézés tekintetében két kardinális kérdés fogalmazható meg, amelyek alapvetően determinálják a mesterséges intelligencia igénybevételének realitását. Egyrészt el kell határolni egymástól a hivatalból induló, valamint az ügyféli kérelemre induló hatósági eljárásokat, mivel mind az észlelés (lásd az eljárás megindulása), mint

³ The Digital Economy and Society Index (DESI). *Shaping Europe's digital future – European Union*. A hivatkozott index szerint Magyarország a 23., Szlovákia a 24., Lengyelország a 25., míg a 18. helyen álló Csehország mutat kissé jobb mutatókat.

⁴ Ennek részletes tárgyalásához lásd Szalai Éva: A közigazgatás működése, tevékenységfajtái. In Fazekas Marianna (szerk.): *Közigazgatási jog. Általános rész I.* Budapest, ELTE Eötvös Kiadó, 2015. 71–92.

a tényállás tisztázása (lásd a döntés előkészítése) szempontjából más logika alapján folytatja le ezeket a procedúrákat a közigazgatás. Ezen a ponton megállapítható, hogy Magyarországon – alapvetően a pénzügyi igazgatás területén – mindkét eljárástípus esetén léteznek működő technológiák, ezek azonban ágazatspecifikus megoldások, amelyek mind rendelkeznek valamely „gyermekbetegséggel”.

A Magyar Államkincstár használja a Téba alkalmazást,⁵ amely egy OPA-alapú informatikai keretrendszer, s ennek keretében alkalmas egyes, kérelemre igénybe vehető normatív családtámogatási eljárások automatizálására, a program hiányossága azonban abban jelenik meg, hogy az alkalmazás magyarázatadási (indokolási) funkciója jelenleg kihasználatlan. A Nemzeti Adó- és Vámhivatal több mesterségesintelligencia-alapú programot is használ, ezek közül az Eskort⁶ alkalmazás a hivatalból induló áfaellenőrzéseket támogató szakértői rendszer, amelyet már 1999-ben bevezetett az adóhatóság. A fejlesztés erénye, hogy van érdemi magyarázatadási funkciója, hátrányaként emelhető ki azonban az a sajátosság, hogy csupán egylépcsős következtetések levonására alkalmas.⁷

A másik alapvető kérdés a hatósági tevékenységgel kapcsolatban a közigazgatás döntési mozgásterére vonatkozik: ebben a tekintetben a normatív szabályozás mellett eldöntendő esetek és a mérlegelést igénylő esetek között célszerű differenciálni. Előbbi az úgynevezett jogilag kötött aktusok kibocsátását jelenti, amikor a hatóság – adott tényállás és szabályozás mellett – csupán egyfajta jogszerű döntést hozhat, ezáltal ez a jogalkalmazási mód könnyedén modellezhető, s így támogatható mesterséges intelligenciával.⁸ A mérlegelés lényegében azt a jogalkalmazási attitűdöt jelenti, amikor – a jogi szabályozás kötetlenebb volta miatt – a hatóság belátására van bízva, hogy több jogszerű döntés közül melyiket alkalmazza (például bírság összegének pontos meghatározása a minimum- és a maximumértékek között, végrehajtási mód kiválasztása stb.). A dolog természetéből fakadóan ennek modellezéséhez egyrészt a gépi tanulás és a szakértői rendszerek kombinációjára, másrészt kifejezetten sok adat feldolgozására és adatbányászati tevékenység alkalmazására egyaránt szükség van.

Ehhez a problémakörhöz kapcsolódik az érdemi határozatok „előállítás” mesterséges intelligencia segítségével, amely a magyar szabályozás tekintetében „gyerekcipőben” jár. Az okok mögött egyrészt a horizontális nézőpont hiánya és az infrastruktúra – jelen állapotában – alkalmatlansága is felhozható, a szakirodalom képviselői között azonban van olyan álláspont, miszerint éppen a közigazgatás

⁵ TÉBA – Családtámogatási ellátások folyósításának korszerűsítése. *Kormányzati Informatikai Fejlesztési Ügynökség (KIFÜ)*.

⁶ Futó Iván – Csekei Tóth Károly: E-kormányzat az APEH informatikája szemszögéből. 3.

⁷ Vö. Fejes Erzsébet – Futó Iván: Mesterséges intelligencia a közigazgatásban – az érdemi ügyintézés támogatása. *Pénzügyi Szemle*, 66. (2021), 1. Különszám. 44.

⁸ Erre hozható példaként a fentebb említett Kincstár Téba alkalmazás.

indokolási kötelezettsége miatt nincs lehetőség az automatizálásra.⁹ Azon túl, hogy a jogalkotó megnyugtatóra ez a megközelítés alkalmas, jelen tanulmány szerzője két indok miatt vitába száll ezzel az elgondolással: egyrészt – ahogy a NAV Es-korttal összefüggésben jeleztem – informatikailag megoldható a magyarázatadó funkció kialakítása, másrészt a közigazgatásban intenzíven alkalmazott formanyomtatványok felhasználásával könnyedén digitalizálható az indokolás is, így tehát emiatt nem indokolt elfordulni a további fejlesztések tervezésétől.

A közigazgatási digitalizáció „kis magyar fejlődéstörténete”

Az előzőekben áttekintettem a közigazgatás alapvető tevékenységfajtai tekintetében alkalmazható mesterségesintelligencia-alapú és egyéb olyan technológiai innovációkat, amelyek adaptációja által fokozható a közigazgatási feladatellátás hatékonysága, egyúttal a felhasználóbarát attitűd is erősíthető.

A tanulmány korábbi fejezeteiben utaltam arra, hogy a digitalizáció egyrészt megkerülhetetlen fejlesztési útként jelenik meg a közigazgatás-politika alakítói előtt, másrészt – tartalmilag – tágabb kategóriaként értelmezhető a mesterséges intelligencia alkalmazásához képest, a közigazgatás(i) működés digitalizálódása hosszabb múltra és gazdagabb eredményekre tekint vissza. A továbbiakban rövid áttekintést adok az e téren megvalósult fejlesztésekről, illetve azok értékeléséről.

Kilényi Géza professzor egyszer azt találta írni egyik tanulmányában, hogy a közigazgatás története a sikertelen reformok történetével azonosítható, amely – bár nyilvánvalóan túlzó – fontos realitásra rámutató megfogalmazásnak tekinthető. Felmerül tehát a kérdés: vajon miért áll ellen következetesen a közigazgatás a mindenkor reformfolyamatoknak, és miért maradt el eddig az áttörés a digitalizációval összefüggésben?

Az okok között első helyen szerepel az a „történelmi sajátosság”, miszerint a rendszerváltozást követően gyakorlatilag megszűntek, illetve magánkézbe kerültek azok a nagy állami intézetek és állami vállalatok, ahol jelentős nemzetközi színvonalú MI K+F-tevékenység folyt.¹⁰ A kutatók alkalmazottként helyezkedtek el, és általában külföldi cégek termékeinek értékesítésével foglalkoztak, így a mesterséges intelligencia egyik alkotóelemét képező szakértői rendszerek fejlesztése gyakorlatilag leállt. Másrészt a digitális robbanás elmaradásának oka lehetett az is, hogy hiányoztak (és bizonyos szempontból ma is hiányoznak) a hiteles „bajnokok”. Fejes Erzsébet és Futó Iván – hivatkozott művében – utal arra a jelenségre, amelynek értelmében általában az első kezdeményezés egy tudásbázisú alkalmazás megvalósítása érdekében egy szállítótól érkezik. „Amennyiben az ajánlattevő egy nagy multinacionális cég, akkor számos referenciával rendelkezett az adott

⁹ Vö. Fejes–Futó (2021): i. m. 44.

¹⁰ Ez alól a tendencia alól üdítő kivételt képez az MTA SZTAKI.

területről. Az igazi kérdés azonban, hogy kit kell meggyőzni a jövőbeli alkalmazás hasznosságáról? A potenciális szállítónak kell találnia házon belül egy »bajnokot« (»champion«) aki megérti – esetleg már ismeri a javasolt megoldásnak a lényeges működési elemeit, aki megfelelően hiteles személy és hajlandó a projekt mellé állni, akár »kampányolni« is érte.¹¹

A közigazgatás területén végbement digitalizációs kísérletekkel kapcsolatban két jogintézmény (tanulságos) bevezetését tekintem át: az elektronikus ügyintézés és az elektronikus anyakönyvi rendszert. Az elektronikus anyakönyvi rendszert az anyakönyvi eljárásról szóló 2010. évi I. törvény intézményesítette, amely – az eredeti elképzelések szerint – 2011. január elején lépett volna hatályba. A folytatás mindenki számára ismert: a jogalkotó előbb egy, majd kettő, végül három és fél naptári évvel „halasztotta el” a hatályba léptetést, így a jogszabály végül 2014. július 1-jétől lett alkalmazandó. Attól jelen munka keretei között eltekintek, hogy milyen kezdeti nehézségek voltak érezhetők az első időkben, az viszont mindenképpen beszédes, hogy milyen körülmények vezettek a halasztott hatálybalépéshez. A hatályosulás elhúzódásához két ok vezetett. Az egyik körülmény a bejegyzett élettársi kapcsolat intézményesítése volt, amelyben nem volt konszenzus a törvényt előterjesztő és a hatálybalépéskor regnáló kormány koncepciója között, így ez a (szak)politikai konfliktus is hátráltatta a végleges normaszöveg kialakulását.¹² A „csúszás” másik oka az infrastruktúra hiánya: egészen egyszerűen nem épült ki (megbízható rendszert alkotva) a jelzett határidőre az elektronikus anyakönyvi rendszer (és annak részeként a biztonsági okmánynyilvántartás), így tárgyi feltételek hiányában nem volt alkalmas a jogszabály hatályosulni.¹³

Nem volt ennél zökkenőmentesebb az elektronikus ügyintézés bevezetése sem, itt azonban még markánsabban éreztette hatását a jogalkotói „sollen” és a valóságban realizálódó „sein” között feszülő szakadék. Az első ambiciózus jogalkotási produktum a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény (a továbbiakban: Ket.) volt, amely külön címben rendelkezett az elektronikus ügyintézésről. Túl azon, hogy rengeteg technikai szabályt tartalmazott ebben a fejezetben (is) a törvény, ami miatt kritikusai „ügyintézői kézikönyvként” tekintettek rá, hamar megmutatkozott, hogy a bevezetett fejezet egész egyszerűen nem tud működni. Ehhez képest az első finomhangolásra a Ket. novella (a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény módosításáról szóló 2008. évi CXI. törvény) hatálybalépésével került

¹¹ Vö. Fejes–Futó (2021): i. m. 44.

¹² A történet korábban kezdődött: a 154/2008. (XII. 17.) AB határozat foglalkozott először a jogintézménnyel, de annak megnyugtató jogi rendezése akadálya volt az anyakönyvi törvény véglegesítésének.

¹³ Megjegyzendő, hogy a késlekedés mellett ezzel egy olyan alkotmányellenes helyzet is tovább konzerválódott, miszerint 2014-ig továbbra is törvényerejű rendelet és belügyminiszteri rendelet regulálta a tárgykört, dacára annak, hogy kizárólagos törvényhozási tárgykörrel volt szó.

sor: ekkor az eljárási kódex már csak elektronikus tájékoztatásról beszélt, a technikai jellegű rendelkezések pedig átkerültek az elektronikus közszolgáltatásról szóló 2009. évi LX. törvénybe. A végső finomítást az a módosítás jelentette, amikor már csak az alapelvek között nyert elhelyezést az ügyfél joga a hatósággal való kapcsolattartás szabad megválasztására, és csupán a hatóságok közötti kapcsolattartás tekintetében érvényesült a kötelező elektronikus út. Lényegében ezt a modellt tartalmazza a mai szabályozás is, amelynek megfelelően az alapvető szintű rendelkezések az általános közigazgatási rendtartásról szóló 2016. évi CL. törvényben, míg a technikai és egyéb részletszabályok az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvényben (Eüsztv.) kaptak helyet.

Kihívások és reakciók a közigazgatás és a mesterséges intelligencia kapcsolatában

A mesterséges intelligencián alapuló közigazgatásban (is) alkalmazható informatikai megoldások eltérő eredményességet mutatnak a különböző fejlett államok gyakorlata alapján. A külföldi példákat vizsgálva kiemelhető, hogy mind a gépi tanulás, mind a szakértői rendszerek alkalmazása nem idegen a nemzetközi szinten, különösen az angolszász államok járnak élen ezen a területen.¹⁴

Amellett, hogy a technika vívmányaival kénytelen lépést tartani az állami működés, látható az is, hogy az elmúlt évek kihívásai (például pandémia, háború, alapvető jogok korlátozása stb.) arra készítetik a közigazgatást, hogy proaktív módon használja ki ezeket a létező infrastruktúrákat. Erre lehet példaként felhozni a magyar okmányügyi igazgatásban azt a törekvést, amely a járási hivatalokban ma is megtalálható úgynevezett ügyfélhívó kioszkok mesterséges intelligenciával történő megerősítésére irányulnak, amelynek eredményeképpen – legalábbis a tervek szerint – a közeljövőben képessé válnak arra, hogy emberi tényező közreműködése nélkül megvalósulhasson a határozat jellegű okiratok (például személyi igazolvány, lakcímet igazoló okmány, vezetői engedély, útleve stb.) online kezdeményezése és kiadása.

A másik törekvés, amely áthatja a hazai kapcsolódó jogalkotást, az ügyintézési határidő rövidítésének (egyik) eszközeként tekint a mesterséges intelligencia alkalmazására. Ennek illusztrálására a korábbi hatósági eljárási törvény által intézményesített, majd a hatályos 2016. évi CL. törvény által továbbfejlesztett automatikus döntéshozatalt lehet említeni. Az alapvető elgondolás szerint az eljárás megindulásától számítva 24 órán belül megtörténik a döntéshozatal, illetve annak

¹⁴ A gépi tanuláson alapul egyebek mellett a 2017 óta létező OPSI és a BIT technológiája is, míg a szakértői rendszerek eredményes alkalmazására találunk példát Angliában (ESI), Ausztráliában (IVAG), Új-Zélandon (CSLC), illetve az Amerikai Egyesült Államokban (e-HASP2).

közlése, amennyiben a tényállás tisztázott, a szükséges információk a hatóság rendelkezésére állnak.¹⁵ E tanulmány terjedelmi keretei nem teszik lehetővé a jogintézmény átfogó értékelését, így csupán annyi megjegyzést kívánok ehhez hozzáfűzni, hogy – a GDPR rendelet fogalmi koordináta-rendszere értelmében – ez nem tekinthető valódi automatizált döntésnek, ugyanis a jelenlegi szabályozás mellett szükség van az emberi tényező jóváhagyó beavatkozására a tényleges döntés megszületéséhez.¹⁶ Ennek megfelelően nem tekinthető a mesterséges intelligencia tiszta alkalmazásának a jogintézmény, holott az irányadó jogalkalmazó tevékenység jellege (tudniillik jogilag kötött aktus kibocsátása) lehetővé tenné a teljes automatizmus alkalmazását.

Végezetül utalok arra is, hogy – a klasszikus hatósági tevékenység mellett – a közszolgáltatások szervezésével összefüggésben is kínálkozik lehetőség a mesterséges intelligencia alkalmazására (a garanciális keretek kiépítését követően). Csupán példálózva említhető a lehetséges ágazatok között a közösségi közlekedés megszervezése (itt lehetne alapozni az Uber létező platformjának működési mechanizmusaira), valamint az úgynevezett alapnyilvántartások és a közigazgatási tervezés összekapcsolása (például a születési anyakönyvi nyilvántartás a településen született gyermekek számából automatizált következtetések levonására tehető alkalmassá a bölcsődei és óvodai férőhelyek számának tervezése tekintetében).

Konklúzióként annak megfogalmazására szorítkozom, hogy vitán felül állnak a közigazgatás digitalizálásának (ebben a körben a mesterséges intelligencia alkalmazásának) a hatékonyság fokozásában vagy az adminisztratív költségek csökkentésében rejlő előnyei, kiemelendő azonban az is, hogy az ügyintézés helyének közelítése a polgárokhoz nem eredményezte a feladat- és hatáskörök decentralizálását. Épp ellenkezőleg: a közigazgatás digitalizálása a centralizáció elvének megerősítésével járt, így a mesterséges intelligencia óvatos térnyerése a központosítás folyamatával azonosítható Magyarországon.

Felhasznált irodalom

Fejes Erzsébet – Futó Iván: Mesterséges intelligencia a közigazgatásban – az érdemi ügyintézés támogatása. *Pénzügyi Szemle*, 66. (2021), 1. Különszám. 24–51. Online: http://doi.org/10.35551/PSZ_2021_k_1_2

¹⁵ Megjegyzendő, hogy az ágazati szabályozás eredetileg a hivatalból induló, egyes közlekedési szabályszegések esetén lefolytatandó eljárásokra modellezte a szabályozást, később azonban kérelemre induló eljárásokra és egyéb ágazatokra is kiterjesztette a jogalkotó (például bizonyos családtámogatások köre, nem hiteles tulajdoni lap kiállítás stb.).

¹⁶ A kérdéskör bővebb tárgyalásáról lásd Sandra Wachter – Brent Mittelstadt – Chris Russell: Counterfactual explanations without opening the black box: Automated decisions and the GDPR. *Harvard Journal of Law & Technology*, 31. (2018), 2. 461–464.

- Firniksz Judit: Rangsorolás – új szabályozási igény a platformok és az információs túlterheltség körében. In Valentiny Pál – Antal-Pomázi Krisztina – Nagy Csongor István – Berezvai Zombor (szerk.): *Verseny és szabályozás*. Budapest, KRTK Közgazdaság-tudományi Intézet, 2021. 165–199. Online: https://kti.krtk.hu/wp-content/uploads/2022/01/vesz2021_6-FirnikszJ.pdf
- Futó Iván – Csekei Tóth Károly: *E-kormányzat az APEH informatikája szemszögéből*. Online: <https://itf.njszt.hu/324rtr4/uploads/2019/06/APEHlf.doc.pdf>
- Szalai Éva: A közigazgatás működése, tevékenységfajtái. In Fazekas Marianna (szerk.): *Közigazgatási jog. Általános rész I*. Budapest, ELTE Eötvös Kiadó, 2015. 71–92.
- TEBA – Családtámogatási ellátások folyósításának korszerűsítése. Kormányzati Informatikai Fejlesztési Ügynökség (KIFÜ). Online: <https://kifu.gov.hu/projekt/teba-csaladtamogatasi-ellatasok-folyositasanak-korszerusitese/>
- The Digital Economy and Society Index (DESI). *Shaping Europe's digital future – European Union*. Online: <https://digital-strategy.ec.europa.eu/en/policies/desi>
- Wachter, Sandra – Brent Mittelstadt – Chris Russell: Counterfactual explanations without opening the black box: Automated decisions and the GDPR. *Harvard Journal of Law & Technology*, 31. (2018), 2. 873–877. Online: <https://jolt.law.harvard.edu/assets/articlePDFs/v31/Counterfactual-Explanations-without-Opening-the-Black-Box-Sandra-Wachter-et-al.pdf>

Vákát

Jogalkotás és digitalizáció – kihívások és dilemmák



A jogalkotás a demokratikus jogállam törvényhozó és végrehajtó hatalmi ágához egyaránt kapcsolódó tevékenység. A digitalizáció térnyerésével kezdetben szigetszerű megoldások születtek a jogalkotáshoz kapcsolódóan, mint az Országgyűlés ParLex rendszere, vagy a Nemzeti Jogszabálytár, azonban az eljárás – a törvénytervezet parlamenti benyújtásáig – továbbra is „hagyományos” úton haladt, a jogalkotásról szóló hatályos szabályozás napjainkban sem tartalmazza az elektronizáció nyomait.

Elméleti síkon is megállapítható, hogy a jogalkotásra vonatkozó normák leprogramozásával a jogalkotás technikai minősége, pontossága nagymértékben javítható. Vizsgálandó, hogy a jogi normáktól elvárható közérthetőségi követelményen egy ilyen rendszer tud-e javítani, valamint használatával fognak-e az adminisztratív terhek csökkenni. Ugyanakkor nem tudjuk megjósolni a jövőt. A tervezett rendszerek projektszerű agilis fejlesztése mindig függ a bennünket körülvevő technológiai fejlődéstől, lokálisan és globális szintereken egyaránt. Ehhez más államok jogalkotási rendszereinek digitalizációja is követendő, vizsgálható lehet, a nemzetközi benchmarking, a jó gyakorlatok vizsgálatának szerepe a gyorsan változó technológiai környezetben okszerű.

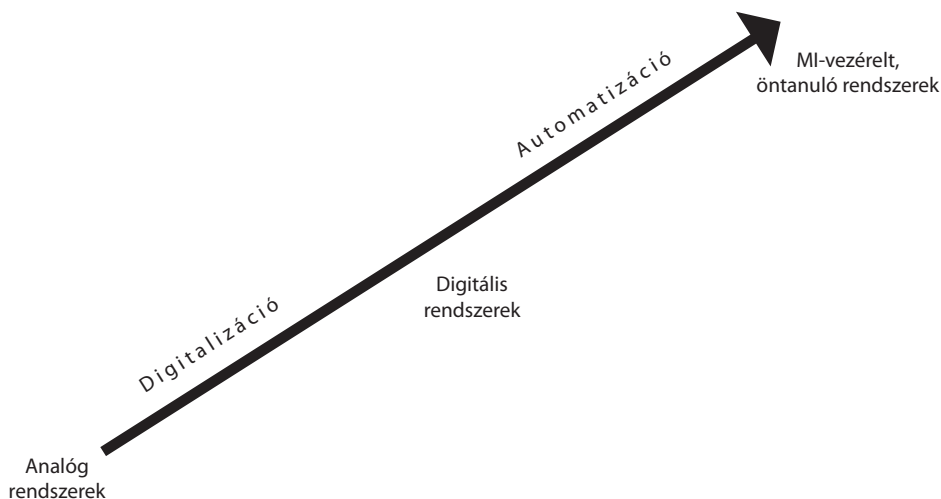
A mesterséges intelligencia a jogi szakmába is megérkezett, jellemzően felhasználói, jogalkalmazói oldalon, azonban álláspontom szerint idővel a jogalkotásban is meg fog jelenni.

Bevezetés

Tanulmányomban az új technológiák hatása a demokráciára témakörben a jogalkotás digitalizációjának mint vitathatatlanul új technológiai vívmánynak a demokráciára gyakorolt hatását kívánom vizsgálni. Ebben a körben elsőként a klasszikus jogalkotás és a demokrácia kapcsolatát mutatom be, majd a jogalkotás digitalizációjára irányuló törekvéseket vázolom fel, amelyeket a 2020-ban beköszöntött pandémia még aktuálisabbá tett. Ezután bemutatom a magyar közigazgatás válaszát a jogalkotás digitalizációjára: az Integrált Jogalkotási Rendszer projektet.

Az analóg rendszerek továbbfejlesztésének napjainkban az első lépése a digitalizáció, ennek útján válnak digitális rendszerré. Az ilyen módon digitalizált rendszerek pedig a számítógépek korában magukban hordozzák az automatizáció lehetőségét, amellyel eljuthatunk a mesterségesintelligencia-alapú öntanuló rendszerekhez. Ez a megközelítés persze leegyszerűsített, egy kisebb, használatban

levő rendszer digitalizációja évekig is eltart, akárcsak az automatizáció, amelynek kimenete többek közt a formálódó uniós jogi szabályozás miatt is bizonytalan.¹



1. ábra: Automatizációs folyamat

Forrás: a szerző szerkesztése

Bár a jogalkotás digitalizációja még a kezdeti lépéseknél tart, tanulmányomban megkísérlem a témában eddig keletkezett tapasztalatokat bemutatni, majd kis kitekintést adni arról, hogy napjaink slágertémája, a mesterséges intelligencia bekapcsolható-e a digitalizált jogalkotási folyamatba a tudomány és a jogi szabályozás jelenlegi állása mellett.

Demokrácia és jogalkotás

A demokrácia és a jogalkotás kapcsolata nem triviális, a hatalommegosztásról szóló elméletekben az egyik funkció vagy hatalmi ág a törvényhozás, amely fogalmilag szűkebb, mint a jogalkotás. A jogalkotás fogalma – bár jogszabályban nem definiált – felöleli a jogszabályalkotást, valamint a közjogi szervezetszabályozó eszközök megalkotását, a jogalkotásról szóló 2010. évi CXIII. törvény (a továbbiakban: Jat.) hatályát megállapító 1. § (1) bekezdése alapján. A jogszabályok típusait a Magyarország Alaptörvénye T) cikk (2) bekezdése sorolja fel: „Jogszabály a törvény, a kormányrendelet, a miniszterelnöki rendelet, a miniszteri rendelet, a Magyar

¹ Lásd Kántor Ákos: Ízelítő az EU formálódó mesterséges intelligencia szabályozásáról. In Miskolczi-Bodnár Péter (szerk.): *XXII. Jogász Doktoranduszok Konferenciája 2022*. Budapest, Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, 2022c. 45–61.

Nemzeti Bank elnökének rendelete, az önálló szabályozó szerv vezetőjének rendelete és az önkormányzati rendelet. Jogszabály továbbá a Honvédelmi Tanács rendkívüli állapot idején és a köztársasági elnök szükségállapot idején kiadott rendelete.”

A fentiek alapján egyedül a törvény a törvényhozó hatalom aktusa, míg a többi típusba tartozó jogszabályt a végrehajtó hatalom alkotja, ezek két típusa az alaptörvényi felhatalmazáson alapuló,² autonóm (eredeti jogalkotói hatáskörben megalkotott) rendelet, valamint a jogalkotásra irányuló konkrét felhatalmazás alapján készült végrehajtási rendelet.³

A hatalommegosztás elméletének történeti alakulásán keresztül is körvonalázódik a jogalkotás demokráciára gyakorolt hatása. A hatalom gyakorlásának fontos eleme a társadalmi normák meghatározása. „A demokrácia az emberek közötti egyenlőség felett öröklik. [...] Ugyanúgy felvetődik az egyenlőség kérdése a hatalom berkein belül, a különböző hatalmi ágak viszonyára vonatkozólag is. Ezeket a viszonyokat írja le a Hatalommegosztás elmélete.”⁴ „A hatalom megosztásának kérdése a maga tisztaságában először John Locke-nál jelentkezett.”⁵ „Locke szerint demokráciáról akkor beszélünk, ha a törvényeket időről időre a többség hozza.”⁶ „Végző soron a törvényhozó konkretizálja a társadalomban is érvényes természeti törvényeket, illetve rendel e törvények emberek általi megsértéséhez előre látható és világos szankciókat.”⁷

A jogalkotás a törvényhozó és a végrehajtó hatalom aktusa is egyszerre, ezt az összekapcsolódást már Montesquieu is vizsgálta. „Hogy a hatalommal ne lehessen visszaélni, ahhoz az kell, hogy a dolgok helyes elrendezése folytán a hatalom szabjon határt a hatalomnak”,⁸ „[a] törvényhozó és a végrehajtó hatalom viszonya. A két hatalmat személyileg szintén el kell választani egymástól; ugyanaz a személy vagy testület egyszerre mindkét állami funkciót nem töltheti be. [...] Önmagában azonban az elválasztás kevés; e két hatalom ugyanis szükségképpen hatással van egymásra – épp ezáltal képesek azon funkciójukat betölteni, hogy korlátozzák a másik hatalmi törekvéseit.”⁹

² Alaptörvény 15. cikk (3) bekezdés: Feladatkörében eljárva a Kormány törvényben nem szabályozott tárgykörben, [...] rendeletet alkot.

³ Lásd Tóth J. Zoltán (szerk.): *Jogalkotástan. Jogdogmatikai és jogszabályszerkesztési ismeretek*. Budapest, Dialóg Campus Kiadó, 2019. 103.

⁴ Horkay Hörcher Ferenc: *Előadások a XIX. és XX. század állambölcselete köréből*. Budapest, Szent István Társulat, 2001. 43.

⁵ Tóth J. Zoltán: *Demokrácia, jogállamiság és alkotmánybíráskodás*. Budapest, Patrocínium Kiadó, 2020. 74.

⁶ Tóth (2020): i. m. 74.

⁷ Tóth (2020): i. m. 75.

⁸ Montesquieu: *A törvények szelleméről*. Ford. Csécsy Imre – Sebestyén Pál. Budapest, Osiris Kiadó – Attraktor, 2000. 247.

⁹ Tóth (2020): i. m. 83–84.

Montesquieu szerint a törvényhozás – mint hatalmi ág – feladata törvények alkotása, módosítása, hatályon kívül helyezése; a törvény az állam általános akarata, míg a végrehajtó hatalom a törvényhozó hatalom által lefektetett „közhatározatokat” hajtja végre.¹⁰

A jogalkotás részben a törvényhozó hatalom, részben a végrehajtó hatalom aktusa, amely felhatalmazás alapján alkot jogszabályokat. Megjegyzendő, hogy a jogalkotás korunkban érinti az önkormányzatok normaalkotási tevékenységét is, egységes mederben halad az önkormányzatok kodifikációs tevékenysége.

A hatalommegosztás legújabb kori kérdéseivel is foglalkozott Bibó István, aki szerint „veszélyes, ha a végrehajtó hatalom belefolyik a társadalom legfőbb – törvények útján való – irányításába, (fordított irányban azonban Bibó itt sem lát veszélyt, sőt kifejezetten kívánatosnak és szükségesnek tartja a végrehajtó hatalom felelősségét és a törvényhozó szerv általi ellenőrizhetőségét)”.¹¹

Bibó vizsgálta a „bürokrácia vagy technokrácia hatalma” kérdését, amely akként körvonalazódik, hogy a modern, tudásalapú szakértő-szervező-végrehajtó apparátus képes kisajátítani az állami intézmények napi működtetését, veszélyeztetve ezzel a bürokrácián kívüli személyek ráhatását a folyamatokra – ezt Bibó a menedzserek forradalmának nevezte.¹² A jelenség napjainkban még aktuálisabb, gondoljunk arra, hogy a digitalizációval a szakmabeli tudás önmagában már nem elégséges általában egy munkakör ellátásához, hanem a szaktudás mellett olyan informatikai kompetenciákkal is kell rendelkeznie az adott szakma gyakorlójának, amelyek az általa használni előírt digitális rendszer működtetésére is képessé teszik.¹³

Mindezek alapján kijelenthető, hogy a jogalkotás mint a törvényhozó hatalom és bizonyos esetekben a végrehajtó hatalom közös aktusa¹⁴ hatással van a demokráciára. A hatás nem is a normális működés esetén érzékelhető, hanem abban az esetben, ha a hatalmi ágak egymástól való függetlensége csorbul, ezáltal a jogalkotás formálissá válik, így rontva a demokratikus elvek megvalósulását.

Jogalkotás és digitalizáció

A Kormány tagjainak feladat- és hatásköréről szóló 182/2022. (V. 24.) Korm. rendelet alapján az igazságügyi miniszter igazságügyért való felelőssége körében

¹⁰ Vö. Montesquieu (2000): i. m. 250.

¹¹ Tóth (2020): i. m. 98.

¹² Vö. Tóth (2020): i. m. 98.

¹³ Hasonlóan az elektronikus adóbevallás bevezetéséhez, amikor is a kizárólag papíralapon dolgozó könyvelők egy része – szakmai tudása és tapasztalata dacára – tovább már nem tudta korábbi tevékenységét végezni.

¹⁴ A törvényhozó hatalom feladata a jogalkotás, azonban törvényben meghatározott esetekben és módon a végrehajtó hatalom is alkot jogot.

felel a jogalkotás minőségének fejlesztéséért,¹⁵ valamint a Magyar Közlöny Lap- és Könyvkiadó Kft. útján gondoskodik a minőségi jogalkotás és a kormányzati döntés-előkészítési és döntéshozó folyamatok egységes és kizárólagos informatikai támogatását, valamint egyes kapcsolódó hatósági tevékenységek informatikai támogatását biztosító integrált jogalkotási rendszernek – a rendszert használó nem kormányzati szervek feladat- és hatáskörét nem érintő – üzemeltetéséről, működtetéséről és fejlesztéséről.

Az igazságügyi miniszter feladatkörét számos szakterületen érinti a digitalizáció: az egyik legkorábban bevezetett újítás a 2008 óta elektronikusan végzett elektronikus cégeljárás¹⁶ a cégnyilvánosságról, a bírósági cégeljárásról és a végelszámolásról szóló a 2006. évi V. törvény alapján. Tíz évvel később történt meg a polgári perek elektronizációja, amelyet a polgári perrendtartásról szóló 1952. évi III. törvény vezetett be 2016-ban,¹⁷ kötelezővé téve a polgári perek elektronikus úton történő vitelét a jogi képviselővel eljáró fél, valamint a belföldi székhellyel rendelkező gazdálkodó szervezet számára.¹⁸ Ugyancsak digitalizációs eredménytermék az igazságügyi miniszter tulajdonosi joggyakorlása alá tartozó Országos Fordító és Fordításhitelesítő Iroda Zrt. által 2017-ben bevezetett, az elektronikus eljárások támogatásához fejlesztett elektronikusan hiteles (e-hiteles) fordítás.¹⁹

Az igazságügyi miniszter szabályozási feladatkörében készíti elő a jogalkotásra, a jogszabályok előkészítésében való társadalmi részvételre vonatkozó jogszabályokat.²⁰ A jogalkotás anyagi és eljárási szabályait a következő jogszabályok tartalmazzák: Magyarország Alaptörvénye T) cikke határozza meg, hogyan lehet kötelező magatartási szabályt megállapítani. Tételesen felsorolja a jogszabályok típusait, és megállapítja, hogy jogszabály nem lehet ellentétes az Alaptörvénnyel. A törvényi szint két jogszabályból áll, az egyik a jogalkotásról szóló 2010. évi CXXX. törvény, a másik a jogszabályok előkészítésében való társadalmi részvételtől szóló 2010. évi CXXXI. törvény. A jogharmonizációval kapcsolatos szabályokat az Európai Unió jogának való megfelelés érdekében szükséges jogszabály-előkészítési feladatok teljesítéséről szóló 302/2010. (XII. 23.) Korm. rendelet tartalmazza.

¹⁵ 182/2022. (V. 24.) Korm. rendelet a Kormány tagjainak feladat- és hatásköréről 122. § (3) bekezdés a) pont ae) alpont.

¹⁶ Bővebben lásd Ormai László: A digitalizáció hatása a hazai elektronikus cégeljárásra. In Zódi Zsolt (szerk.): *Jogi technológiák. Digitális jogalkalmazás*. Budapest, Ludovika Egyetemi Kiadó, 2022. 371–399.

¹⁷ 1952. évi III. törvény a polgári perrendtartásról 340/B. §.

¹⁸ Bővebben lásd Kékedi Szabolcs – Zódi Zsolt: A bírósági informatika helyzete Magyarországon. In Zódi Zsolt (szerk.): *Jogi technológiák. Digitális jogalkalmazás*. Budapest, Ludovika Egyetemi Kiadó, 2022. 41–63.

¹⁹ Az e-hiteles fordítás elektronikus aláírással ellátott dokumentumokról készül, és kizárólag elektronikus formában vehető át (es3 vagy dosszié formátumban), tehát nincs papíralapú példánya, hiszen az elkészült fordítás elektronikus aláírással is rendelkezik: Hiteles fordítás. *Országos Fordító és Fordításhitelesítő Iroda Zrt.*

²⁰ 182/2022. (V. 24.) Korm. rendelet 121. § (2) bekezdés.

A jogszabályszerkesztésről szóló 61/2009. (XII. 14.) IRM rendelet tartalmazza a jogalkotás részletesebb, már-már technikai szintű szabályait, végül a Kormány ügyrendjéről szóló 1352/2022. (VII. 21.) Korm. határozat rögzíti a jogalkotás folyamatának eljárási szabályait.

A jogalkotás területén már korábban megindult a digitalizáció, de ahogy a közigazgatásban is, kezdetben egymástól elkülönült, szigetszerű megoldások születtek. Elsőként a 2012. január elsején indult Nemzeti Jogszabálytár említem meg, amelyet a Magyar Közlöny Lap- és Könyvkiadó Kft. üzemeltet. A portálon ingyenesen lehet hozzáférni a hatályos jogszabályokhoz, valamint 2013 júliusától az önkormányzati rendeletekhez.²¹ A Nemzeti Jogszabálytár folyamatos bővül, már egyes jogszabályok idegen nyelvű fordításait is tartalmazza.²² A Nemzeti Jogszabálytár létrehozásával keletkezett az az adatbázis, amely a jogalkotási digitalizáció egyik lába.

A jogalkotás digitalizációja szempontjából a másik fontos lépés a törvényalkotási folyamat országgyűlési szakaszát elektronizáló ParLex elektronikus irományszerkesztő és folyamatmenedzselő rendszer bevezetése volt, amelyre 2017-ben került sor. A ParLex – álláspontom szerint – a jogalkotási digitalizáció pilotrendszerének is tekinthető, hiszen a teljes jogalkotási folyamat egy részét tartalmazza, a törvénytervezet országgyűlési benyújtásától menedzseli a dokumentumokat egészen a köztársasági elnök számára aláírásra előkészített változat elkészítéséig.

A jogalkotási eljárás – a tervezet parlamenti benyújtásáig – ekkor még „hagyományos” úton haladt. A fent említett két rendszer egymáshoz nem kapcsolódott, teljesen külön dolgoztak, az adatátadás sem volt formalizált, hanem duplikáltan, aláírt papíralapú dokumentumok átadásával és szerkeszthető fájlok elektronikus úton való küldésével valósult meg. Meg kell említeni, hogy a jogalkotásról szóló – 2022 nyarán módosult – hatályos szabályozás²³ továbbra sem hordozza magán az elektronizáció nyomait.

Az IJR-projekt

Az Igazságügyi Minisztérium 2017 januárjában sajtóközleményben jelentette be, hogy az EU társfinanszírozásában megvalósuló KÖFOP-1.0.0-VEKOP-15 – 2016–00029 Az adminisztratív terhek csökkentése – Integrált Jogalkotási Rendszer (a továbbiakban: IJR) elnevezésű projekt keretében olyan fejlesztések valósulhatnak meg, amelyek célja az adminisztratív terhek csökkentése az úgynevezett belső (közigazgatáson belüli, hivatalok/állami szervek közötti) folyamatok elektronikus támogatása által.

²¹ Magyar Közlöny Lap- és Könyvkiadó – Szolgáltatások.

²² Nemzeti Jogszabálytár Jogszabályfordítások.

²³ Vö. 1352/2022. (VII. 21.) Korm. határozat a Kormány ügyrendjéről.

A projekt célja az adminisztratív terhek csökkentése volt, valamint az elektronikus közigazgatás kiépítését elősegítő környezet megerősítése. A rendszer célja hatékonyabban, szakértői támogató metódusokkal, folyamatvezérelten készülő és jobb minőségű jogszabályok alkotása. A projekt konzorciumi formában valósult meg, amelynek vezetője az Igazságügyi Minisztérium, tagjai a Magyar Közlöny Lap- és Könyvkiadó Kft., az Országgyűlés Hivatala, a Miniszterelnökség, a Nemzeti Adatvédelmi és Információszabadság Hatóság, a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. és a Kormányzati Informatikai Fejlesztési Ügynökség.²⁴

Az adminisztratívteher-csökkentési program 2006-ban került EU-szinten fókuszba, az OECD 2007-es ajánlásában²⁵ a bürokráciacsökkentés öt pillérét határozta meg, amelyek közül a harmadik az információs és kommunikációs technológiák széles körű alkalmazása. A közigazgatási IKT széles körű használata nem csupán a központi közigazgatás költségeit csökkentheti hatékonyan, hanem hozzájárulhat az alsóbb szintek adminisztratív terhei okozta többletköltségek csökkentéséhez is.²⁶

2006-ban az Európai Unió Bizottsága javasolta, hogy az Európai Tanács 2007. tavaszi ülésén 25%-os csökkentési célt tűzzön ki 2012-re, amelyet az EU és tagállamai közösen érnének el.²⁷ Ennek érdekében a 2006–2012 közötti időszakra cselekvési tervet fogalmaztak meg az adminisztratív terhek csökkentésére. „A jobb szabályozás célja, hogy mindezt úgy tegyünk, hogy annak a lehető legtöbb haszna, de a lehető legkevesebb költsége legyen. A jobb szabályozás jelentősen felfrisseníti a termelékenységet és a foglalkoztatást, így elősegíti a növekedést és munkahelyteremtést. Európában a szabályozási környezetet nemzetközi kontextusban az Unió és a tagállamok egyaránt fejlesztik – ezért a jobb szabályozás közös felelősség.”²⁸ Vagyis kevesebb adminisztratív teher mellett a vállalkozások a felszabaduló erőforrásukat a gazdasági tevékenységükre tudják fordítani, ami a gazdaság növekedését eredményezheti már rövid távon is.

Az Integrált Jogalkotási Rendszer bevezetéséről és az ahhoz kapcsolódó feladatokról szóló 1612/2019. (X. 24.) Korm. határozat rendelte el az Integrált Jogalkotási Rendszer (a továbbiakban: IJR) bevezetését, fokozatosan, 2020. augusztus 1-jétől.

A kormányhatározat az IJR következő funkcióit említi a központi közigazgatáshoz kapcsolódóan: az IJR használatával kell eleget tenni

²⁴ KÖFOP-1.0.0-VEKOP-15 – 2016-00029 Integrált Jogalkotási Rendszer sajtóközlemény. 2017.

²⁵ OECD: Cutting Red Tape: National Strategies for Administrative Simplification. 2006.

²⁶ Vö. Budai Balázs Benjámin: *A közigazgatás újragondolása*. Budapest, Akadémiai Kiadó, 2017.

²⁷ Az Európai Közösségek Bizottsága: *A Bizottság jelentése a Tanácsnak, az Európai Parlamentnek, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. Az adminisztratív terhek csökkentésének cselekvési programja az Európai Unióban*. COM(2007)23 végleges (2007. január 24.).

²⁸ Az Európai Közösségek Bizottsága: *A Bizottság közleménye a Tanácsnak, az Európai Parlamentnek, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. Az Európai Unión belüli jobb szabályozás stratégiai felülvizsgálata*. COM(2006)689 végleges (2006. november 14.).

- a) a Kormány törvényalkotási programja, jogalkotási terve és a jogszabály előkészítéséért felelős miniszter jogalkotási tájékoztatója megtervezésének és azok végrehajtása ellenőrzésének;
- b) a Kormány és a Kormány tagjai jogalkotói hatáskörébe tartozó jogszabályok és az általuk megalkotásra kerülő közjogi szervezetszabályozó eszközök és egyedi határozatok – ide nem értve a minősített adatot tartalmazó jogszabályokat, közjogi szervezetszabályozó eszközöket és egyedi határozatokat – előkészítésének;
- c) a Kormány ügyrendje és a minisztériumok, munkaszervezetek szervezeti és működési szabályzatai szerinti véleményezésnek, egyeztetésnek, valamint a szakmai és politikai döntés-előkészítő és döntéshozó szervek ülései megszervezésének, lebonyolításának és dokumentálásának;
- d) a szakmai és politikai döntés-előkészítő és döntéshozó szervek ülésein tárgyalt napirendi pontok nyomon követésének és a kiadott feladatok végrehajtása ellenőrzésének;
- e) a Kormány által kezdeményezett törvényjavaslatok és országgyűlési határozati javaslatok előkészítésének, az azokkal kapcsolatos b) alpont szerinti feladatoknak és azok Országgyűlés részére történő benyújtásának;
- f) a Magyar Közlönyben és a Hivatalos Értesítőben kihirdetésre, illetve közzétételre kerülő tartalmak kihirdetést, illetve közzétételt megelőző lektorálásának és kihirdetésre, illetve közzétételre átadásának.

Az IJR önkormányzati alrendszerére vonatkozásában az IJR útján történő megvalósításáról kell gondoskodni

- a) a helyi önkormányzati rendeletek megalkotásának; valamint
- b) a helyi önkormányzati rendeletek egységes kihirdetésének és az IJR éles üzemben történő bevezetésekor már kihirdetett és hatályos, illetve azt követően hatályba lépő önkormányzati rendeletek visszamenőleges rögzítésének.

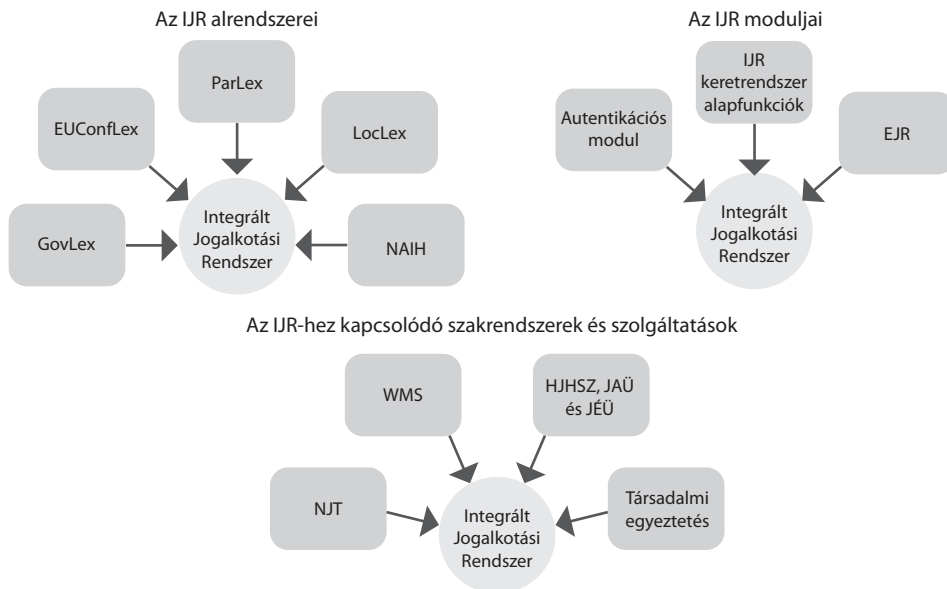
Az 1612/2019. (X. 24.) Korm. határozatban megfogalmazott elvárások alapján az IJR a jogi technológiák „Legaltech 3.0” korszaka szerinti, automatikus vagy félautomatikus dokumentum-összeállító rendszernek (document assembly systems) feleltethető meg. Az ilyen rendszerek a 2010-es években kaptak lendületet, lényegük, hogy egy szövegelemeket tartalmazó adatbázist kombinálnak bizonyos szabályokkal és – általában – űrlapszerű beviteli felületekkel, és segítségükkel többször használt dokumentumokat lehet könnyedén, szinte automatikusan előállítani.²⁹

Az Integrált Jogalkotási Rendszer (IJR) a kormányhatározat alapján több lépcsőben állt üzembe, utolsó eleme 2021-ben. A ParLex 2020. augusztus 1-jén, a LocLex 2021. április 1-jén, a GovLex 2021 augusztusában.

²⁹ Zódi Zsolt: Bevezetés: Jogi technológiák. In Zódi Zsolt (szerk.): *Jogi technológiák. Digitális jogalkalmazás*. Budapest, Ludovika Egyetemi Kiadó, 2022. 26.

Az IJR meglévő rendszereket kapcsol össze újonnan fejlesztett elemekkel. További újdonsága, hogy egyetlen elektronikus rendszerbe foglalja a jogalkotást, az első betű leütésétől egészen a jogszabály vagy közjogi szervezetszabályozó eszköz kihirdetéséig, illetve közzétételéig. Fontos tulajdonsága az interoperabilitás, vagyis a különböző informatikai rendszerek együttműködésre való képessége. A rendszer biztonsága is kiemelendő, mivel a zárt rendszerben történő kommunikáció kiválthatja az előterjesztések nyílt hálózaton keresztül történő (e-mail-es) küldözgetését, valamint praktikus előnye, hogy számontarthatja a tervezet aktuális verzióját, így egy tervezetnek nem kering több, esetleg már nem aktuális változata a felhasználók között. Fontos megjegyezni, hogy egy egységes rendszer támogathatja a közös munkavégzést is.

Az IJR-hez kapcsolódó alrendszereket, modulokat, illetve a kapcsolódó szakrendszereket és szolgáltatásokat a 2. ábra szemlélteti.



2. ábra: Az IJR felépítése

Forrás: Mátyás Ferenc: Április 1-jétől kötelező lesz az IJR és a LocLex használata. *Jogászvilág*, 2021. március 18.

Az IJR alrendszerei közül elsőként a koordinatív funkciókat ellátó *GovLex* alrendszer említendő, amely a jogalkotás eljárási részét menedzseli a Kormány ügyrendjéről szóló Korm. határozat alapján. Az *EUConfLex* alrendszer feladata a jogharmonizáció kezelése, azaz az Európai Unió jogának való megfelelés érdekében szükséges jogszabály-előkészítési feladatok teljesítéséről szóló 302/2010. (XII. 23.) Korm.

rendelet szerinti eljárás menedzselése.³⁰ A *LocLex* önkormányzati alrendszer, amelyben a helyi önkormányzati rendeletek készülnek.

Az IJR moduljai közül elsőként az autentikációs modult kell megemlíteni, amely kiemelkedő biztonsági jelentőségű, mivel az előterjesztések szövege mint döntés-előkészítő anyag 10 évig nem nyilvános.³¹ Az *EJR* – elektronikus jogszabályszerkesztő modul a kodifikációs tevékenység motorja. Ez a modul tartalmazza a jogalkotás formai követelményeit előíró szabályokat, a jogalkotási törvény és a jogszabályszerkesztésről szóló IRM rendelet alapján. Az IJR-hez kapcsolt alrendszerek közül kiemelendő a Nemzeti Jogszabálytár (*NJT*), amely egy nyilvánosan is elérhető, publikált szöveges adatbázis, amelynek elemeivel dolgozik a jogszabályszerkesztő modul. A jogszabályok kihirdetése előkészítése a *WMS* modulban történik, ebből kerül a normaszöveg a hivatalos lapba.³²

Törvény IJR-beli elkészítése során a jogalkotásban részt vevő alrendszerek, modulok és szakrendszerek sorozata a következő lehet:

A tervezet szövege az *EJR* rendszerben készül el. A *GovLex* rendszerben történik a tervezet véleményezése több körben, valamint közigazgatási és társadalmi egyeztetése. Szintén ebben a modulban történik a tervezet benyújtása a Közigazgatási Államtitkári Értekezlet ülésére, kormánykabinetre vagy kormányülésre. A törvénytervezet az Országgyűléshez való benyújtásával átkerül a *ParLex* alrendszerbe, amely az országgyűlési szakon viszi végig a tervezetet, a benyújtástól annak elfogadásáig, egészen a köztársasági elnök által aláírandó példány elkészítéséig. Ezután kerül az elfogadott jogszabály a *WMS* modulba, ahol előkészítik a Magyar Közlönyben való megjelenésre, valamint a jogszabály bekerül a Nemzeti Jogszabálytár adatbázisába.

A fentiekben elképzelt, modellezett folyamat alapján látható, mennyi adatátadás szükséges az egyes alrendszerek, modulok, szakrendszerek és szolgáltatások között, ezért kiemelten fontos ezen elemek introperabilitása. Meg kell jegyezni, hogy a fentiekben modellezett folyamat más jogszabálytípusok (kormányrendelet, miniszteri rendelet) esetében eltérő, sőt egymástól is eltérő, ez villantja meg a rendszertől elvárható komplexitást.

Az Integrált Jogalkotási Rendszer friss, jelenleg nem kizárólagosan használt rendszer, ezért hatásainak vizsgálata napjainkban csak elkezdődhet, az első komolyabb eredmények a rendszer átfogó használatát vagy alkalmazásának kizárólagossá válását követően fognak jelentkezni.

³⁰ Bővebben: Az Integrált Jogalkotási Rendszer új tervezett informatikai alrendszere, az *EUConfLex*.

³¹ Lásd 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról 27. § (5) bekezdés.

³² Két új alrendszer a hatalmas gépezetben: az *EJR* és a *GovLex*.

Előzetes tapasztalatok

A Covid-19 világszerte gyorsította a digitalizációt

A pandémia miatti lezárásokkal előtérbe került a távoli munkavégzés. Ehhez a meglévő rendszereket rekordgyorsasággal kellett átállítani a távmunkára, valamint olyan rendszereket kellett digitálisan elérhetővé tenni, amelyekkel kapcsolatosan ez az igény korábban fel sem merült. Egyes vélemények szerint a pandémia időszaka évtizedes digitalizációs lemaradást hozott be, Magyarország 2021. évi Nemzeti Reform Programja így fogalmaz a közszolgálati digitalizációval kapcsolatosan: „2020-tól kezdődően jelentős előrelépés történt az állami elektronikus ügyintézés megalapozó, a szervezeten belüli munkafolyamatok elektronizáltsági fokának növelését támogató fejlesztések tekintetében. [...] A jelenlegi Covid-19-válság hatására az elkészült alkalmazások kihasználtsága, az online ügyintézés szerepe a lakosság körében jelentősen megnövekedett. [...] Az állam digitális kapacitásainak bővítése kiemelt célként jelenik meg a HET-ben is, tekintettel arra, hogy még mindig jelentős lemaradás figyelhető meg az e-közigazgatási szolgáltatók igénybevétele, valamint a teljes körű online ügyintézési lehetőségek köre esetében.”³³

A digitális kompetenciák hiánya

Az Európai Bizottság által a tagállami digitális gazdasági és társadalmi fejlettség mérésére számolt 2021. évi DESI mutató alapján Magyarország a 27 uniós tagállam között a 23. helyen állt. Megjegyzendő, hogy az e-kormányzat-felhasználók internethasználókhöz viszonyított aránya alapján 9. helyen van, ami az EU-átlag feletti. Eszerint az internethasználók hazánkban nagy arányban veszik igénybe az e-kormányzat szolgáltatásokat. Az uniós átlagnál valamivel jobban szerepel Magyarország (12.) az internet-hozzáférés területén, ezen belül vezető helyezést foglal el az 1 Gbps sebességű széles sávú rendszerek lefedettségi arányát tekintve. Viszont a magyaroknak csupán 49%-a rendelkezik legalább alapszintű digitális készségekkel, ami számottevően elmarad az 56%-os uniós átlagtól, és más mutatók is viszonylag alacsony szintű digitális készségeket mutatnak. A kkv-knak csupán 46%-a rendelkezik legalább alapszintű digitális intenzitással, szemben a 60%-os uniós átlaggal, és a kulcsfontosságú digitális technológiák (nagy adathalmazok, mesterséges intelligencia és felhő) elterjedtsége alacsony. A közszolgáltatások digitalizálása dimenzióban az e-kormányzati felhasználók (70%) kivételével valamennyi hazai mutató elmarad az uniós átlagtól.³⁴

³³ Magyarország 2021. évi Nemzeti Reform Programja. 22.

³⁴ Lásd Magyarország 2022. évi Nemzeti Reform Programja. 15–16.

A jogalkotás digitalizációja révén javulhat a normák technikai minősége, pontossága

A kodifikáció jellemzően humán tevékenység, amelynek során a kodifikátor a jogi normáknak megfelelő formába, a jogalkotói szándéknak megfelelő tartalommal készíti el a normaszöveg tervezetét, amelyet jogszabályban meghatározott eljárás szerint kell elfogadni és kihirdetni, ennek megsértése akár a jogszabály közjogi érvénytelenségét okozhatja.

Az elektronizáció a jogalkotásra vonatkozó anyagi jogi normák és eljárási szabályok leprogramozásával olyan rendszert hozhat létre, amelyben már a jogszabály készítésekor jelezheti a rendszer, ha a jogszabály az előírt formai követelményektől eltér, illetve mérlegelés nélkül le is tilthatja a készítés folytatását a hiba orvoslásáig. A szöveggeneráló megoldások az emberekhez képest nagyobb konzisztenciát tudnak biztosítani, szabványosabb végeredményt hoznak létre, gyorsabban és több nyelven.³⁵ Az eljárási szabályok betartása felett is öröközhet a szoftver, ha valamilyen szükséges lépés kimarad az elkészítés során, azt a rendszer képes naplózni, így a hiány nyilvánvaló lesz.

A jogi normáktól elvárható közérthetőségi követelményen a rendszer tud-e javítani?

A jogszabályszerkesztésről szóló IRM rendelet a jogszabály tervezetének a megszövegezésére vonatkozó általános követelmények között említi, hogy „[a] jogszabály tervezetét a magyar nyelv szabályainak megfelelően, világosan, közérthetően és ellentmondásmentesen kell megszövegezni”.³⁶ A közérthetőség azonban nem formai, hanem tartalmi követelmény. Míg a jogalkotásról szóló normáknak való megfelelés leprogramozható, a tartalmi elvárások, úgymint hogy világos, közérthető, ellentmondásmentes legyen a norma szövege, már olyan elvárás, amely egy szoftver lehetőségeit meghaladja. A jogi precizitás önmagában is a közérthetőség ellen hat, elég csak arra gondolnunk, hogy egyes jogszabályokban elhelyezett sok külső és belső merev hivatkozás és közbevetés megnehezíti az értelmezést.³⁷

³⁵ Ehud Reiter – Robert Dale: Building Natural Language Generation Systems. Cambridge, Cambridge University Press, 2000. 29–30. Idézi Homoki Péter: Miként lehet a szöveggeneráló eszközöket a jogászai hivatások körében hasznosítani? In Zódi Zsolt (szerk.): *Jogi technológiák. Digitális jogalkalmazás*. Budapest, Ludovika Egyetemi Kiadó, 2022. 192.

³⁶ 61/2009. (XII. 14.) IRM rendelet a jogszabályszerkesztésről 2. §.

³⁷ Például a polgári perrendtartásról szóló 2016. évi CXXX. törvény 50. § (2) bekezdése: „Az (1) bekezdés szerinti perbeállítás kezdeményezése során a 49. § (2) és (4) bekezdését kell alkalmazni.” Vagy a 209. § (6) bekezdése: „(6) A fél az (1) bekezdésben meghatározott határidő után beszámítással – ideértve az ellen-beszámítást is – írásban vagy a tárgyaláson szóban akkor élhet, ha a (2)–(4) bekezdés szerinti kizáró ok nem áll fenn.”

Szabályozási kihívások

Az Integrált Jogalkotási Rendszer bevezetéséről és az ahhoz kapcsolódó feladatokról szóló 1612/2019. (X. 24.) Korm. határozat 6. pontja felhívja az igazságügyi minisztert, hogy – szükség esetén a Kormány más tagjának és a Miniszterelnöki Kormányiroda közigazgatási államtitkárának bevonásával – az IJR bevezetése, működtetése és fenntartása érdekében vizsgálja meg a jogalkotással, jogszabály-előkészítéssel kapcsolatos és más szabályozási tárgyú jogszabályok, illetve közjogi szervezetszabályozó eszközök módosításának szükségességét, és tegyen javaslatot azoknak az IJR bevezetésével összefüggésben szükséges, valamint a jogalkotással összefüggő adminisztratív terhek csökkentését eredményező módosítására. Jelenleg a jogalkotási folyamat digitalizációjára vonatkozó rendelkezések, az Integrált Jogalkotási Rendszer működéséről, használatáról szóló normatív szabály jogszabályi szinten nem található.

Adminisztratív terhek csökkenése

Az adminisztratív terhek csökkenését jelen esetben a közigazgatás vonatkozásában kell értelmezni. Az egyes ügyfeleknél jelentkező, de társadalmi szinten is érzékelhetővé váló kockázatok folyamatos csökkentése több tényező együttes hatásaként jöhet létre. Ilyen tényező, hogy az ügyfél az eljárás kapcsán tájékozottabbá válik, aminek következtében közvetlen költségmegtakarítás és adminisztratív tehercsökkenés lép fel mind az ügyfél-, mind az ügyintézői oldalon.³⁸ A jogalkotás folyamatának egységes rendszerbe terelése véleményem szerint pozitív hatásokkal kecsegtet. Ezek egy része időmegtakarítást jelent, mivel az online végzett műveletek (például iratjavítás) esetében nincs kézbesítési idő és kézbesítési költség, a megfelelően használt rendszerekben az információterjedés szinte azonnali. Ez lerövidíti a határidőket is, gyorsítja, dinamizálja az államigazgatás működését, javítja a reakcióképességét. Fontos továbbá, hogy egy egységes, integrált rendszerben kell dolgozni, ezért nem fordulhat elő az az eset, hogy az ügyintéző az általa használt sok rendszer közül az egyikbe nem lép be, így az információ vagy feladat megakad nála. Homoki szerint nem cél, hogy a jogászok maguk közvetlenül használjanak természetes nyelvi szöveggalkotó eszközöket, de ha az ilyen eszközök elérhetővé válnak jogi hivatásokat kiszolgáló informatikai vállalkozások részére, akkor ez csökkenti a vállalkozások költségeit.³⁹

³⁸ Az Integrált Jogalkotási Rendszer (IJR) hatásai a gazdasági és a társadalmi szereplőkre.

³⁹ Homoki (2022): i. m. 202.

*A jogalkotás digitalizációja mérföldkönek tekinthető
a közvetlen demokrácia felé vezető úton?*

A jogalkotás folyamata nem nélkülözheti a társadalmi véleménynyilvánítást, ennek kereteit határozza meg a jogszabályok előkészítésében való társadalmi részvételtől szóló 2010. évi CXXXI. törvény. A törvény alapján társadalmi egyeztetésre kell bocsátani a törvény, kormányrendelet, miniszteri rendelet tervezetét és indokolását, sőt lehetőség van a tervezet koncepciójának társadalmi egyeztetésre bocsátására. Ez a hatályos szabályozás alapján általános egyeztetés formájában valósul meg, a Kormány honlapján megadott elérhetőségen keresztül biztosított a véleményezés lehetősége,⁴⁰ vagy közvetlen egyeztetés formájában, amikor a jogszabály előkészítéséért felelős miniszter kér fel személyeket, intézményeket vagy szervezeteket közvetlenül a tervezet véleményezésére.

Mivel az elektronizált jogalkotás biztosíthatja a dokumentumok közös szerkesztésének lehetőségét, a jogalkotás digitalizációja technikailag magában hordozza a jogszabályok közös megalkotásának, végső soron a közvetlen (részvételi) demokrácia⁴¹ megvalósításának lehetőségét.

Tóth J. Zoltán a *Demokrácia, jogállamiság és alkotmánybíráskodás* című könyvében összehasonlította a közvetett és a közvetlen demokrácia előnyeit és hátrányait, egyben öt pontban meghatározta, miért nem tud hatékony módon megvalósulni a közvetlen demokrácia. Vizsgálata B) pontja szerint „technikailag és logisztikailag a szavazásban való részvétel nem minden állampolgár számára megoldható [...] [a] mai technikai fejlettségi szinten akárhány kérdés feltehető és megválaszolható egy számítógép (vagy annak megfelelő más eszköz, így akár egy okostelefon) birtokában, képernyő előtt. (A referendárius demokráciát ma már tipikusan nem urnás, hanem elektronikus, internetes szavazással képzelik el, ez az úgynevezett e-demokrácia koncepciója.)”⁴²

Álláspontom szerint a jogalkotás digitalizációja utat nyit a jogszabálytervezetek elkészítésében való széles körű együttműködésnek, ami néhány lépéssel megelőzi a referendumokat, mivel maga a szavazásra bocsátandó politikai kérdés megfogalmazása is történhet közvetlenül. Természetesen a digitalizáció sem old meg minden problémát, amennyiben az ellenérdekelt felek a vitában elektronikus úton megrekednek, szükség nyílhat az álláspontok szóbeli megvitatására,⁴³ amelyhez szintén

⁴⁰ Például A honvédelemről és a Magyar Honvédségről szóló törvény tervezete.

⁴¹ „A részvételi demokrácia esetében (ahogyan maga az elnevezés is jelzi) a nép választójoggal rendelkező tagjai képviselők közbejötté nélkül, maguk döntenek a felvetődő politikai kérdésekről.” Tóth (2020): i. m. 145.

⁴² Tóth (2020): i. m. 159.

⁴³ Lásd 1352/2022. (VII. 21.) Korm. határozat a Kormány ügyrendjéről 13. pont (3) bekezdése: A fennmaradó vitás kérdésekben, különösen a kívánt közpolitikai cél elérését veszélyeztető észrevétel vagy vélemény fenntartása esetén a Miniszterelnöki Kormányiroda közigazgatási államtitkára

online eszközök állnak rendelkezésre, azonban ezen sok résztvevős viták levezetése továbbra is komoly kihívás.

A fenti indokolás mellett fogalmaztam meg azon álláspontomat, hogy a jogalkotás digitalizációja mérföldkő lehet a közvetlen demokrácia felé, azonban ez nem jelenti azt, hogy cél lenne a közvetlen demokrácia megvalósítása, viszont a fentebb tárgyalt adminisztratív terhek csökkentése szempontjából a népszavazások és választások elektronikus útra terelése már középtávon is jelentős mértékben csökkenthetné azok költségeit.

Ugyanakkor nem tudjuk megjósolni a jövőt. A tervezett rendszerek projektszerű agilis fejlesztése mindig függ a bennünket körülvevő technológiai fejlődéstől, lokálisan és globális szintereken egyaránt. A külső körülmények változása hatással van a fejlesztési irányokra, ahogyan a pandémia előtérbe hozta a távoli munkavégzést, az energiaválság miatt újra kell gondolni a működést sok cégnek, vagy a növekedő infláció miatt a fejlesztések üteme lelassul. Ugyancsak hatással van a digitalizációra az automatizáció, mivel a mesterségesintelligencia-alapú öntanuló rendszerek fejlődésével elérkezhet az a pont, amikor érdemesebb lesz az egész rendszert új alapokra helyezni, vagyis a mesterségesintelligencia-alapú rendszert fejleszteni a már meglévő digitalizált rendszer további bővítése helyett. Az agilis fejlesztés ismérve a rövid – általában kéthetes – sprintekben történő fejlesztés, ami nagyon gyorsan tud reagálni a külső és belső körülmények változására, ez előnye a hagyományos prediktív fejlesztési projektekhez képest, amikor az eredeti céltól való eltérést ritkábban, mérföldkövenként értékelik, emiatt a változáskezelési eljárás ritkább és hosszadalmasabb feladat.

Kitekintés – jogalkotás és a mesterséges intelligencia

Korunk leggyakrabban emlegetett fogalma a folyamatautomatizálással kapcsolatosan a mesterséges intelligencia. A neurális hálózatokon alapuló öntanuló rendszerek a jövőben megoldást jelenthetnek az emberi erőforrás szűkösségére,⁴⁴ emellett munkájukat legtöbbször az embernél pontosabban, alaposabban végzik. Ezen rendszerek még kialakulóban vannak, akárcsak a mesterséges intelligencia jogi szabályozása az Európai Unióban.

a Közigazgatási Államtitkári Értekezletre való benyújtást megelőzően egyeztetést folytat, vagy arról gondoskodik, és javaslatot tesz a vita megoldásának módjára.

⁴⁴ Az emberi erőforrás szűkössége a szakképzett humán munkaerőre vonatkozik. A föld lakossága gyorsuló tempóban növekszik, azonban lokálisan a humán erőforrás hiányával szembesülünk. Ezért a hiányzó erőforrást gépekkel pótoljuk, amelyek önmaguktól képesek tanulni, nagy hatékonysággal. Ennek visszahatása is kezd kialakulni, ugyanis ezáltal egyes munkakörök részben vagy teljesen feleslegessé válhatnak – például szupermarket-pénztáros az önkiszolgáló kasszák világában –, sőt egyes kompetenciáink feleslegessé válhatnak, például a számolás a számológépek mellett, a telefonszámok memorizálása a mobiltelefonok mellett vagy a tájékozódás képessége a navigációs eszközök mellett.

„A 2020 májusában elkészült Magyarország Mesterséges Intelligencia Stratégiája⁴⁵ című dokumentum a 2020–2030 közötti időszakra határoz meg célokat a mesterséges intelligencia alkalmazásával kapcsolatosan. A stratégiában célként került megfogalmazásra, hogy az ügyintézés 60%-a elektronikusan, önkiszolgáló módon történjen 2030-ra.”⁴⁶ A dokumentum ágazatonként konkrét célokat fogalmaz meg. Az államigazgatás vonatkozásában „[c]él a közszolgáltatások elektronikus elérésének, digitalizációjának elősegítése, melyben az MI egy az alkalmazható technológiák közül. Ezen fejlesztések az e-közigazgatásba illeszkednek, amely terület már jelenleg is integrációt alakít ki, folyamatokat fejleszt, amelyek hatékonyságát lehetséges továbbfejleszteni, illetve új csatornákat lehet hatékonyabban kiszolgálni.”⁴⁷ A stratégia a jogalkotási folyamatról nem tesz említést, azzal kapcsolatos célt sem fogalmaz meg, ezért vizsgálódásom alapjának a stratégia azon megállapítását tartom, amely szerint: „Cél az MI-vel kapcsolatos kísérletezési kedv növelése.”⁴⁸

A szakirodalom alapján az IJR-t az automatikus vagy félautomatikus dokumentum-összeállító rendszerek közé lehet besorolni. Az ilyen szöveggeneráló eszközök a legegyszerűbb esetben gépi tanulási képesség nélküli szoftverből, valamint egy szótárból állnak, azonban technológiailag állhat mögöttük akár egy többretegű neurálisháló-architektúra is.⁴⁹ Ez azt is jelenti, hogy a jogalkotás digitalizált rendszerének mesterséges intelligenciával való összekapcsolásának vizsgálata okszerű.

„A mesterséges intelligencia már a jogi szakmába is megérkezett, de jellemzően a felhasználói, jogalkalmazói oldalon, azonban álláspontom szerint a jogalkotásban is meg fog jelenni idővel, különösen azért, mert a jogszabályok fordítása-fordíthatósága az európai uniós tagságunkra tekintettel a későbbiekben – az Unió Fordítási Főigazgatósága (DGT) gépi fordítási kapacitásának növekedése mellett – igényként jelentkezhet. Ez a folyamat a jogtudomány szempontjából is figyelemre méltó.”⁵⁰ A globális gazdaság miatt a jogszabályok fordítása a gépi fordítás kapacitásának növekedése mellett igényként jelentkezhet.⁵¹ Bár a fordítás mint nyelvi közvetítés nem hat vissza a jogalkotás nyelvi minőségére, azonban szükséges megjegyezni, hogy jó minőségű, jól értelmezhető jogi szövegről egyszerűbb fordítást készíteni, és a fordítás is jobb minőségű lesz. A gépi jogalkotás – gépi fordítás relációjában

⁴⁵ Magyarország Mesterséges Intelligencia Stratégiája 2020–2030. 2020. május.

⁴⁶ Kántor Ákos: Az e-ügyintézésről az e-jogalkotás felé. In Miskolczi-Bodnár Péter (szerk.): *XXIII. Jogász Doktoranduszok Országos Konferenciája 2022*. Budapest, Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, 2022b. 153.

⁴⁷ Magyarország Mesterséges Intelligencia Stratégiája 2020–2030. 38.

⁴⁸ Magyarország Mesterséges Intelligencia Stratégiája 2020–2030. 29.

⁴⁹ Homoki (2022): i. m. 189.

⁵⁰ Kántor Ákos: A jogalkotás digitalizációja és a mesterséges intelligencia alkalmazási lehetőségeinek vizsgálata. In Miskolczi-Bodnár Péter (szerk.): *XXI. Jogász Doktoranduszok Konferenciája 2021*. Budapest, Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, 2022a. 34.

⁵¹ Lásd a jogszabályfordításokat a Nemzeti Jogszabálytárban: National Legislation Database – Translated legislation.

ez azt jelentené, hogy gépi jogalkotás által produkált – következetes szóhasználatú, jól strukturált, egyszerű mondat szerkezetű – szöveget a gépi fordító alkalmazás nagyobb eredményességgel (kevesebb utószerkesztéssel, így rövidebb idő alatt, alacsonyabb költség mellett) tudna idegen nyelvre lefordítani.

A jogalkotás informatikai rendszerének mesterséges intelligenciával való összekapcsolása mellett technológiai érvként szerepel az is, hogy az ilyen rendszerek két fő alkotóeleme az algoritmus, valamint az adatbázis. Az adatbázis rendelkezésre áll, mivel a Nemzeti Jogszabálytár lényegében egy jogi, lexikális adatbázis, amely betanító adatbázisként rendelkezésre is állhat. Az algoritmus elkészítéséhez pedig lehetne kiinduló állapotban az IJR-be leprogramozott, digitalizált szabályokat használni. Homoki Péter szerint a többrétegű neurális háló modellekre épülő megoldások a jogi szövegösszegzés terén is ígéretesek lehetnek, azonban ezek használata egy adott tagállami kis nyelven is további befektetést, kutatást, fejlesztést igényel.⁵²

Formálódó jogi szabályozás (MI)

Bár a mesterséges intelligencia – tudva vagy nem tudva – már a mindennapjaink része, sok – és ezek között több jogi jellegű – kérdés még tisztázatlan. Az Európai Unió 2018 óta foglalkozik élénken a mesterséges intelligencia kérdésével számos előkészítő dokumentumában, ezek közül kiemelendő a mesterséges intelligenciáról szóló jogszabály.⁵³ A javaslatot 2021. április 21-i dátummal tették közzé tekintélyes, 118 oldalas terjedelemben, 17 oldalnyi melléklettel.⁵⁴ A Javaslat elemzése jelen tanulmánynak nem tárgya, azonban annyit meg lehet jegyezni, hogy a piaci igényekre reflektáló fejlesztések mellett a kötelező erejű uniós jogalkotás (rendelet) nem halad túl gyorsan, de ez a szabályozás tárgyából és a jogalkotási eljárás belső jellegzetességeiből is adódik. Viszont ez azt is jelenti, hogy kihirdetett jogi szabályok hiányában a fejlesztés is kockázatos, a jogi szabályozás hiánya, illetve a megváltozása minden projekt esetében komoly külső kockázati tényezőként rangsorolt.

Etikai kérdések

„A bizottság 2019-ben kiadott közleménye szerint a jog és etika egymás mellett kell hasson: »a mesterséges intelligencián alapuló alkalmazásoknak nemcsak a jogszabályokkal kell összhangban lenniük, hanem az etikai elveknek is meg kell felelniük,

⁵² Homoki (2022): i. m. 198.

⁵³ Európai Bizottság: *Javaslat. Az Európai Parlament és Tanács rendelete a mesterséges intelligenciára vonatkozó harmonizált szabályok (A mesterséges intelligenciáról szóló jogszabály) megállapításáról és egyes uniós jogalkotási aktusok módosításáról*. COM(2021)206 végleges (2021. április 21.).

⁵⁴ Kántor (2022c): i. m. 55.

és biztosítaniuk kell, hogy az alkalmazásuk ne okozzon nemkívánt károkat». ⁵⁵ A közlemény ⁵⁶ arra a következtetésre jut, hogy a mesterséges intelligencia csak akkor tekinthető megbízhatónak, ha azt a széles körben elfogadott etikai értékeket tiszteletben tartva fejlesztik ki és használják. ⁵⁷

Az etikai kérdések témám szempontjából két csoportra oszthatók, amelyek egymással rész-egész viszonyban állnak. Az általános etikai szabályok körében a mesterséges intelligencia alkalmazásával kapcsolatos általános etikai kérdéseket említem, ezeknek bőséges irodalma van az Európai Unióban, jelen tanulmányban ezért erre nem térek ki.

A szűkebb halmazban az a specifikus kérdés merül fel, hogy alkothat-e gép jogot. „Az IJR alapján úgy tűnik, hogy a számítógéppel támogatott jogalkotás a jogszabályszerkesztés formai követelményeinek betartását segíti, a normaszöveg tartalmi rendelkezéseinek vizsgálatára nem alkalmas, nem is feladata. A »gépi« jogalkotás esetében is kérdés lesz, hogy a formai megfelelésen túl a mesterséges intelligencia »meg tudja-e érteni«, tudja-e majd értelmezni a jogszabályok tartalmát. Úgy gondolom, a jogértelmezés annyira komplex, összetett tevékenység, amelyet a gép nem tud elvégezni. Többek közt azért sem, mert csak a normaszöveget ismeri, így viszont legfeljebb a norma nyelvtani értelmezését tudná elvégezni, ami a jogértelmezésnek mindössze az első lépése. Viszont amennyiben a mesterséges intelligencia nem képes jogszabály értelmezésére, ebből az is következik, hogy nem lehet képes önállóan jogszabály alkotására sem.» ⁵⁸

A kérdés feloldása lehet, ha a gépi jogalkotást összekapcsoljuk emberi utómunkával, ahogyan a gépi fordításnál is történik, a nyers gépi fordítást utószerkesztéssel hozzák a megrendelő által kívánt minőségi szintre. Ez a megoldás annyira elterjedt, vált, hogy a gépi fordítást követő utószerkesztésnek 2017-ben az önálló szabványa is elkészült. ⁵⁹ Álláspontom szerint, amennyiben a jogalkotás digitalizációja az automatizáció irányába fog tovább haladni, ehhez hasonló irányban lesz célszerű elindulni, vagyis az adatbázis elemeiből algoritmikus szabályok szerint gépileg összeállított normaszöveg humán utószerkesztésével. Ez a megoldás átvágja a gordiuszi csomót, hiszen annak ellenére, hogy a jogot (normaszöveget) formailag gép alkotná, annak elfogadása előtt mindenképp emberi kontroll alá kell kerülnie.

⁵⁵ Európai Bizottság: *A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. Az emberközpontú mesterséges intelligencia iránti bizalom növelése.* COM(2019)168 végleges (2019. április 8.). 3.

⁵⁶ Európai Bizottság (2019): i. m. 10.

⁵⁷ Kántor (2022c): i. m. 50.

⁵⁸ Kántor (2022a): i. m. 33.

⁵⁹ ISO 18587:2017 Translation services – Post-editing of machine translation output – Requirements; MSZ ISO 18587:2017 Fordítási szolgáltatások tanúsítása – A gépi fordítás kimenetének utólagos szerkesztése – Követelmények.

Összegzés

Korunkban a technológia fejlődése felgyorsította a digitalizációt, egyre több közügy és magánügy intézhető digitálisan, személyes megjelenés nélkül, sőt újabban már emberi közreműködés sem szükséges nagyon sok korábban hatósági aktushoz.⁶⁰

A digitalizáció a jogászokat is elérte, több már digitalizált jogterületet követően a jogalkotás digitalizációja is megkezdődött, kezdetben szigetszerű megoldásoktól jutott el 2021-re az egységes, a jogalkotás rendszerét átfogó megoldásig, az Integrált Jogalkotási Rendszerig. A jogalkotás részben a törvényhozó, részben pedig – felhatalmazás alapján – a végrehajtó hatalom aktusa, minősége hatással van a demokráciára, ami akkor vehető észre nyilvánvalóan, ha a jogalkotással szemben támasztott demokratikus elvárások nem teljesülnek.

Jogosan merül fel a kérdés, hogy a jogalkotás digitalizációja a közvetlen demokrácia felé vezető út egyik első lépése lehet-e, mivel a jogalkotásban való részvételt, a vélemények továbbítását a digitalizált rendszer képes lehet továbbítani, akár fel is dolgozni, azonban hazánkban a digitális kompetenciák a DESI mutató alapján az EU-átlaghoz képest is hiányosak, komoly képzési munkára lenne szükség ahhoz, hogy az egyébként jogilag sem egyszerű jogalkotási folyamatba az informatikai eszközökkel való bekapcsolódást elsajátítsák a választójoggal rendelkező állampolgárok. Amennyiben sikerülne, a befektetés megtérülhetne, mivel a rendszer vélhetően teret tudna biztosítani a népszavazások költséghatékony lebonyolításához is.

Továbbgondolva a jogalkotás digitalizációs lehetőségeit, felmerül az automatizáció – a mesterséges intelligencia bevonási – lehetősége. A szakirodalom alapján a jogi szövegösszegzés terén is komoly eredményeket értek el mesterséges intelligencia felhasználásával, igaz, jogalkalmazói területen. Az IJR esetében a mesterséges intelligenciát természetes nyelvi szövegalkotó eszköz támogatására lenne érdemes bevonni, a Nemzeti Jogszabálytár mint nyelvi betanító adatbázis felhasználásával.

A mesterséges intelligenciával kapcsolatosan szinte minden tanulmányban olvashatunk kételyeket és dilemmákat, ezeket én kihívásoknak nevezem, mivel már nem kérdés, hogy szükség van a mesterséges intelligenciára, a kihívások pedig megoldandó feladatot jelentenek. Az egyik tárgyalt csoport a tanulmányban a szabályozási kihívások, amelyekkel az unió napjainkban is küzd a több mint egy éve készült mesterséges intelligenciáról szóló rendelettervezetével, a másik az etikai kihívások csoportja, amelynek klasszikus központi kérdése, hogy alkothat-e a gép jogot?

A digitalizált jogalkotás hatással van a demokráciára, mivel magában hordozza a széles körű konszenzuson alapuló jogalkotás és a közvetlen demokrácia lehetőségét. Ha a jogalkotás öntanuló, mesterségesintelligencia-alapú platformra

⁶⁰ Lásd Kiosk projekt: NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.: *Mesterséges intelligenciával támogatott ügyintézési pont (KIOSK) kiterjesztése a kormányhivatalokra, illetve más külső ügyintézési helyszínekre.*

helyeződne át, akkor javasolt a gépi fordításnál már bevált utószerkesztést alkalmazni a gép által alkotott jogszabályok esetében, így tartva meg a végső humán kontrollt a jogalkotás felett.

Felhasznált irodalom

- A honvédelemről és a Magyar Honvédségről szóló törvény tervezete. Online: <https://kormany.hu/dokumentumtar/a-honvedelemrol-es-a-magyar-honvedsegrol-szolo-torveny-tervezete>
- Az Európai Községek Bizottsága: *A Bizottság jelentése a Tanácsnak, az Európai Parlamentnek, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. Az adminisztratív terhek csökkentésének cselekvési programja az Európai Unióban*. COM(2007)23 végleges (2007. január 24.)
- Az Európai Községek Bizottsága: *A Bizottság közleménye a Tanácsnak, az Európai Parlamentnek, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. Az Európai Unión belüli jobb szabályozás stratégiai felülvizsgálata*. COM(2006)689 végleges (2006. november 14.)
- Az Integrált Jogalkotási Rendszer (IJR) hatásai a gazdasági és a társadalmi szereplőkre. Online: https://mhk.hu/files/IJR_tarsadalmi_gazdasagi_hatasok_cikktervezet_v2.pdf
- Az Integrált Jogalkotási Rendszer új tervezett informatikai alrendszere, az EUConfLex. Online: https://mhk.hu/files/EUConfLex_vegleges_v2_MKLLK.pdf
- Budai Balázs Benjámin: *A közigazgatás újragondolása*. Budapest, Akadémiai Kiadó, 2017.
- Európai Bizottság: *A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. Az emberközpontú mesterséges intelligencia iránti bizalom növelése*. COM(2019)168 végleges (2019. április 8.)
- Európai Bizottság: *Javaslat. Az Európai Parlament és Tanács rendelete a mesterséges intelligenciára vonatkozó harmonizált szabályok (A mesterséges intelligenciáról szóló jogszabály) megállapításáról és egyes uniós jogalkotási aktusok módosításáról*. COM(2021)206 végleges (2021. április 21.)
- Hiteles fordítás. Országos Fordító és Fordításhitelesítő Iroda Zrt. Online: www.offi.hu/hiteles-forditas/hiteles-forditas
- Homoki Péter: Miként lehet a szöveggeneráló eszközöket a jogász hivatások körében hasznosítani? In Zódi Zsolt (szerk.): *Jogi technológiák. Digitális jogalkalmazás*. Budapest, Ludovika Egyetemi Kiadó, 2022. 185–205.
- Horkay Hörcher Ferenc: *Előadások a XIX. és XX. század állambölcselete köréből*. Budapest, Szent István Társulat, 2001.
- Kántor Ákos: A jogalkotás digitalizációja és a mesterséges intelligencia alkalmazási lehetőségeinek vizsgálata. In Miskolczi-Bodnár Péter (szerk.): *XXI. Jogász Doktoranduszok Konferenciája 2021*. Budapest, Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, 2022a. 27–35.
- Kántor Ákos: Az e-ügyintézésről az e-jogalkotás felé. In Miskolczi-Bodnár Péter (szerk.): *XXIII. Jogász Doktoranduszok Országos Konferenciája 2022*. Budapest, Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, 2022b. 145–154.
- Kántor Ákos: Ízelítő az EU formálódó mesterséges intelligencia szabályozásáról. In Miskolczi-Bodnár Péter (szerk.): *XXII. Jogász Doktoranduszok Konferenciája 2022*. Budapest, Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, 2022c. 45–61.
- Kékedi Szabolcs – Zódi Zsolt: A bírósági informatika helyzete Magyarországon. In Zódi Zsolt (szerk.): *Jogi technológiák. Digitális jogalkalmazás*. Budapest, Ludovika Egyetemi Kiadó, 2022. 41–63.

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól
- 302/2010. (XII. 23.) Korm. rendelet az Európai Unió jogának való megfelelés érdekében szükséges jogszabály-előkészítési feladatok teljesítéséről
- 451/2016. (XII. 19.) Korm. rendelet az elektronikus ügyintézés részletszabályairól
- 182/2022. (V. 24.) Korm. rendelet a Kormány tagjainak feladat- és hatásköréről
- 61/2009. (XII. 14.) IRM rendelet a jogszabályszerkesztésről
- 1612/2019. (X. 24.) Korm. határozat az Integrált Jogalkotási Rendszer bevezetéséről és az ahhoz kapcsolódó feladatokról
- 1352/2022. (VII. 21.) Korm. határozat a Kormány ügyrendjéről

Kelemen Roland

A cyberfare state alapgondolata – Az egyén és kapcsolatai átalakulásának hatása az állam működésére és biztonságára¹



A tanulmány a cyberfare state állammodell alapgondolatára építve mutatja be a kibertér hatását az egyénre és azok kapcsolódásaira, vagyis a társadalmi hálózatokra. Ennek során a dolgozat kimutatja, hogy a társadalmi totalitás ezen szegmenseinek alapjellemzőiben jelentős kvalitatív és kvantitatív változások mentek végbe az elmúlt évtizedekben, amelyek alakították azok dinamikáját, formálhatóságát és összességében az állam biztonságára gyakorolt hatásukat is. Ennek megfelelően az államoknak reagálniuk kellett a jelenségre, amelyre a jogállamhoz való viszonyuk alapján eltérő válaszokat adtak. A smart total control cyberfare state államai a kibertér vívmányait is felhasználva elmozdultak az orwelli állam irányába, míg a demokratikus berendezkedésű államok esetében az egyének (felhasználók) képességeinek erősítése, tudásuk gyarapítása az egyetlen járható út. A tanulmány második felében az erre irányuló lépéseket tekinti át a szerző.

Bevezetés

A 21. század első évtizedeiben az államok, azok intézményrendszere és a hátterüket jelentő társadalmak jelentős átalakuláson estek át. Ennek az átalakulásnak a motorja a kibertér és az ahhoz kapcsolódó technológiák voltak. E technológiák behatoltak nemcsak az emberek életének minden szegmensébe, de egyre inkább formálták a társadalmi totalitás egyes részeit is, így az államok működését sem hagyták érintetlenül, ideértve annak szinte minden területét. A technológiai átalakulás soha nem látott sebességre kapcsol, aminek eredményeként megdőlni látszik Moore törvénye.² Ezen

¹ Ezen állammodell alapstruktúrájának a kidolgozása a szerző saját munkájának az eredménye, amit az alábbi tanulmányban adott közre: Kelemen Roland: Cyberfare state – Egy hibrid állammodell 21. századi születése. *Military and Intelligence CyberSecurity Research Paper*, 2. (2022), 1. 1–32.

² Az innovációnak a gyorsaságát mutatja, hogy Moore törvénye, amely szerint az integrált áramkörök összetettsége körülbelül 18 havonta megduplázódik, napjainkban egyre inkább megdőlni látszik, hiszen ez a tendencia gyorsulóban van. Lásd Gordon E. Moore: Cramming More Components onto Integrated Circuits. *Electronics*, 38. (1965), 8. 114–117. E jelenség motorja korunk egyik nívója, konvergáló technológiája a tárgyak internete (IoT – Internet of Things), amely az információtudomány fejlődésével, a szenzorok használatának fokozódó térnyerésével (ami magával hozza az árak rapid csökkenését) egyre inkább a mindennapi életünk részévé válik mind az otthonokban, mind pedig a közsférában. Lásd Németh Richárd: Kibertámadások gazdasági vonatkozásai a vállalati sférában.

átalakulás legalább ilyen mélyen érinti az emberek hétköznapijait vagy a társadalmi alrendszereket. Emellett pedig jelentős biztonsági kihívások elé állítja az államokat, amelyek alkotmányos szabályaik, történeti és politikai hagyományaik mentén eltérő válaszokat adnak ezekre a kihívásokra.

Míg a cyberfare state egyik altípusa, a smart total control cyberfare state felfogásában és biztonsági megoldásaiban az egyének és az egyének kapcsolatai, vagyis a társadalmi hálózatok felett a lehető legteljesebb felügyeletet igyekeznek kialakítani (lásd például a kínai Aranyhajó rendszert vagy a társadalmi kreditrendszert, a „halal” internetprotokollt)³, addig a nyugati demokratikus államok esetében szükségszerűen a jogállami paradigmák tiszteletben tartása mellett kell a kibertérből és a hozzá kapcsolódó technológiákból eredő pozitív hatások melletti biztonsági kockázatokat kezelni.

Jelen tanulmányban röviden azt kívánom áttekinteni, hogy a kibertér és a hozzá kapcsolódó eszközök milyen hatást gyakoroltak az egyénekre és kapcsolataikra, és ezen hatások milyen irányú változást eredményeztek az államok biztonsági környezetében. Ezen áttekintést követően pedig kitérek arra, hogy a nyugati, demokratikus államok szövetségi (NATO), illetve európai uniós szinten milyen válaszokat adtak erre a problémára.

A kibertér hatása az egyénre és a társadalmi hálózatokra

Az elmúlt pár évtizedben ugrásszerű változás következett be a társadalmi totalitás egészében, amely nem hagyta változatlanul az egyes részkomplexumokat, így a társadalmi struktúrát és a társadalmi hálózatokat sem. Alvin Toffler elmélete szerint az emberi történelem három hullámra osztható. Az első hullámban a gazdasági termelés alapja a földművelés, ahol a társadalmi struktúra és a leginkább jellegadó társadalmi hálózatok egybeestek. A második hullámot az ipari társadalom korának tekinti. Ezen időszakban felerősödött az egyén társadalmi szerepe, a társadalmi hálózataik hatóereje már nem feltétlenül függött a társadalmi struktúrában betöltött helyüktől. Végül a harmadik hullám az információ kora, vagyis az információs társadalom térnyerése.⁴ Fontos elméleti alapja volt annak a felismerésnek, hogy az információ, a tudás a társadalmi struktúrában betöltött szerepet, viszonyokat alapjaiban határozza meg.⁵ Ugyanis az információ már önálló értékévé vált, annak

In Dernóczy-Polyák Adrienn (szerk.): *Kutatási jelentés 1.* Győr, Universitas-Győr Nonprofit Kft., 2019. 307–325.

³ Gosztonyi Gergely: A kínai internetcenzúra modellje. *Pro Futuro*, 12. (2022a), 1. 1–9; Gosztonyi Gergely: Special Models of Internet and Content Regulation in China and Russia. *ELTE Law Journal*, 9. (2021), 2. 87–99.

⁴ Alvin Toffler: *A harmadik hullám (információs társadalom A-tól Z-ig)*. Budapest, Typotex, 2001.

⁵ Fritz Machlup: *The Production and Distribution of Knowledge in the United States*. Princeton University Press, 1962; Z. Karvalics László: „A tudás termelése és elosztása az Egyesült Államokban”:

megszerzése és birtoklása tett valakit, illetve valakiket tényleges hatalmi tényezővé. Ezen folyamatban a technológiai robbanás mellett óriási szerepe volt a globalizáció kiteljesedésének. E körben „[a] globalizációt akként gondolhatjuk el, mint a jelenkori társadalmi élet világméretű összekapcsoltságának szélesedő, mélyülő és gyorsuló valóságát, annak kulturális, kriminális, pénzügyi, spirituális, és számos egyéb aspektusával”.⁶ Ehhez viszont elengedhetetlen attribútummá vált a kibertér, tudniillik a kibertér kiépülésének köszönhetően váltak ténylegesen globálissá az emberi interakciók, a gazdaság és a kultúra. Fontos felismerés, hogy a technológia önmagában nem határozza meg a történelmi fejlődést és a társadalmi változásokat, viszont a technológia felhasználásának vagy fel nem használásának a módja megmutatja egy társadalom alkalmazkodási képességét.⁷ Mint a bevezetőben erre utaltam, a smart total controll cyberfare state államai e technológia révén elmozdultak egy orwelli világ irányába, ahol az egyének és kapcsolataik felett az állam és a technológiai partnerei fúzióban fellépve a védelem, a biztonság, a status quo megőrzése érdekében a lehető legteljesebb kontroll kialakítása irányába haladnak. A nyugati társadalmak mindeközben megpróbálják a technológia pozitív, jóléti funkcióit hangsúlyozni és továbbra is erős gátak között tartani az állami információéhséget.⁸ Így egyre nagyobb teret nyertek az államoktól elkülönült szereplők. „Korunkra a nemzetállamok riválisaivá nőttek ki magukat többek között a tőke-, a termelési, a kommunikációs, bűnözői hálózatok, a nemzetközi intézmények, a szupranacionális katonai gépezetek, a nem kormányzati szervezetek, a nemzetek feletti vallások, sőt, még a különböző társadalmi mozgalmak is.”⁹ A tudás- (és információ-) intenzív társadalomban tehát az állam másodlagos szereplővé kezd válni a transznacionális tényezők mellett (tekintsünk e körben a közösségimédia-platformok tevékenységére irányuló állami szabályozás kialakításának eredendő lehetetlenségére). Furcsa kettőssége ennek társadalmi oldalról, hogy az állam információhoz jutását korlátozzák, és hangosan tiltakoznak egy-egy hírszerzési kiszivárgás esetében (lásd Wikileaks, Snowden-ügy), de eközben a többség hallgatásba burkolózik azzal kapcsolatban, hogy „[a]z információ [...] kifürkészése és az adatok felhasználók hozzájárulásával, de az átadott adatkör mélységére és súlyára kiterjedő átfogó ismeret hiányában történő rendelkezésre bocsátása a legnagyobb tech-cégek részére milyen visszaélési lehetőséget

Fritz Machlup újraértékelése az információs társadalom elméletétörténetében. *Információs Társadalom*, 9. (2009), 2. 20–34.

⁶ Pongrácz Alex: A hálózat csapdájában? Globalizáció és totalitás. In Farkas Ádám (szerk.): *Védelmi alkotmányosság az új típusú biztonsági kihívások erőterében*. Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2018. 43.

⁷ Manuel Castells: *The Information age. Economy, Society, and Culture*. I. kötet. *The Rise of the Network Society*. 2. kiadás. Oxford, Blackwell Publishing, 2010. 7.

⁸ Pongrácz Alex: Variációk hibrid állammodell-építésre. *Military and Intelligence Cybersecurity Research Paper*, 2. (2022), 3. 3–8.

⁹ Pongrácz Alex: A globalizáció toposzai. In Kecskés Gábor (szerk.): *Doktori Műhelytanulmányok 2014*. Győr, Széchenyi István Egyetem Állam- és Jogtudományi Doktori Iskola, 2014. 158.

biztosít akár [...] az Amazon, a Facebook és a Google”¹⁰ számára. Ezzel a társadalmi struktúra – amely korábban maximum nemzetállami értelmezést jelentett – annak az igénynek megfelelően, vagy azt felhasználva, kiszolgálva, hogy az állam hatalmi tényezőként másodvonalba kerüljön, valamint annak köszönhetően, hogy életünk minden területe lényegében összekapcsolódott, és a szerveződés világméretűvé vált, így már sokkal inkább értelmezhető transznacionális vagy globális közegben, semmint államon belül. Ez a társadalmi struktúrát megkettőzi, és a nemzeti társadalmi struktúra mellett kialakult egy transznacionális vagy globális társadalmi struktúra is. Az egyének társadalmi hálózatainak is e kettős struktúra irányába kell igazodniuk, ami már eredendően konfliktusok forrása, és a nemzeti társadalmakon belüli törésvonalakat eredményez.

A fentiekén túl a kibertér és a hozzá kapcsolódó technológiák önmagukban jelentős hatást gyakoroltak, ugyanis átalakították az emberek hétköznapiját, a szolgáltatóközpontú gondolkodás átvette az uralmat a korábbi tradicionális működés felett. Az IoT vagy IoD¹¹ rendszerek már szükségszerűen módosították az emberek egymás közötti és az ember-gép közötti, sőt a gép-gép közötti interakciókat is. Minden adat, minden eszköz és minden személy valós időben elérhetővé vált a világ bármely pontján, ami átalakította a társadalmi hálózatok dinamikáját is. Mivel egy-egy nagyobb társadalmi hálózat sohasem alszik, vagyis a kapcsolatok egy része mindig aktív magatartást tanúsít, mindig képes arra, hogy a célnak megfelelő reakciót adjon egy-egy felmerülő jelenségre, hírre, információra, és akár ennek megfelelően „riassza” a hálózat többi tagját.

A kibertér fontos hatása, hogy az ahhoz való csatlakozás révén lehetővé válik, hogy befolyásolják az éntudatot, képessé téve egyes aktorokat annak módosítására, „átprogramozására”. Mindez azért alakulhat így, mert a kibertér egyes szegmensei lényegében szándékosan úgy vannak tervezve, hogy az egyén sajátos világnézete, érdeklődési köre, tervei, céljai, függőségei mentén kapjon információt, érjen el felületeket, jusson hozzá kapcsolódó termékekhez. Lényegében a közösségimédia-platformok ezen felismerés mentén szervezik saját üzleti modelljüket.¹² Mindez úgy történik, hogy ez a speciális közeg új esélyt kínál az egyéneknek: egy más közösséghez tartozást, a lehetőségek tárházát, akár úgy is, hogy látszatra a hagyományos létezése nem változik, valójában azonban teljesen felülírja azt. A „[c]yberkörnyezetben csökken az ítélőképesség és nő az impulzivitás, némileg hasonlóan ahhoz, ahogyan az alkohol hat ránk. A cyberközeg sajátos jellemzői – a külső kontroll vagy felügyelet

¹⁰ Farkas Ádám: *A védelem és biztonság-szavatolás szabályozásának alapkérdései Magyarországon*. Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2022. 41.

¹¹ Baranyi Péter et al.: Introducing the Concept of Internet of Digital Reality – Part I. *Acta Politechnica Hungarica*, 18. (2021b), 7. 225–240; Baranyi Péter et al.: Internet of Digital Reality: Infrastructural Background – Part II. *Acta Politechnica Hungarica*, 18. (2021a), 8. 91–104.

¹² Tökéletes példái ennek a szűrőbuborék-rendszerek és a kapuőrök tevékenysége. Lásd Koltay András: A social media platformok jogi státusa a szólásszabadság nézőpontjából. *In Media Res*, 8. (2019), 1. 1–56.

hiánya, a névtelenség, a távolság, a fizikai elkülönültség érzete – elősegítik a gátlások levetkőzését.”¹³

Ez a kontrollvesztés önmagában növeli az ismeretlenek közötti szindikalizáció lehetőségét. Ez egy olyan robbanásszerű kvantitatív változást jelent, amely ennek köszönhetően kvalitatív jellemzőit is módosítja a társadalmi hálózatoknak. Ugyanis az új hálózatok méretüket tekintve minden korábbi társadalmi kapcsolati hálót meghaladnak, és számuk és méretük folyamatosan gyarapodik. Ehhez hozzájárul, hogy míg korábban a közösség egy földrajzilag jól lehatárolható területre összpontosult, és ezen belül tudtak kialakulni az azonos elvek mentén cselekvő személyek kapcsolatrendszerei is, mára ez teljesen átalakult. Így bár hagyományos térben az egyéni kapcsolatok visszaszorulása, elszorvadása figyelhető meg, addig a kibertérben az emberi létezés fokmérője a hálózathoz tartozás lett.¹⁴ Az egyén mindent megtesz, hogy egy-egy közösség részese lehessen, míg mások hagyományos térbeli céljaik eléréséhez használják az általuk vagy mások által kialakított hálózatokat. Emellett viszont az alaptényezője változik meg a társadalmi hálózatnak, hiszen korábban a társadalmi hálózatok bizalmi oldalát a lokalitás, a kölcsönös ismertség adta, ebből adódóan voltak erősek a kisebb helyi hálózatok és gyengébbek a nagyobb, regionális vagy országos hálózatok; ez viszont átalakul, mivel ezeknél a hálózatoknál a hálózat erőssége már nem földrajzilag körülírható, sokkal inkább a benne megjelenő erősebb individuumok jelenléte vagy egy mindenek fölé helyezett cél primátusa jelenti az összetartó és bizalmi kapcsolatot. Erős vezető(k), tagok vagy egy vallásként tisztelt cél rendkívüli kötőerőt jelent ezekben a hálózatokban. Előbbiek maguk determinálják a hálózat makrotulajdonságait, utóbbi viszont a tagok kollektív tudata mentén alakulhat, mert egy magasztos cél lehet pozitív, de szélsőséges mentalitással társulva biztonsági kockázatot is jelenthet. Utóbbiak megfigyelhetők voltak a korábbi társadalmi hálózatok esetében is, azonban itt, ha emellé rendeljük a kvantitatív és technológiai jellemzőket is, valamint a társadalmi struktúra egy részének a társadalmi totalitáson kívülre kerülését, ami lehetővé teszi az egyes cselekmények relativizálását, mivel lehet olyan cél, amit a belső társadalmi struktúra ellenérzéssel fogad, míg a külső akár támogat is vagy fordítva (erre alkalmas példa lehet a migrációval kapcsolatos állásfoglalások, Black Lives Matter mozgalomra és utóhatásaira adott eltérő válaszok), így a hatalmi viszonyban lévők részéről érzékelhetően jelentősebb potenciállal/kockázattal bíró hálózatok rajzolódnak ki, amit a lassabb ismerttetett tulajdonságok tovább erősítenek.

Tovább vizsgálva a formáló körülményeket, meg kell állapítani, hogy a kibertér növeli a kialakított hálózatok testreszabottságát is, mivel a kialakult közösségek tagjai közötti interakciók a kibertérnek köszönhetően már országhatárokat, sőt

¹³ Mary Aiken: *Cybercsapda. Hogyan változtatja meg az online tér az emberi viselkedést?* Ford. Török Csaba. Budapest, Harmat Kiadó, 2020. 35.

¹⁴ Pintér Róbert: Úton az információs társadalom megismerése felé. In Pintér Róbert: *Az információs társadalom. Az elmélettől a politikai gyakorlatig*. Budapest, Gondolat – Új Mandátum, 2007. 25.

kontinenseket is átlépnek. A hasonlóan gondolkodó egyének határok nélkül tudnak kommunikálni, egymással információkat megosztani, csoportokat létrehozni, hálózatokat szervezni. Ami tovább erősíti a határokon átnyúló társadalmi struktúráknak a hatalmi pozícióját, hiszen lehetőséget ad, hogy akár információs műveletek mentén alakíthassák egy-egy társadalmi hálózat szemléletét.

Ezzel párhuzamosan pedig fokozódik ezeknek a hálózatoknak a közösségformáló szerepe. Hozzájárul ehhez a hálózatok hiperdiadikus jellege is. A hagyományos térben a viselkedési minták átvétele családtagok, barátok, osztálytársak, kollégiumi szobatársak stb. szokásainak másolásával történik meg, vagyis egy-egy viselkedési minta terjedése a legtöbbször lineárisan valósul meg. Ha ez a lineáris lánc megszakad, akkor ennek az új magatartási formának az átadása is megghiúsul. A hiperdiadikus terjedésnek köszönhetően egy szervezetben, így például egy munkahelyen, kollégiumi közösségben, egyetemen már horizontálissá válik az információáramlás, bonyolultabbak és nehezebben visszakövethetőek a hatások, viszonzthatások. E horizontális terjedést helyezzük át a kibertérbe, ahol a hálózat tagjainak száma több ezerre, tízezerre, sőt akár millióra is emelkedhet. A minta terjedése így már nem egyszerűen hiperdiadikus, hanem szuper-hiperdiadikus. Itt egy-egy viselkedési minta átadásához, víruszerű terjedéséhez nem kell az, hogy minden szereplő azt magáévá tegye, támogassa, elsjátítsa.¹⁵ Az így kialakított hálózatoknak létrejönnek olyan tulajdonságai és funkciói, amelyek az egyéntől elszakadnak, azokra nincsen valós befolyása.¹⁶ Hozzájárul ehhez a kibertérnek a gátlásokat háttérbe szorító jellege, valamint az is, hogy egyes csoportokon belül eltérő aktivitású, eltérő célú és eltérő végletekben gondolkodó szereplők vesznek részt. Ezekből adódóan a kibertérben létrejövő kapcsolati hálózatokban az egyén radikalizálódása rendkívül felgyorsul.

Az egyén radikalizálódása a csoporton belüli aktivitás fokozódása mellett a csoporton túlra ható (kiber)tevékenységekben figyelhető meg, így például közösségi oldalakon történő toborzás, az elveiknek, nézeteiknek megfelelő hírek terjesztése, saját nézeteik igazolása, akár – még nem hagyományos értelemben vett – agresszív módon is. A kontrollt veszített egyén a legtöbb esetben ezzel az agresszióval még jogi normát nem sért. A kiberagresszió fogalma viszont rendkívül szemléletes – „[a] cyberagresszió úgy értelmezhető, mint minden olyan, az egyén negatív érzelmeiből fakadó, cybertérben megnyilvánuló manifesztáció, ami magára a cselekvőre vagy másra nézve negatív hatású, vagy valamely normát sért, de még nem tartalmazza a fenyegetést és a kényszerítést, hanem azok megelőző, bevezető

¹⁵ Gondoljunk bele, a közösségi hálón mennyi olyan „kihívással” (ilyenek voltak többek között a dezodor-, a koronavírus-, a koponyatörő, a kiki-, vagy a tüzes kihívás) találkoztunk az elmúlt években, amelyek a digitális közösséghez tartozó egyének legtöbbjét sokkolták, mégis óriási számú követőre találtak. Lásd bővebben: Coronavirus challenge és a legveszélyesebb netes kihívások. *Generali előrelátók blog*, 2020. április 24.

¹⁶ Nicholas A. Christakis – James H. Fowler: *Kapcsolatok hálójában. Mire képesek a közösségi hálózatok, és hogyan alakítják sorsunkat?* Budapest, Typotex, 2010. 38–41.

szakasza”¹⁷ –, hiszen kifejezésre juttatja, hogy az egyén itt lépi át a Rubicont, vagyis teszi meg az első olyan lépéseket, amelyek a későbbi, már akár bűncselekményi tényállást megvalósító cselekményhez vezethetnek. Sajnálatos módon a kibertér gátlásmódosító hatása okán az elkövető legtöbbször – bár hagyományos térben leg többjük ilyen nem tenne – nem is érzékeli, hogy rendkívüli mértékben átlépte az emberek között kialakult kommunikáció hétköznapi normáit.

A radikalizálódása a hálózathoz kapcsolódó szereplőknek eltérő fokozatot ölt, pontosan abból adódóan, hogy eltérő magatartási mintákat vesznek át a szereplők a csoport többi tagjától. Eltérő lesz az is, hogy miként viszonyul egy-egy tag a belső vagy külső társadalmi struktúrához, vagy azok mindegyikéhez. Ugyanis már a korábbi történeti közegben kialakult az az ereje az egyes társadalmi hálózatoknak, hogy a társadalmi struktúrában kevésbé jelentősek is hatni tudnak a kialakult társadalmi viszonyrendszerre. Így az a társadalmi hálózat, amely a belső társadalmi struktúrával szembehelyezkedik, de a külső társadalmi struktúrát támogatja, lehetőségként jelenik meg a külső tényezők számára – olyan lehetőségként, amely később támogatható, erősíthető társadalmi töréspontot eredményezhet. Emellett a mindkét struktúrát bíráló, támadó és tagadó hálózatok radikalizálhatóságában rejlik a legnagyobb potenciál, hiszen ezen csoportok kisebb ráfordítással is szélsőséges radikalizmusra hajlamosak.

A fentiek okán megállapítható, hogy ezen szuper-hiperdiadikus mintakövetésen alapuló nagy méretű hálózatok esetében a hálózat méretéből adódóan kevésbé jellemző a homogén magatartási minták átvétele. A csoport attitűdje, a radikalizmusának szintje tehát nem az egyén felől határozható meg, mivel „[a] kapcsolati hálóknak makroszintű tulajdonságai vannak. A makroszintű tulajdonságok olyan, az egészre jellemző új vonások, amelyek a részek közötti kölcsönhatásokra és köztük fennálló kapcsolatokra vezethetők vissza.”¹⁸ Ez pedig adódik a kvantitatív jellemzőkön túl abból is, hogy az egyes tagok a korábban meghatározott célok mentén eltérően reagálnak a társadalmi struktúrákra. És míg korábban a jelentősebb társadalmi hálózatok vagy közvetlen kapcsolatban voltak a társadalmi struktúrával, vagy törekedtek arra, hogy abba beolvadjanak, addig az elmúlt évtizedekben ezen hálózatok egy része kimondottan alkalmas arra, hogy ezen struktúrák valamelyikét felszámolja.

Melyik társadalmi hálózat tud ilyen potenciált magában hordozni? Érdemes itt idézni a világhírű magyar hálózatkutató, Barabási Albert-László szavait: „Igen, tényleg van szólásszabadság a hálón. Azonban annak nagyobb a valószínűsége, hogy hangunk túl gyenge ahhoz, hogy meghallják. Azokat az oldalakat, amelyeknek csak kevés bejövő mutatója van, lehetetlen véletlen barangolással megtalálni. Ehelyett örökké a középpontokhoz vagyunk irányítva.”¹⁹ Ezen következtetést erősíti egy

¹⁷ Kiss Tibor: *Agresszió a cybertérben*. Budapest, Nemzeti Közszerződési Egyetem, 2020. 28.

¹⁸ Christakis-Fowler (2010): i. m. 42.

¹⁹ Barabási Albert-László: *Behálózva – A hálózatok új tudománya*. Budapest, Libri Kiadó, 2020. 191.

Avaaz-jelentés, amely a 2020-as amerikai elnökválasztás után készült. Ennek első fejezete azt az egyértelműnek ható alcímet kapta, hogy „Miként hagyta cserben a Facebook az amerikai választókat”. A választások után Sheryl Sandberg, a Meta ügyvezető igazgatója azt mondta, hogy a Facebook óriási erőfeszítéseket tett a dezinformáció ellen, mégpedig sikerrel. Eredményként azonosíthatták, hogy – véleményük szerint – nem volt orosz beavatkozás ebben az időszakban a platform határozott fellépése miatt. Az Avaaz azonban rámutatott arra, hogy a vizsgált száz legnézettebb *fake* poszt így is 162 milliós nézettséget ért el, emellett hangsúlyozta, hogy ez a száz poszt nem az összes közül a száz, hanem a Facebook tényellenőrei által azonosított *fake news* közül a száz legnézettebb. A jelentés rátért arra is, hogy amíg a platformok kizárólag önértékelést végeznek, továbbá a kutatók és a hatóságok számára csak azok az információk lesznek elérhetők, amelyeket kiadnak, addig a dezinformáció valós mértékéről még becsléseket is nehéz adni.²⁰ Jól mutatják e fenti gondolatok, hogy a kibertérben a társadalmi hálózatok soha nem látott mértékben formálhatók, és ezáltal szembeállíthatók a társadalmi struktúrával, amihez hozzájárul a közösségi médiaplatform-szolgáltatók üzleti gyakorlata, amit eszközként használnak a hibrid konfliktusok ellenérdeklő felei is.

Az egyéni reziliencia kialakítására tett lépések – ez lehet a Nyugat válasza a problémára?!

A 21. században az átalakult társadalmi, gazdasági és biztonsági környezet megváltoztatta az állam működését és az államról való gondolkodást, megteremtve a technológia nóvumaira épülő, arra reagáló állammodellt, a cyberfare state-et. Ezen új állammodellnek – bár első pillantásra nem úgy tűnhet – a központi aktora az egyén, hiszen az a társadalmi, gazdasági és állami sérülékenységgel centrális figurájává vált a technológiai újításoknak köszönhetően. Jól illusztrálja ezt, hogy az informatikai szakemberek a leggyengébb láncszemként tekintenek a humán faktorra. Nem véletlenszerű, hogy a nem jogállami keretek között működő államok (smart total control cyberfare state) esetében mindent megtesznek annak érdekében, hogy az ezen aktor jelentette biztonsági kockázatokat a lehetőségekhez mérten redukálják, úgy, hogy az egyéni szabadságjogokat figyelmen kívül hagyó korlátozó, megfigyelő rendszereket építenek ki, mindezt jóléti megoldásoknak álcázva.

Ezzel szemben a jogállami keretek között működő államok esetében a társadalmi reziliencia kialakítása során még csak az utóbbi években indult meg annak felismerése, hogy az állami, önkormányzati és gazdasági szereplőkön túlmutató, ellenálló képességet növelő programokat, szabályozásokat kell kialakítani. Azonban ezek például a kínai, orosz vagy szingapúri rendszerekhez képest időbeli csúszásban vannak,

²⁰ *Facebook from Election to Insurrection: How Facebook Failed Voters and Nearly Set Democracy Aflame.* Avaaz Report, 2021. március 18.

és sok esetben még csupán bábállapotban léteznek. Már az is üdvözlendő, hogy a NATO és az Európai Unió néhol megcsúszva, de azonosította ezen fenyegetések körét, és elkezdett fejlődési programokat kidolgozni. Ezt tükrözi vissza a NATO modern technológiákkal kapcsolatos Emerging Disruptive Technology (EDT) rendszere, amelyhez kapcsolódó tanácsadó csoport 2020-as jelentésében hangsúlyozta ezen technológiák társadalmi hatásait, valamint azt, hogy szükséges ez a területen az oktatás és képességfejlesztés. Utóbbiak azért elengedhetetlenek, mert ezek a technológiák rendkívül bonyolult rendszereket eredményeznek, ahol a döntéshozóknak (politikai, gazdasági), illetve az egyéneknek úgy kell eligazodniuk, hogy nem rendelkeznek átfogó ismeretekkel, amelyek viszont nélkülözhetetlenek volnának a NATO versenyképességéhez akár szervezeten belül, akár azon kívül is. Ami viszont nem jelent egyet azzal, hogy minden szereplőnek mélyszélességi műszaki ismeretekkel kell rendelkeznie, vagyis a cél sokkal inkább a tudatosság, az alapismeretek szintjének növelése, azaz a technológiai műveltség magasabb szintre helyezése. A szervezeten belüli képesség növelésére kínálnak lehetőséget az egyes NATO képzési központok. Emellett elkerülhetetlennek vélik az együttműködés kialakítását a magánszektorral és a felsőoktatással is. Szintén kiemelik, hogy ezen együttműködések lehetőséget teremthetnek külsős ismeretterjesztő projekteknek, továbbá egyetemi képzések fejlesztésének, amelynek keretében a NATO mester- és doktori képzések esetében ösztöndíjprogramokat hozhatna létre, ezzel növelve társadalmi elfogadottságát is.²¹ A NATO, bár a gazdasági és akadémiai szférára irányultan megkezdte az együttműködés kereteinek kialakítását (ilyen a DINA [Defence Innovation Accelerator for the North Atlantic] és az EDT-hez kötődő tudományos tanácsadó testület is), azonban az egyénekre irányuló programok a gyakorlatban még váratnak magukra, pedig a szakértők között egyre inkább világossá vált, hogy „[a]z emberek tömeges adatainak [...] elemzésével és felhasználásával cselekvésünk, gondolkodásunk befolyásolható [...] technikailag lehetővé vált az egyes társadalmak integritásának, az állami intézmények iránti bizalom kártékony befolyásolása is”.²²

Az Európai Unió²³ 2019-es globális kül- és biztonságpolitikai stratégiája e területen nem mutat újdonságot. Szintén hangsúlyozza az együttműködés szükségességét az egyes szférákkal, valamint a kiberbiztonság területén a NATO-val való kapcsolatok megerősítését.²⁴ Ilyen együttműködési projekt például a dezinformációs szcenáriók korai felismerésére és a reagálás javítására szolgáló 2015-ben felállított

²¹ NATO Advisory Group on Emerging and Disruptive Technologies. Annual Report. Brüsszel, NATO Emerging Security Challenges Division, 2020. 10. 14–15.

²² Molnár Ferenc: A reziliencia kérdése és a NATO. *Védelmi-biztonsági Szabályozási és Kormányzás-tani Műhelytanulmányok*, 1. (2021), 15. 6.

²³ Az Európai Unió stratégiai autonómiája az EDT területén sok tekintetben irreálisnak tűnik. Lásd Ester Sabatino – Alessandro Marrone: Emerging Disruptive Technologies: The Achilles' Heel for EU Strategic Autonomy? *LAI Istituto Affari Internazionali*, (2021), 31.

²⁴ The European Union's Global Strategy – Three years on, looking forward. 2019. 11–13. Az ezen dokumentum alapját jelentő korábbi stratégiát lásd Molnár Anna: Közös jövőkép, közös cselekvés:

East StratCom Task Force elnevezésű munkacsoport. 2018-ban cselekvési tervet fogadtak el a félretájékoztatással szemben. Ez osztott tagállami és uniós intézményi fellépésről rendelkezett. A koordinált válasz négy pilléren nyugszik, a negyedik pillér a tudatosság növelése és a társadalom rezilienciájának javítása. A társadalmi ellenálló képesség növelése érdekében előirányozták a független tényellenőrzőkből álló csoportok létrehozását, akiknek feladata a dezinformálás feltárása és a közvélemény tájékoztatása.²⁵ 2020 decemberében az Európai Bizottság előterjesztette az Európai Demokráciára vonatkozó cselekvési tervet. Ennek negyedik pontja szól a dezinformáció elleni küzdelemről. Szorosabb együttműködés kialakítása mellett érvel a magánszektorral, a civil társadalommal, a tudományos élettel és az unió nemzetközi partnereivel, azonban még mindig csak a hibrid konfliktus jobb megértése érdekében. A Bizottság álláspontja abban nem változott, hogy a dezinformálás elleni küzdelem egyik legfontosabb terepe a polgárok médiatudatos nevelése.²⁶

Az unió üdvözlendő kísérletei közé tartozik a Bizottság által előterjesztett Digitális szolgáltatások egységes piacáról szóló rendeletjavaslat. A rendelet célja az Alapjogi Chartában biztosított jogokat tiszteletben tartó, de biztonságos, kiszámítható és megbízható online környezet kialakítása. „Mindez – a várakozások szerint – az emberi jogok, a jogegyenlőség, a jogbiztonság, a szabadság és a demokrácia, azaz összefoglalóan a jogállam megerősödéséhez vezet el majd, hiszen az egységes felelősségi szabályok, az átláthatóság és kiszámíthatóság az online környezetben visszaszorítja a fentebb tárgyalt hamis hírekkel és dezinformációval kapcsolatos problémákat.”²⁷ A rendelet továbbra is engedi a tartalommoderálást a platformok részéről. Egyértelműen előrelépés, hogy a platformok felelősségének megállapítását is lehetővé teszi a javaslat a jogellenes tartalmakért. A tartalommoderálással kapcsolatban előírja, hogy évenként erről kötelesek jelentést tenni a szolgáltatók. A beszámoló részének kell lenniük az önálló tartalommoderálás okainak és az arra indokot adó (belső vagy külső) szabályozási alapoknak, s az ezekkel összefüggő belső panaszkezeléssel kapcsolatos információk megosztásának és értékelésének. Utóbbiból következik, hogy a platformoknak a korábbitól eltérően átlátható belső panaszkezelési rendszert kell működtetniük, aminek része az eltávolítás, a hozzáférhetetlenné tétel, a szolgáltatás felfüggesztésével vagy megszüntetésével kapcsolatos döntések felülvizsgálata és indokolása. Ezek már önmagukban olyan szabályok,

erősebb Európa. Az EU globális kül- és biztonságpolitikai stratégiája. *Nemzet és Biztonság*, 9. (2016), 2. 75–85.

²⁵ Európai Bizottság: *Közös Közlemény az Európai Parlamentnek, az Európai Tanácsnak, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. Cselekvési terv a félretájékoztatással szemben.* JOIN(2018)36 végleges (2018. december 5.).

²⁶ Európai Bizottság: *A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának az Európai Demokráciára vonatkozó cselekvési tervről.* COM(2020)790 végleges (2020. december 3.).

²⁷ Gosztorny Gergely: *Cenzúra Arisztotelésztől a Facebookig. A közösségi média tartalomszabályozási gyakorlatának komplexitása.* Budapest, Gondolat Kiadó, 2022b. 145.

amelyek előrelépést jelenthetnek az egyéni felhasználók védelme érdekében, és így segíthetnek a társadalmi reziliencia kialakításában, hiszen többek között a dezinformációs műveletek hatékonyságát csökkenthetik. Ilyennek tekinthető a rendelet 20. cikke is, amelynek értelmében az online platformok felfüggeszthetik a szolgáltatás nyújtását olyan személynek, aki gyakran oszt meg nyilvánvalóan jogellenes tartalmat. Ezt szolgálja még az online hirdetések átláthatósága is, hiszen visszakövethetőbbé teszi az egyes félrevezető tartalmakat. Az online óriásplatformokkal szembeni plusz elvárás a kockázatértékelés, amely kiterjed olyan tartalmak megjelenhetőségére, amelyek a társadalmi párbeszédre negatív hatással vannak. Ezen esetekben a kockázatcsökkentési intézkedés keretében történhet többek között tartalommoderálás vagy a szolgáltatás korlátozása.²⁸

Összegzés

Az elmúlt évtizedekben a társadalmi hálózatok jelentős változásokon mentek át, amelyek jellemzőiket mind kvantitatív, mind kvalitatív oldalon átírták. A jelenkor társadalmi hálózatai méretüket tekintve soha nem látott kapcsolódási pontokat foglalnak magukba, mivel a kibertér lehetővé tette a földrajzilag nem kötött, lokális hálózatok meghaladását. Ez pedig elvezet oda, hogy a jelenkor társadalmi hálózatai tematizáltabbak, mint korábban, emellett sokkal inkább a közös cél, érdeklődés az alapja a bizalomnak, mintsem – mint korábban – a lokális ismertség. E hálózatoknak a szindikalizáló ereje jóval túlmutat a korábbi évszázadok hálózatain, és magába olvasztja a hasonlóan gondolkodó, hasonló témák iránt érdeklődő egyéneket, attól függetlenül, hogy ténylegesen mennyire egységes a világnézetük az adott témakörben. Az egyes magatartási minták már nem diadikus vagy hiperdiadikus módon terjednek a kapcsolati pontok között, hanem szuper-hiperdiadikus módon, amiből adódóan egy-egy magatartási séma nehezebben visszakövethető, átvétele nehezebben vagy egyáltalán nem megakasztható. Utóbbi jellemzők teszik, hogy ezen hálózatok a korábbi évszázadok hálózataihoz képest már nem definiálhatók a mikro-, vagyis az egyéni jellemzők oldaláról, hanem sokkal inkább makrotulajdonságok jellemzik őket.

Fontos tapasztalás, hogy a társadalmi struktúra és a társadalmi hálózatok kapcsolata átalakult. Míg a korábbi évszázadokban az volt a jellemző, hogy a társadalmi struktúrában jelentős szerepet betöltő társadalmi hálózatok voltak csak képesek befolyásolni a társadalmi struktúra viszonyait, esetleg biztonsági kockázatként megjelenni, addig leginkább a 19. század közepétől azt figyelhetjük meg, hogy a társadalmi struktúrában kevésbé jelentős társadalmi hálózatok is képesek

²⁸ Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (2022. október 19.) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (digitális szolgáltatásokról szóló rendelet). L 277/1 (2022. október 27.). 6–28. cikk.

hatni a társadalmi struktúrára, és sok esetben képesek voltak veszélyeztetni a nemzeti biztonságot is. Azonban a kibertér megjelenéséig ezen társadalmi hálózatok is mindig a társadalmi struktúrára reagáltak, vagy be kívántak olvadni, vagy módosítani kívánták azt. Ezzel szemben az utóbbi évtizedek átalakulása mára oda vezetett, hogy a társadalmi totalitáson kívüli társadalmi struktúra(k) jött(ek) létre (például ilyenek lehetnek egyes franchise típusú terrorszervezetek, ideológiai alapú transznacionális szerveződések), így akár az egyes társadalmi hálózatok már nem is a társadalmi totalitás szerinti társadalmi struktúrájukhoz képest definiálják magukat, hanem egy társadalmi totalitáson túli társadalmi struktúrához képest, amely révén a társadalmakon belül további töréspontok keletkezhetnek.

E problémákra a cyberfare state modell két pólusa eltérő választ ad. Míg a nem vagy kevésbé demokratikus államok (például Kína, Oroszország, Szingapúr, India stb.) totális kontroll irányába mozdultak el az egyének vonatkozásában, addig a jogállami keretek között mozgó államalakulatok inkább az egyéni tudatosság erősítése mellett törtek lándzsát. E területeken az elmúlt években a felismerésen túl azonban összességében – az egyénre irányuló programok tekintetében – előrelépés nem történt, a független tényellenőrök rendszerének felállítása lényegi elmozdulást nem eredményezett, eredményezhetett az egyéneken nyugvó biztonsági kockázatok mátrixában. Még úgy sem, hogy „[a] NATO a kollektív védelem egyik kulcsfontosságú fejlesztési irányát látja a rezilienciában, ami azt is jelenti, hogy a szövetség szintjén hatékony ellenálló képesség nem korlátozódik a kormányzatok működésére, hanem azt rétegzettként értelmezi. Ez a rétegzettség a kellően informált, tudással felvértezett egyénektől és civil társadalomtól, a civil (állami, piaci) és katonai szervezeteken át, a teljes társadalmak ellenálló képességét jelenti.”²⁹ Mindezzel szemben azt látjuk, hogy továbbra is holisztikus mind a NATO, mind az EU megközelítése. Annak ellenére van ez így, hogy minden fontosabb és a témát érintő stratégiai dokumentumban megállapítják a rendszerek összetettségét, bonyolultságát, ahol „az érintett emberek és csoportok képességbeli [...] heterogenitása nem alakult át gyökeresen”,³⁰ vagyis az egyének és az általuk létrehozott társadalmi hálózatok lényegében nincsenek felvértezve azzal a tudással, amelynek köszönhetően önmagukat meg tudják óvni az ártó tényezőktől. Nyilván ez nem jelenti azt, hogy a kibertér valamennyi ártalmával szemben kizárólag szövetségi, uniós és állami programoknak köszönhetően tud ellenállni az egyén, azonban a megfelelő és átfogó nevelési, oktatási és képzési programok, valamint a káros hatásokat jobban lekövető jogalkotás³¹ hiányában

²⁹ Molnár (2021): i. m. 12.

³⁰ Farkas Ádám – Spitzer Jenő: Az információs korszak és az állami reziliencia egyes kérdései. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok*, 1. (2021), 18. 19.

³¹ Jogalkotásban az egyént is érintő egyes területeken már találkozunk megoldásokkal, azonban az átfogó szemléletű megoldások hiányoznak itt is. Lásd bővebben Szépvölgyi Enikő: Az európai uniós reklámszabályozás és a kiskorúak védelme – a digitalizáció kihívásai. *Külgazdaság*, 66. (2022), 5–6. 109–122; Sorbán Kinga: A társadalmi tudatosság és az online közvetítő szolgáltatók szerepe az informatikai bűnözés elleni fellépésben. *Iustum Aequum Salutare*, 16. (2020b), 3. 179–192; Sorbán

nem lehet kialakítani a szükséges egyéni, társadalmi, nemzeti és szövetségi ellenálló képességet. A feladat összetett és „[...] ahhoz, hogy felnőjünk a cybertérben felmerülő új problémákhoz, arra lenne szükség, hogy a törvényeink és az oktatási rendszerünk ugyanolyan rohamos tempóban kövessék a változásokat, mint ahogyan a technológiákat fejlesztik és piacra dobják – ez pedig gyakorlatilag lehetetlen”.³² Azonban a deklarációk szintjét már a nyugati demokratikus alapokon nyugvó államoknak is meg kell haladniuk, mivel az egyénre irányuló – jogállami kereteken nyugvó – tényleges cselekvés hiányában behozhatatlan stratégiai hátrányba kerülnek a másik pólust jelentő államokkal szemben.

Felhasznált irodalom

- Aiken, Mary: *Cybercsapda. Hogyan változtatja meg az online tér az emberi viselkedést?* Ford. Török Csaba. Budapest, Harmat Kiadó, 2020.
- Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (2022. október 19.) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (digitális szolgáltatásokról szóló rendelet). L 277/1 (2022. október 27.).
- Barabási Albert-László: *Behálózva – A hálózatok új tudománya*. Budapest, Libri Kiadó, 2020.
- Baranyi Péter – Csapó Ádám – Budai Tamás – Wersényi György: Internet of Digital Reality: Infrastructural Background – Part II. *Acta Politechnica Hungarica*, 18. (2021a), 8. 91–104. Online: http://acta.uni-obuda.hu/Wersenyi_Csapo_Budai_Baranyi_115.pdf
- Baranyi Péter – Csapó Ádám – Budai Tamás – Wersényi György: Introducing the Concept of Internet of Digital Reality – Part I. *Acta Politechnica Hungarica*, 18. (2021b), 7. 225–240. Online: http://acta.uni-obuda.hu/Baranyi_Csapo_Budai_Wersenyi_114.pdf
- Castells, Manuel: *The Information age. Economy, Society, and Culture*. I. kötet. *The Rise of the Network Society*. 2. kiadás. Oxford, Blackwell Publishing, 2010.
- Christakis, Nicholas A. – James H. Fowler: *Kapcsolatok hálójában. Mire képesek a közösségi hálózatok, és hogyan alakítják sorsunkat?* Budapest, Typotex, 2010.
- Coronavirus challenge és a legveszélyesebb netes kihívások. *Generali előrelátók blog*, 2020. április 24. Online: <https://blog.generalielorelatok.hu/biztonsag/coronavirus-challenge-es-veszelyes-internetes-kihivasok/>
- Európai Bizottság: *A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának az Európai Demokráciára vonatkozó cselekvési tervről*. COM(2020)790 végleges (2020. december 3.)
- Európai Bizottság: *Közös közlemény az Európai Parlamentnek, az Európai Tanácsnak, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. Cselekvési terv a félretájékoztatással szemben*. JOIN(2018)36 végleges (2018. december 5.)

Kinga: A bosszúpornó és deepfake pornográfia büntetőjogi fenyegetettségének szükségességéről. *Belügyi Szemle*, 68. (2020a), 10. 8–104.

³² Aiken (2020): i. m. 214.

- Facebook: From Election to Insurrection. How Facebook Failed Voters and Nearly Set Democracy Aflame.* Avaaz Report. 2021. március 18. Online: https://secure.avaaz.org/campaign/en/facebook_election_insurrection
- Farkas Ádám: *A védelem és biztonság-szavatolás szabályozásának alapkérdései Magyarországon.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2022.
- Farkas Ádám – Spitzer Jenő: Az információs korszak és az állami reziliencia egyes kérdései. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok*, 1. (2021), 18. Online: https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/VBSZK%20M%C5%B1helytanulm%C3%A1nyok_2021_18_Farkas-Spitzer_Az%20inform%C3%A1ci%C3%B3s%20korszak%20%C3%A9s%20az%20%C3%A1llami%20rez%C3%ADliencia%20egyes%20k%C3%A9rd%C3%A9sei.pdf
- Gosztonyi Gergely: Special Models of Internet and Content Regulation in China and Russia. *ELTE Law Journal*, 9. (2021), 2. 87–99. Online: <https://doi.org/10.54148/ELTELJ.2021.2.87>
- Gosztonyi Gergely: A kínai internetcenzúra modellje. *Pro Futuro*, 12. (2022a), 1. 1–9. Online: <https://doi.org/10.26521/profuturo/2022/1/11118>
- Gosztonyi Gergely: *Cenzúra Arisztotelésztől a Facebookig. A közösségi média tartalomszabályozási gyakorlatának komplexitása.* Budapest, Gondolat Kiadó, 2022b.
- Kelemen Roland: Cyberfare state – Egy hibrid állammodell 21. századi születése. *Military and Intelligence CyberSecurity Research Paper*, 2. (2022), 1. 1–32.
- Kiss Tibor: *Agresszió a cybertérben.* Budapest, Nemzeti Közszerzői Egyetem, 2020.
- Koltay András: A social media platformok jogi státusa a szólásszabadság nézőpontjából. *In Media Res*, 8. (2019), 1. 1–56.
- Machlup, Fritz: *The Production and Distribution of Knowledge in the United States.* Princeton, Princeton University Press, 1962.
- Molnár Anna: Közös jövőkép, közös cselekvés: erősebb Európa. Az EU globális kül- és biztonságpolitikai stratégiája. *Nemzet és Biztonság*, 9. (2016), 2. 75–85.
- Molnár Ferenc: A reziliencia kérdése és a NATO. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok*, 1. (2021), 15. 1–13.
- Moore, Gordon E.: Cramming More Components onto Integrated Circuits. *Electronics*, 38. (1965), 8. 114–117.
- NATO Advisory Group on Emerging and Disruptive Technologies.* Annual Report. Brüsszel, NATO Emerging Security Challenges Division, 2020. Online: www.nato.int/nato_static_fl2014/assets/pdf/2021/3/pdf/210303-EDT-adv-grp-annual-report-2020.pdf
- Németh Richárd: Kibertámadások gazdasági vonatkozásai a vállalati szférában. In Dernóczy-Polyák Adrienn (szerk.): *Kutatási jelentés 1.* Győr, Universitas-Győr Nonprofit Kft., 2019. 307–325.
- Pintér Róbert: Úton az információs társadalom megismerése felé. In Pintér Róbert: *Az információs társadalom. Az elmélettől a politikai gyakorlatig.* Budapest, Gondolat – Új Mandátum, 2007.
- Pongrácz Alex: A globalizáció toposzai. In Kecskés Gábor (szerk.): *Doktori Műhelytanulmányok 2014.* Győr, Széchenyi István Egyetem Állam- és Jogtudományi Doktori Iskola, 2014. 157–168.
- Pongrácz Alex: A hálózat csapdájában? Globalizáció és totalitás. In Farkas Ádám (szerk.): *Védelmi alkotmányosság az új típusú biztonsági kihívások erőterében.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2018. 43.
- Pongrácz Alex: Variációk hibrid állammodell-építésre. *Military and Intelligence Cybersecurity Research Paper*, 2. (2022), 3. 3–8.

- Sabatino, Ester – Alessandro Marrone: Emerging Disruptive Technologies: The Achilles' Heel for EU Strategic Autonomy? *LAI Istituto Affari Internazionali*, (2021), 31. Online: www.iai.it/sites/default/files/iaicom2131.pdf
- Sorbán Kinga: A bosszúpornó és deepfake pornográfia büntetőjogi fenyegetettségének szükségességéről. *Belügyi Szemle*, 68. (2020a), 10. 81–104. Online: <https://doi.org/10.38146/BSZ.2020.10.4>
- Sorbán Kinga: A társadalmi tudatosság és az online közvetítő szolgáltatók szerepe az informatikai bűnözés elleni fellépésben. *Iustum Aequum Salutare*, 16. (2020b), 3. 179–192.
- Szépvolgyi Enikő: Az európai uniós reklámszabályozás és a kiskorúak védelme – a digitalizáció kihívásai. *Külgazdaság*, 66. (2022), 5–6. 109–122. Online: <http://doi.org/10.47630/KULG.2022.66.5-6.109>
- The European Union's Global Strategy – Three Years on, Looking Forward*. 2019. Online: www.eeas.europa.eu/sites/default/files/eu_global_strategy_2019.pdf
- Toffler, Alvin: *A harmadik hullám (információs társadalom A-tól Z-ig)*. Budapest, Typotex, 2001.
- Z. Karvalics László: „A tudás termelése és elosztása az Egyesült Államokban”: Fritz Machlup újraértékelése az információs társadalom elmélettörténetében. *Információs Társadalom*, 9. (2009), 2. 20–34.

Vákát

II. rész

Platformok és szabályok



Vákát

Zódi Zsolt

A platformszabályozás megold(hat)atlan dilemmái



Az elmúlt években az internetes platformok csaknem minden országban a szabályozók célkeresztjébe kerültek, és megszületett egy sor nemzeti és EU-s norma. A szabályozás elég részletesnek tűnik, ugyanakkor már most lehet látni, hogy ezek a normák néhány kérdésre biztosan nem fognak választ adni. A tanulmány ezek közül a nehezen megoldható kérdések közül elemez néhányat: az általános monitorozási kötelezettség hiányát mint a platformjog kulcsszabályát, és ennek problematikus voltát, a kiterjedt ex ante szabályozás kockázatait, az adatok szabályozásával kapcsolatos dilemmákat és belső jogi ellentmondásokat, a hagyományos adatvédelmi jog válságát, valamint a nemzetállamok és a platformok sok ponton problematikus viszonyát.

Bevezetés

Az elmúlt években az internetes platformok csaknem minden országban a szabályozók célkeresztjébe kerültek, és megszületett egy sor nemzeti és EU-s norma. Ezek részben ágazatiak,¹ részben a teljes platformscénát horizontálisan szabályozók.² Közös jellegzetességük, hogy túlnyomórészt úgynevezett ex ante szabályokat tartalmaznak, azaz a platformokat folyamatosan bizonyos követelményeknek történő folyamatos megfelelésre szorítják. További jellegzetességük, hogy a középpontjukban a felhasználók védelme és az online veszélyek elhárítása áll, hogy főszabályként

¹ Az Európai Parlament és a Tanács (EU) 2019/1150 rendelete (2019. június 20.) az online közvetítő szolgáltatások üzleti felhasználói tekintetében alkalmazandó tisztességes és átlátható feltételek előmozdításáról. L 186/57 (2019. július 11.) (P2B rendelet); Az Európai Parlament és a Tanács (EU) 2018/1808 irányelve (2018. november 14.) a tagállamok audiovizuális médiaszolgáltatások nyújtására vonatkozó egyes törvényi, rendeleti vagy közigazgatási rendelkezéseinek összehangolásáról szóló 2010/13/EU irányelvnek (Audiovizuális médiaszolgáltatásokról szóló irányelv) a változó piaci körülményekre tekintettel való módosításáról. L 303/69 (2018. november 28.) (AVMS irányelv); Az Európai Parlament és a Tanács (EU) 2019/790 irányelve (2019. április 17.) a digitális egységes piacon a szerzői és szomszédos jogokról, valamint a 96/9/EK és a 2001/29/EK irányelv módosításáról. L 130/92 (2019. május 17.).

² Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (2022. október 19.) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (digitális szolgáltatásokról szóló rendelet). L 277/1 (2022. október 27.) (DSA); Az Európai Parlament és a Tanács (EU) 2022/1925 rendelete (2022. szeptember 14.) a digitális ágazat vonatkozásában a versengő és tisztességes piacokról, valamint az (EU) 2019/1937 és az (EU) 2020/1828 irányelv módosításáról (digitális piacokról szóló jogszabály). L 265/1 (2022. október 12.) (DMA).

nem változtatnak az online szolgáltatók alapvető „felelőtlenségén”, végül hogy nem kérdőjelezik meg az európai adatvédelem alapvető elveit és paradigmáját.

Ezeknek a normáknak a hatékonyságával kapcsolatban még alig vannak tapasztalataink. Az egyetlen kivétel ez alól a legkorábbi *sui generis* platformjogi rendelet, a P2B rendelet, amely már 2019-től hatályban van. Az Observatory of the Online Platform Economy 2021-ben készült jelentése³ az egyetlen olyan kutatás, amely egy szűk spektrumon megmérte az úgynevezett P2B rendeletnek az érvényesülését. Ebből az tűnt ki, hogy a vállalkozások 20–28% közti része (függően a platformtól és a rendelkezéstől) javulást tapasztalt a korábbi kiszolgáltatottságát illetően. Javultak a vita- és panaszkezeléssel kapcsolatos benyomások, a tájékoztatás, a transzparencia.

Ez alapján hátra is dőlhetnénk, eszerint az európai platformjog működik, és bizonyára így lesz majd a fő jogszabállyal, a Digital Services Acttal (DSA) is. Az idilli képbe ugyanakkor bezavar, hogy néhány területen a jelenlegi szabályozás inkább feszültségeket fog okozni, illetve hogy messze nem fog minden problémát megoldani. A platformokkal kapcsolatban egy sor fontos dilemma továbbra is velünk marad még hosszabb időn keresztül. Ez az írás ezekkel a dilemmákkal foglalkozik.

Pontosabban azt a három dilemmát ismertetem, amelyeket a közelmúltban elfogadott vagy a jogalkotók rövid távú terveiben szereplő dokumentumok sem fognak feloldani. Előrebocsátom, hogy ezek közt szándékosan nem szerepeltetem a szólásszabadság dilemmáját, mert ezt annyira szerteágazónak, bonyolultnak és nagy terjedelműnek gondolom, hogy egy ilyen cikkbe egyszerűen nem fér bele. De a dilemmák közt tulajdonképpen első helyen ezt kell említeni.

A három általam tárgyalt dilemma a következő. Az első dilemma, vagy inkább dilemmacsoport *a szabályozás módszerével* függ össze, és több részdilemmát takar. Ezek közül az első a platformszabályozás sarokpontja, az általános monitorozási kötelezettség hiánya mint általános szabály, és ennek fenntarthatósága. A második szabályozási dilemma az *ex ante* szabályozás mint általános módszer megfelelése. A kérdés tehát így hangzik: jó módszer-e a szabályozásra az általános monitorozás kötelezettségének hiányát előíró szabály, és jó módszer-e a széles körű *ex ante* (megfelelési) szabályozás?

A második nagy dilemmacsoport az adatok jogi státuszával kapcsolatos. Mint az köztudott, a platformok üzleti modellje a példátlanul széles körű adatgyűjtésen alapul, a platformok adatfeldolgozó nagyüzemek.⁴ Ez két, egymástól alig elválasztható problémahalmazt vet fel. Az egyik problémahalmaz az adatvédelmi jogban jelentkezik, és röviden arról szól, hogy a platformok alapvető üzleti modellje

³ Lucie Lechardoy – Alena Sokolyanskaya – Francisco Lupiáñez Villanueva: Study on “Support to the Observatory for the Online Platform Economy”. Monitoring of the implementation of the Platform to Business Regulation. (h. n.), Observatory of the Online Platform Economy, 2021.

⁴ Julie Cohen: *Between Truth and Power. The Legal Constructions of Informational Capitalism*. Oxford, Oxford University Press, 2018.

feloldhatatlan ellentmondásban van a hagyományos európai adatvédelmi elvekkel és paradigmával. A másik vetület az, hogy Európában, de máshol is a világon egy új adatjogi szabályozás van kialakulóban, amely logikájában mind a hagyományos magánjoggal, mind pedig a hagyományos adatvédelmi joggal lényegében összeegyeztethetetlen. Ez az új adatjog az adatokra mint erőforrásra tekint, és gyakran azzal a követeléssel lép fel, hogy az adatok a magánjogi dolgokhoz hasonlóan lehessenek tulajdonjog tárgyai. A kérdés itt tehát az, hogy a platformok üzleti modellje és az új adatjogi szemlélet milyen feszültségeket okoz a szabályozásban?

Végül a harmadik dilemmacsoport arról szól, hogy az államok maguk is igen ellentmondásosan viszonyulnak a platformokhoz, és nincsen egyértelmű, széles körben elfogadott narratíva arra vonatkozóan, hogy milyen egy nemzetállam és a platform ideális kapcsolata. Ez olyan kérdésekben manifesztálódik, mint hogy valóban fenyegetést jelentenek-e a nemzetállamokra a platformok, vagy éppenséggel lehetőséget, egészen odáig, hogy az államok maguk is váljanak platformmá.

A szabályozás módszerének dilemmái

Ebben az első részben tehát azokat a dilemmákat ismertetem, amelyek a jelenlegi szabályozás *módszerével* kapcsolatosak. Két témakört érintek. Az első a platformszabályozás legfontosabb szabályával, az *általános monitorozási kötelezettség hiányával* kapcsolatos, a második pedig általában az ex ante szabályozás kockázatait öleli fel.

Az általános monitorozási kötelezettség hiánya mint főszabály

A platformjog egyik, még az 1990-es időkből velünk maradt szabálya az általános monitorozási kötelezettség hiánya, az a szabály, hogy a tárhelyszolgáltatók (amelyek közé a platform is beletartozik) nem kötelesek aktívan figyelni a rendszerükben a tartalmakat.⁵ A szabály eredetileg azért keletkezett, hogy megvédje azokat az éppencsak a szárnyaikat bontogató internetes tartalomszolgáltatókat, akik a felületükön felhasználói tartalmak közzétételét engedélyezték. A szabállyal kapcsolatban a legnagyobb kétely az, hogy egyáltalán fenntartható-e, ugyanis már most is olyan sok kivétellel rendelkezik, hogy jogtechnikailag ugyan lehet főszabálynak tekinteni, a valóságban azonban már inkább kivétel. Három példát említek meg három különböző területről ennek alátámasztására.

⁵ Az Európai Parlament és a Tanács 2000/31/EK irányelve (2000. június 8.) a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem, egyes jogi vonatkozásairól (Elektronikus kereskedelemről szóló irányelv). L 178/1 (2000. július 17.). (E-kereskedelmi irányelv, vagy E-ker irányelv) 14. és 15. cikkek; DSA 8. cikk.

Az első a platformok önként végzett kiterjedt szűrési és moderálási aktivitása.⁶ Mint az köztudott, minden platform, de különösen a közösségimédia-platformok annak ellenére végeznek folyamatos tartalommonitorozást, hogy erre formálisan nem kötelesek. Ennek az a legfőbb magyarázata, hogy szeretnék a felületüket biztonságos térnek tudni, ahol véletlenül sem kerül fel mondjuk egy élőben közvetített tömegmészárlás.⁷ A biztonság mellett az előzetes szűrésnek vannak praktikus okai is. Mint az köztudott, ha az internetre valami felkerül, azt nagyon nehéz onnan leszedni, és ha valóban az a cél, hogy bizonyos tartalomfajták fel se kerüljenek, ezt csak előzetes szűréssel lehet megakadályozni.

Az önkéntes szűrésen kívül bizonyos jogszabályi kötelezettségek és bírói ítéletek is abba az irányba mutatnak, hogy az előzetes monitorozási kötelezettség hiányának inkább csak szimbolikus jelentősége kezd lenni. Az EU új szerzői jogi irányelve például szövegezésében megfordítja a monitorozásikötelezettség-hiányt, és úgy fogalmaz, hogy az online tartalmegosztó szolgáltatók „felelősséggel tartoznak a szerzői jogi védelem alatt álló művek és más védelem alatt álló teljesítmények engedély nélküli nyilvánosságához közvetítéséért”, kivéve, ha „minden tőlük telhetőt megtettek annak biztosítása érdekében, hogy azon konkrét műveket és más védelem alatt álló teljesítményeket, amelyekre vonatkozóan a jogosultak megadták a szolgáltatóknak a lényeges és szükséges információkat, elérhetetlenné tegyék”. A bevett gyakorlat szerint „mindent megtenni” azt jelenti, hogy a platformok a művek digitális lenyomatát adatbázisban tárolják, és már a feltöltéskor ellenőrzik – praktikusán tehát informatikai eszközökkel folyamatosan monitoroznak.

Végül a bírói gyakorlat is a monitorozásikötelezettség-hiány ellen dolgozik. Két ügyet említek meg az Európai Unió Bírósága (EUB) gyakorlatából ennek illusztrálására. Az első egy 2019-es, a Glawischnig-Piesczek v. Facebook ügy. Ebben a felperesre – aki az osztrák parlament zöld képviselője – tettek a Facebookon gyalázkodó, becsmérlő kijelentéseket, amelyeket a képviselő kért eltávolíttatni. Némi huzavona után (a Facebook nem volt hajlandó eltávolítani a tartalmat) végül a bíróság kötelezte a szolgáltatót a poszt eltávolítására, de ezt csak ausztriai területi hatállyal és csak a poszt vonatkozásában tette meg. Ekkorra azonban az internet és a Facebook is már tele volt a becsmérlő kijelentésekkel, így a fellebbezési bíróságon már az a konkrét kérdés merült fel, hogy az eltávolításnak nem kell-e területileg egy szélesebb kört (vagy minden országot), illetve a közlések minden variánsát (azaz tartalmilag azonos közléseket) is magában foglalnia. Az EUB pedig azt a döntést

⁶ Monika Bickert – Brian Fishman: Hard Questions: How We Counter Terrorism. *Facebook News*, 2017. június 15. A policy részletes elemzését lásd Stuart Macdonald – Sara Giro Correia – Amy-Louise Watkin: Regulating Terrorist Content on Social Media: Automation and the Rule of Law. *International Journal of Law in Context*, 15. (2019), 2. 183–197.

⁷ Amy Gunia: Facebook Tightens Live-Stream Rules in Response to the Christchurch Massacre. *Time*, 2019. május 15.

hozta, hogy nemcsak a konkrét posztot, hanem minden „azonos értelmű információt” el kell ebben az esetben távolítani, és mindezt „világsszinten” kell megtenni.⁸ Nem nehéz belátni, hogy az azonos értelmű és minden országra kiterjedő információ eltávolítása géppel végzett általános és folyamatos tartalomszűrést követel.

A másik ügy, amely a monitorozási kötelezettség hiányának mint főszabálynak a kérdését legalábbis – mondjuk így – erősen finomította, az úgynevezett Cyando-ügy volt.⁹ A Cyando-ügy két egymástól függetlenül indult eljárás egyesítése, amelyekben az volt a két kulcskérdés, hogy egyrészt mi minősül „nyilvánossághoz közvetítésnek”, mikor mondhatjuk egy platformra, hogy egy tartalmat „kvázikiadóként” kezel, illetve hogy amennyiben megállapítható, hogy nem az, másodlagosan az egyes platformoknak a felhasználóik által feltöltött tartalmak vonatkozásában milyen kötelezettségei vannak – mit jelent az, hogy a tárhelyszolgáltatónak nem kell monitoroznia a rá feltöltött tartalmakat. Mindkét ügyet a jogtulajdonosok indították, a YouTube esetében egy zenei producer egy zeneszáma, míg a második ügyben az Elsevier kiadó egy kiadványa miatt, a Cyando nevű cég által üzemeltetett fájlmegosztó portál ellen. A YouTube-ügyben a nemzeti bíróság a YouTube-nak adott ígazat, mivel úgy látta, hogy egyrészt a YouTube olyan technikai megoldásokat üzemeltet, amelyekkel folyamatosan képes a szerzői jogsértések nagy részét kiszűrni, másrészt a sérelmezett zeneszámot azonnal eltávolította a felületéről, amikor arról tudomást szerzett. A Cyando esetén a bíróság álláspontja más volt: itt a Cyando egy olyan tárhelyet üzemeltetett, amelyre bárki, ellenőrzés nélkül tudott tartalmakat feltölteni, majd ezeknek a tartalmaknak a linkjét szabadon terjeszthette. Magának a tárhelynek nem volt sem tartalomjegyzéke, sem keresőfunkciója, így nem minősül nyilvánossághoz való közvetítésnek a tárhelyre való feltöltés, azonban ettől függetlenül a céget az a kötelezettség terheli, hogy amennyiben tudomására jut, hogy jogellenesen töltöttek fel tartalmakat a felületére, azonnal meg kell szüntetni az ehhez való hozzáférést – amit egyébként a Cyando több esetben sem tett meg. Az ügyben a bíróság egy több pontból álló, egymással is összefüggő elemekből álló szempontrendszerrel dolgozott ki arra vonatkozóan, hogy a platform a „következmények tudatában” cselekszik-e, és ezáltal megvalósul-e a „nyilvánossághoz közvetítés”, amely egyúttal megalapozza a platform *elsődleges* felelősségét is. Ezek a szempontok a következők: a platform működtetője tudja-e, hogy a felhasználók szerzői jogilag védett tartalmakat osztanak meg a felületen, tesz-e megfelelő technikai intézkedéseket a védett tartalmak kiszűrésére, részt vesz-e a tartalom kiválogatásában, biztosít-e eszközöket a tartalom megosztásához, tudottan ösztönzi-e a védett tartalmak illegális megosztását célzó eszközöket (mert az például

⁸ Eva Glawischnig-Piesczek v. Facebook (2019) C-18/18.

⁹ Egyesített C-682/18 (YouTube) és C-683/18 (Cyando) ügyek. Mindkét ügyről részletes elemzést ad Gosztonyi Gergely: *Cenzúra Arisztoteléstől a Facebookig. A közösségi média tartalomszabályozási gyakorlatának komplexitása*. Budapest, Gondolat Kiadó, 2022. 205–209.

az üzleti modelljének része, mint a Cyando esetében), és végül, hogy a platform fő használati módja az illegális tartalmak megosztása-e.¹⁰ Mint látható, a megfelelő technikai intézkedések megtétele igen hangsúlyos szempont – ami lényegileg ismét csak folyamatos monitorozást jelent.

Az ex ante szabályozás kockázatai

A másik, a szabályozással kapcsolatos dilemma, kritika annak kiterjedt ex ante jellegével kapcsolatban fogalmaz meg kételyeket. Az új európai platformjog ugyanis nagyrészt ex ante szabályozás, azaz olyan kötelezettségeket ró a platformokra, amelyeknek folyamatosan meg kell felelniük. (Szemben az ex post szabályokkal, amelyek azt mondják meg, hogy jogellenes helyzetek bekövetkezte esetén ki a felelős.)

Ez azt a fontos kérdést veti fel, amely a – főleg amerikai – szakirodalomban régebb óta komolyan tárgyalt, hogy az egyelőre még alig látott jövőbeli kockázatok vajon jó eszközökkel próbálja-e a jogalkotó csökkenteni. Cass Sunstein ezeket a törvényeket egyenesen „felelőtörvényeknek” nevezi, és szerint ezekkel nagyon óvatosan kell bánni, mert az „elővigyázatossági elv”, amelyből ezek a jogszabályok kiindulnak, egyfelől nem mondja meg, hogy *mennyi* elővigyázatosságra van szükség egy adott veszély elhárításához, másrészt az elv „költségvak”, Sunstein könyvében egy sor példát hoz arra, hogy amennyiben az elővigyázatossági elv a jogszabályok része lett volna, akkor milyen találmányokkal lennének szegényebbek. Ezek közt szerepel például a repülőgép és a röntgen is.¹¹

A DSA kodifikációjának folyamatában az elővigyázatossági szabályok száma és szigora is folyamatosan nőtt. Ráadásul, mivel a platformjog amúgy is „méltóságot védő” ex ante szabályokból áll túlnyomórészt, jellemzően pluszban is ilyen szabályok kerültek be utólag a szövegbe – olyan szabályok, amelyek nem a felhasználók biztonságát, pszichéjét vagy életét védik, hanem szólásszabadságát vagy döntési autonómiáját –, ami szintén fontos dolog, csak sokkal nehezebben megfogható. Sunstein fő érve könyvében az, hogy csak tudományosan bizonyított veszélyek esetén lehet alkalmazni az elővigyázatossági elvet, és hogy minden alkalmazás egyben felvet más kockázatokat, amelyek szintén elővigyázatosságot igényelhetnek. Sunstein másik fontos konklúziója ehhez kapcsolódóan az, hogy a világ tele van veszélyekkel, és ezek közül szinte véletlenszerű, hogy mit tart a közvélemény vagy egyes érdekcsoportok veszélyesnek, és mi határozza majd meg a közhangulatot, mitől fognak félni az emberek. Ha végigtekintünk az elmúlt évtizedeken, csakugyan

¹⁰ Felix Reda – Joschka Selinger: YouTube/Cyando – an Important Ruling for Platform Liability. Part 1 and Part 2. *Kluwer Copyright Blog*, 2021. július 1.

¹¹ Cass Sunstein: *Laws of Fear. Beyond the Precautionary Principle*. Cambridge, Cambridge University Press, 2005. 25.

látunk olyan veszélyeket, amelyek csaknem hisztérikus hangulatba hozták egy időre az embereket (például az AIDS, a kergemarhakór,¹² a Y2000-összeomlás,¹³ a genetikailag módosított élelmiszerek stb.), és amelyek egy részéről kis túlzással ma már azt sem tudjuk, hogy miért is féltünk tőlük. A platformokat kétségtelenül szabályozni kell, de a jelenlegi ex ante szabályozás mértéke és irányai egyáltalán nem biztos, hogy helyesek. Nekem az a határozott benyomásom, hogy a platformoktól (és nem ide tartozik, de a mesterséges intelligenciától) való félelem *eltúlzott*, az ex ante kötelezettségekből pedig feleslegesen sok van.

Sunstein érvelését látványosan alátámasztja, hogy újabb és újabb ötletek jelennek meg az ex ante megfelelési elvárások fokozására. Ezek közül az egyik az, hogy a platformok „titkos” algoritmusait auditálni kellene, vagyis ezeknek előzetes termékmegfelelőségi eljárásokon kellene átesniük, akár csak a drónoknak, vagy az autóknak, illetve a legújabb tervek szerint a magas kockázatú mesterséges intelligencia algoritmusoknak.¹⁴ Ezt a koncepciót vallja egyébként magáénak Lawrence Lessig is, aki erről egy budapesti előadásában beszélt.¹⁵

Az „adatjog” dilemmája

A dilemmák második köre, amely a platformszabályozás jelenlegi rendszerében még elég sok problémát fog okozni, az az adatok jelenlegi teljesen kaotikus szabályozása. Ennek több leágazása is van, ezek közül kettőt emelek ki: a hagyományos adatvédelemnek a platformokon betarthatatlan voltát, valamint az új adatjog, a magánjog és az adatvédelmi jog tisztázatlan viszonyát.

A hagyományos adatvédelem válsága a platformokon

Az európai adatvédelmi szabályozás néhány egyszerű megfontoláson és élethelyzeteken alapszik. Hagyományos célpontja a „nagy adatkezelő” és ezen belül is paradigmátikus az az állami szervezet vagy nagyvállalat, amely egy vagy néhány jól körülhatárolható cél érdekében (ügymint: ügyintézés, szolgáltatás nyújtása) adatokat kér

¹² Sunstein (2005): i. m. 39.

¹³ “These were followed by accusations that the likely incidence of failure had been greatly exaggerated from the beginning”. Y2K bug. *Encyclopedia Britannica*.

¹⁴ Európai Bizottság: *Javaslat. Az Európai Parlament és a Tanács Rendelete a mesterséges intelligenciára vonatkozó harmonizált szabályok (a mesterséges intelligenciára vonatkozó jogszabály) megállapításáról, és egyes uniós jogalkotási aktusok módosításáról*. COM(2021)206 végleges (2021. április 21.).

¹⁵ Lawrence Lessig előadása a budapesti Society of Internet Platforms konferencián: Presentation by Lawrence Lessig on the Impact of Internet Platforms on Democracy. *Eötvös József Kutatóközpont*, 2021. október 21.

be az adatalanyoktól. Mivel a cél mindig meghatározható, és a legtöbb esetben partikuláris, valamilyen gazdasági tevékenységhez, vagy ügýtípushoz köthető, ez körberajzolja azt az adatkört, és az adatok tárolásának észszerű időtartamát is, amely ennek a célnak az eléréséhez szükséges.¹⁶ Így például egy állásra történő jelentkezés esetén nem lehet egészségügyi adatokat elkérni a jelentkezőktől, viszont mondjuk egy életbiztosítás megkötése előtt igen. Ugyanígy, jól meghúzható az az időbeli korlát, ameddig az adatokat a cél eléréséhez tárolni szükséges. Például egy munkakörre történő kiválasztási folyamat lezárultával a sikertelen jelentkezők adatait – ha külön nem kérték el tőlük és jelölték meg a célt, amiért elkérik – meg kell semmisíteni, vagy egy kültéri kamera képét, amennyiben nem vett fel bűncselekményt, szintén.

A másik előfeltevés vagy élethelyzet, amelyen az európai adatvédelem nyugszik, az, hogy az adatok beszerzése jól látható, elkülönült tevékenység, amely egy valamilyen más főtevékenységhez mint melléktevékenység csatlakozik, és az adatok egy jól meghatározott körére terjed ki. Paradigmatikus esete, hogy az adatkezelő kitöltet egy űrlapot, vagy az ügyintéző felír bizonyos adatokat. Az adatalanyok számára nemcsak az világos, hogy milyen adatot adtak meg, hanem az is, hogy miért.

Ennek az előfeltevés-rendszernek a problémáit bizonyos szempontból már a platformok előtt is látni lehetett, mert már az internet megjelenése is okozott bizonyos zavarokat. A 29. cikk szerinti adatvédelmi munkacsoport (WP29) már 2010-ben kibocsátott egy állásfoglalást, amelyben még nem is a platformok gyakorlatával, hanem az egyszerű cookie-alapú adatgyűjtéssel kapcsolatban fejezte ki aggodalmát, és jelezte, hogy az nem felel meg az adatvédelem (rég) adatvédelmi irányelvben¹⁷ lefektetett szabályainak. (Amelyek a GDPR-ben lényegileg ugyanazok maradtak.) A dokumentum „komolyan aggódik a viselkedésalapú hirdetés magánéleti és adatvédelmi implikációi miatt”, és kijelenti, hogy „mindaddig azok a módszerek, ahogy az iparág információt adott [...], kudarcot vallottak”.¹⁸

A WP29 2010-es állásfoglalása után az European Data Protection Board (EDPB) is foglalkozott a felhasználók „célzásával”.¹⁹ Az anyag kiindulópontként azt rögzíti, hogy a célzás a közösségi médiában már rég nem azt jelenti, hogy a felhasználó által tudatosan megadott egyszerű demográfiai adatok (férfi-nő, életkor stb.)

¹⁶ Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet). L 119/1 (2016. május 4.) (GDPR), 5. cikk.

¹⁷ Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról. L 281/31 (1995. november 23.).

¹⁸ Article 29 Working Party: *Opinion 2/2010 on online behavioural advertising*. 2010. június 22. 20–21.

¹⁹ European Data Protection Board: *8/2020-as állásfoglalása a közösségi média felhasználóinak megcélzásáról*.

alapján céloznak, hanem az úgynevezett megfigyelt és származtatott adatok alapján is. Ezzel kapcsolatban az anyag semmilyen jobb megoldást nem tud mondani, mint hogy az érintett hozzájárulása lehet az egyetlen jogalap ezen módszerek esetén.

Nem csoda, hogy az adatvédelmi hatóságok válasza a fentebbi kihívásokra meglehetősen egyszerű: elkezdtek keményen és szinte folyamatosan bírságotlani a platformokat. Ugyanakkor véleményem szerint itt egy strukturális problémáról és a hagyományos adatvédelem válságáról beszélhetünk, a bírságotlás nem fenntartható megoldása a problémának. Mi a magyarázata ennek? Az okok szerteágazóak.

Először is van itt egy paradigmaprobléma, amit röviden (és jobb kifejezés híján) „adat-mindenhatóságként” lehetne leírni. Lényege, hogy mivel az online térben *minden* csak adat, és bármilyen jog által szabályozott hagyományos élethelyzetet fel lehet fogni adatkezelésként, adattranszferként, adatfeldolgozásként, adat-összekapcsolásként, adatmegsemmisülésként stb., amelynek ráadásul szinte mindig van valamilyen magánszemélyhez köthető aspektusa is, a hagyományos adatvédelmi jog elkezdte kiterjeszteni a hatályát szinte mindenre, egyfajta „minden joga” lett belőle. Nadezhda Purtova, a kifejezés kiötlője helyesen mutat rá sokat hivatkozott cikkében, hogy „[a]hogy a környezetünk rohamosan közeledik ahhoz, amit egyesek »online«-nak hívnak, ahol mindennapi létezésünket az információs technológia közvetíti, ebben a környezetben minden – időjárás, szennyvíz, vizsgakönyvek – egyre inkább »datifikálódik«, és szó szerint minden adattal kapcsolatban lehet hitelesen úgy érvelni, hogy az személyes”.²⁰

Ez az adatvédelem nincsen felkészülve arra a helyzetre sem, hogy az „adatalany” úgy dönt, hogy a magánéletének egy részét egy internetes oldalon fogja élni, a társas kapcsolatait szervezésének egy részét ezzel az oldallal fogja végeztetni. Ugyanígy (a Google esetén) arra sem, hogy internetes jelenlétünk egy sor kulcsmozzanatát (privát érdeklődésünkhöz kapcsolódó kereséseket, privát levelezésünket) egyetlen platformon végezzük. A hagyományos adatvédelem nem tudott mit kezdeni azzal a ténnyel sem, hogy ami az internetre felkerült, az lényegében onnan már soha nem törölhető egészen az elfeledtetéshez való jog „feltalálásáig”,²¹ ami pedig egy sor újabb problémát vet fel.

Ebben a helyzetben az adatvédelmi jog fundamentumai rendülnek meg: nem, vagy csak korlátoosan használható az informált hozzájárulás elve, lényegében nem értelmezhető az adattakarékosság elve, és ami a legnagyobb gond, nagyon nehezen értelmezhető a célhoz kötöttség elve.

²⁰ Nadezhda Purtova: The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, 10. (2018), 1. 41.

²¹ Viktor Mayer-Schönberger: *Delete. The Virtue of Forgetting in the Digital Age*. Princeton, NJ, Princeton University Press, 2011.

Utóbbira nézzük például a Facebookot. Jelenlegi szabályai szerint a Facebook azzal a céllal gyűjti az adatokat, „hogymilyen személyre szabott élményt nyújtunk a számunkra [...]”. A rendelkezésre álló adatokat felhasználjuk termékeink biztosítására és továbbfejlesztésére. Idetartozik a funkciók, tartalmak és ajánlások – például [...] a történetek és a hirdetések – személyre szabása.”²² Vajon milyen módon tud ez a célmeghatározás bármilyen adatgyűjtést és felhasználást behatárolni, egyáltalán létezik-e olyan adatgyűjtés, amely ebbe a célmegjelölésbe „nem fér bele”? Nézzünk négy esetet: a Facebook gyűjti, hogy milyen típusú posztokat lájkoltam, hogy milyen posztot kattintottam át, hogy milyen poszt felett lassítottam le a görgetéssel, hogy mely posztra kezdtem el reagálni, de töröltem ki végül a bejegyzést. Négy eset, amelyek egyre mélyebbre hatolnak a felhasználói viselkedés megismerésében, mégis, az adatvédelmi szabályzat célmeghatározása alapján egyikről sem lehet eldönteni, hogy „belefér” vagy „már nem fér bele”, hiszen ezen általános célmegjelölés (és funkció) alapján egyszerűen minden belefér. De ugyanígy elgondolkodhatunk arról is, hogy ez a célmeghatározás vajon hogyan korlátozza időben az adatok tárolását? Mi az az időtartam, ameddig az adat ennek a célnak a függvényében tárolható?

Az adattakarékosság elvével még nagyobb a probléma: hogyan értelmezhető, ha egyáltalán van bármilyen értelme az adattakarékosság alapelveinek a közösségi média-platformokon, és a Google-hoz köthető platform-ökoszisztémában? Hogyan lehet több tízezer, de akár csak több ezer adatpont gyűjtéséhez „informált hozzájárulást” adni? Kicsit más kontextusban, de lényegében ugyanerre a következtetésre jut a magyar irodalomból Pataki Gábor és Szőke Gergely László is.²³ Pataki és Szőke elnagyoltnak és homályosnak nevezi a Google adatkezelési tájékoztatóját, amit főképp az okoz, hogy „nem átlátható módon rögzít hat, majd tizenegyet adatkezelési célt ugyanabban a tájékoztatásban, illetve mindezekhez négy jogalapot is csatol”.²⁴ Ezenfelül (egyebek mellett) nem beszél a külföldre továbbításról, nem említi minden érintetti jogosítványt, és egyáltalán nem beszél a profilozásról.²⁵

A Google esetén Bart van der Sloot és Frederick Zuiderveen Borgesius²⁶ tanulmánya is megerősíti ezt az érvet. Sőt, a Google más szempontból, nemcsak a felhasználókról gyűjtött adat szempontjából, hanem a keresőbe beírt személy és a róla

²² Meta adatvédelmi szabályzat. *Meta*, 2022. július 26.

²³ Pataki Gábor – Szőke Gergely László: A Google és a Facebook adatvédelmi tájékoztatási gyakorlatok a GDPR szabályozásának tükrében. In Polyák Gábor (szerk.): *Algoritmusok, keresők, közösségi oldalak és a jog – A forgalomirányító szolgáltatások szabályozása*. Budapest, HVG-ORAC, 2020. 89–104.

²⁴ Pataki–Szőke (2020): i. m. 94.

²⁵ Pataki–Szőke (2020): i. m. 95.

²⁶ Bart van der Sloot – Frederick Zuiderveen Borgesius: Google and Personal Data Protection. In Aurelio Lopez Tarruella (szerk.): *Google and the Law. Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models*. The Hague, TMC Asser Press – Springer, 2012. 75–112.

összegyűjtött információ szempontjából is problémát jelent. Éppen erre mutat rá a González-ügy²⁷ is, amely azzal a dilemmával szembesítette az Európai Unió Bíróságát, hogy a keresőmotorok, bár a hagyományos értelemben nem végeznek személyesadat-gyűjtést, csak „egybeszerkesztik” és egy felületen prezentálják az interneten található tartalmakat, mégis képesek új minőséget létrehozni egy személyről azzal, hogy róla „rendszerezett összefoglalót” tudnak adni. Az EUB a González-ügyben adatkezelőnek minősítette a Google-t, de a probléma véleményem szerint ezzel nem lett megoldva, mert a Google-t lehetetlen mindazokkal az adatkezelői kötelezettségekkel megterhelni, amellyel egy normál adatkezelőt. Az könnyen beláthatóan képtelenség, hogy a Google több milliárd ember személyes adatát az adatvédelmi szabályok szerint kezelje. A jogalkotó nem is ment el idáig: amit megkövetel, az csak az elfeledtetéshez való jog gyakorlásának lehetővé tétele.²⁸

Az új adatjog viszonya a hagyományos magánjoghoz

Az adatfelhasználás új módjai tehát a hagyományos adatvédelmet válságba sodorták. Ezek az új módszerek a magánjogban is egyre több zavart okoznak, ugyanis jelenleg az adatok megítélésével kapcsolatban egy nehezen kezelhető „duplafenekű” szabályozás látszik kibontakozni. Míg a személyes adatok vonatkozásában a hagyományos, „méltóságalapú”, alapjogias szemléletmód uralkodik, addig a személyes adatnak nem minősülő adatok terén az ágazati „ad hoc” jellegű szabályozások jellemzőek, amelyeknek – legalábbis a legutóbbi időkgig – nem volt közös „adatszemlélete”: az általuk szabályozott jelenségeket olykor nem is adatként definiálták, nem így tekintettek rá. A szerzői jog „műről” beszél, a médiajog „médiatartalomról”, a közadatok nyilvánosságáról szóló első irányelv „dokumentumokról”, vagy épp más területek „üzleti titokról” (vagy általában véve titokról), adatbázisról,²⁹ esetleg „know-how”-ról, és sok minden másról, éppen az adott jogág életviszonyainak és a korábbi, még nem mindent adatként látó és láttató szabályozásnak megfelelően.

Ugyanakkor ezek fölé a diverz koncepciók fölé kezd ernyőként ráterülni az „erőforrás-alapú adat” szabályozási megközelítés, amely az adatra mint a gazdaság és az innováció egyik legfontosabb hajtóerejére és alapjára tekint, amelynek a köz- és magánszféra, az üzleti vállalkozások és a magánszemélyek, kis és nagy adatgenerálók és adatfelhasználók közt *alapvetően szabadon kell áramolnia*. Az ennek

²⁷ González-ügy. EUB, (2014) C-131/12.

²⁸ GDPR 17. cikk.

²⁹ Az Európai Parlament és a Tanács 96/9/EK irányelve (1996. március 11.) az adatbázisok jogi védelméről. L 77/20 (1996. március 27.).

a koncepciónak a jegyében született joganyag végső igazolása a korlátok felszabaddítása ennek az áramlásnak az útjából, és a leglátványosabb új termékei az adatmegosztási jogszabály (Adatkódex, Data Act)³⁰ és az adatkormányzási rendelet.³¹ És bár mindkét tervezet hangsúlyozza, hogy kizárólag a nem személyes adatokra vonatkozik (az eleve így keletkezett, vagy a személyes jellegtől megfosztott adatokra), ez az érvelés több ponton is elég ingatag. Egyfelől a 2010-es évek elején még oly népszerű big data diskurzus mutatta ki, hogy a nyílt interneten található adatok miatt elég egyszerű bármilyen adathalmazt visszanevesíteni.³² Másrészt ezzel összefüggésben, a személyes adatok definíciója miatt szinte minden ennek minősül, ahogy ezt Purtova már idézett írásában kimutatta.³³ Harmadrészt, a személyes jellegtől megfosztott adatok értéke jóval kisebb, mint az ilyen jelleggel rendelkezőké,³⁴ és az adatipar egy sor szolgáltatása nem is értelmezhető személyes adatok nélkül. Végül negyedrészt, a viselkedési adatok fékevesztett gyűjtése és a mikroprofilozás (egyre pontosabb, egyre kisebb csoportokat képező felhasználói profilok) miatt az egyértelmű azonosíthatóság, az „érintettel helyreállítható kapcsolat” jelentősége eltűnik. Egy olyan világban, ahol én vagyok egyedül egy mikroprofilba illeszthető természetes személy, teljesen mindegy, hogy a nevemet az adott profilt használó cég tudja-e, vagy sem, mert enélkül is teljesen személyre szabott manipulációra képes adott esetben.

Itt tehát két kérdés van függőben, az egyik, hogy vajon valóban megvalósul-e az adattulajdonlás jogi konstrukciója, a másik, hogy lesz-e egységes „adatjog”, vagy fennmarad a kettős, vagy még inkább hármas rendszer, amelyben minden pillér teljesen más filozófia és igazolás mentén kezeli az adatokat. Nem kizárt az sem, hogy valamiféle hibrid jön létre, amelyben az adatjog elnyel, felszámol egyes területeket (például a közadatok újrahasznosításával vagy a közérdekű adatok nyilvánosságával, esetleg az adatbázis-szabályozással kapcsolatosakat), de másokat nem.

³⁰ Európai Bizottság: Javaslat. Az Európai Parlament és a Tanács rendelete, a méltányos adathozzáférésre és adatfelhasználásra vonatkozó harmonizált szabályokról (adatmegosztási jogszabály). COM(2022)68 végleges (2022. február 23.).

³¹ Európai Bizottság: Javaslat. Az Európai Parlament és a Tanács rendelete az európai adatkormányzásról (Adatkormányzási rendelet). COM(2020)767 végleges (2020. november 25.).

³² Például Paul Ohm: Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*, 57. (2010), 6. 1701–1777.

³³ Purtova (2018): i. m. 41.

³⁴ Mark James Elliot et al.: *The Anonymisation Decision-Making Framework*. Manchester, UKAN, 2016. A szerzők egyfajta alkuként ábrázolják a személyes adatoktól megfosztott adatokat, és bár arra a következtetésre jutnak, hogy létezik értelmes és használható alkupont, azt nem vitatják, hogy általában és főszabály szerint a személyes adatok értékesebbek, mint az anonimizáltak.

Az állam és a platformok viszonya

A harmadik megoldatlan dilemmacsoport a platformokkal kapcsolatban az, hogy hogyan viszonyuljon az állam a platformokhoz. Itt, hasonlóan az előző két problémacsoportéhoz, a sok probléma és dilemma közül csak kettőre térek ki: arra, hogy a platform valóban vetélytársa, kihívója-e az államnak, és arra, hogy az államoknak mennyire kell a platformot mint koordinációs mechanizmust használniuk.

A platform mint az állam vetélytársa

A platformok és a kormányzatok kapcsolata igen összetett, és először ennek egy apró, de fontos szeletére szeretnék itt rámutatni, arra a közkeletű félreértésre, amely arról szól, hogy a platformok a nemzetállamok „versenytársai” lennének. Ennek a nézetnek népes táborra van, így például Gilles Babinet,³⁵ Julie Cohen,³⁶ Vili Lehdonvirta,³⁷ Mireille Hildebrandt³⁸ vagy William H. Davidow és Michael S. Malone.³⁹

Én magam nem osztom ezt az (olykor apokaliptikus körítéssel tált) nézetet, és csak meg tudom ismételni az ellentábor érveit. Érdemes abból kiindulni, hogy az internetről is igen hamar kiderült, hogy az álmodozók jóslatai ellenére nem hierarchia és hatalom nélküli bázisdemokratikus közösség, valamiféle „szervezet nélküli szerveződés”, mert az offline hatalmaknak igenis van rá komoly befolyásuk. Legutoljára például Sebastian Berg⁴⁰ szedte ízekre John Perry Barlow ismert internetfilozófus 1996-os kiáltványát, amelyben Barlow a háló szabadságát követelve egy hatalom és előítéletek nélküli világot vizionált az online térben.⁴¹ Az igazság – mondja Berg – az, hogy a jelenleg létező politikai intézmények, mint az állam, a pártok és a nagy cégek továbbra is nagy hatalommal bírnak, és nem úgy tűnik, hogy hatalmukat a platformok érdemben kikezdték volna. A platformok

³⁵ Gilles Babinet: The End of Nation States? Part 1: Technology-Induced Sovereignty Transfers. *Institut Montaigne Blog*, 2018. november 27.; Gilles Babinet: The End of Nation States? Part 2: Meta-Platforms for the Common Good. *Institut Montaigne Blog*, 2019. január 21.

³⁶ Cohen (2018): i. m.

³⁷ Vili Lehdonvirta: *Cloud Empires. How Digital Platforms are Overtaking the State and How We Can Regain Control*. Cambridge, MA, MIT Press, 2022.

³⁸ Mireille Hildebrandt: The Virtuality of Territorial Borders. *Utrecht Law Review*, 13. (2017), 2. 13–27.

³⁹ William H. Davidow – Michael S. Malone: *The Autonomous Revolution. Reclaiming Future We've Sold to Machines*. Oakland, CA, Berrett-Koehler Publishers, 2020.

⁴⁰ Sebastian Berg: Myth #31: The Internet Enables Organizing Without Organization. In Matthias C. Kettmann – Stephan Dreyer (szerk.): *Busted! The Truth about the 50 Most Common Internet Myths*. Hamburg, Verlag Hans-Bredow-Institut, 2019. 142–145.

⁴¹ John Perry Barlow: A Declaration of the Independence of Cyberspace. *Electronic Frontier Foundation*.

egyszerűen nem „erősebbek”, mint egy nemzetállam: ezt nem bizonyítja sem az, hogy a Facebook többet tud rólunk, mint a saját államunk – hiszen hiába tud többet, azért rendőrt nem tud küldeni a házhoz, hogy házkutatást tartson –, sem pedig az, hogy a platformok vezetőit alkalmasint olyan nagy csinnadrattával fogadják, mint az államfőket. A hiba ott van az érvelésben, hogy a platformok nem a nagyvállalat és nem is a nemzetállam mint entitás, pláne nem valamilyen konkrét nagyvállalat és konkrét nemzetállam versenytársai. Ez annál is furcsább lenne, mivel a Facebook Inc. vagy az Alphabet maguk is nagyvállalatok, tőzsdei jelenléttel. Véleményem szerint ezeket a szerzőket az téveszti meg, hogy *a platform az igazgatás, irányítás, a társadalmi kontroll új, hatékony formája*, amely a platformhatalmon keresztül manifesztálódik, és amely a *bürokrácia* kihívójává vált. Még rövidebben megfogalmazva, a platform sem a nagyvállalat *jogi és szervezeti* formáját, sem a nemzetállam jogi és szervezeti formáját és autoritását *nem* veszélyezteti. A platform a bürokratikus igazgatást és a piacot *mint kontrollmechanizmusokat* veszélyeztetni azzal, hogy az egyre több területre kiterjedő online tér sajátos, általános kontrollmechanizmusává vált.

A platform tehát nem versenytársa az államnak, azonban nagyon is versenytársa a bürokráciának és a hagyományos piaci mechanizmusoknak. Működése emiatt érinti az állami működést, több szempontból is. Először is úgy, hogy az államoknak kezdeni kell valamit azzal, hogy a platform hajlamos „inváziós falként” viselkedni, és például a piaci mechanizmusokat emulálva (valójában azokat kiszorítva, megölve) egy torz és végső soron a többség jólétét csökkentő működésbe fordulni. Ezenfelül és ezzel összefüggésben magára hagyottan fokozottan diszfunkcionális működésre hajlik.

Az államok platformizálása – platformállamok, felhőbirodalmak

Másrészt azonban, mivel a platform a bürokrácia versenytársa, sőt sok szempontból hatékonyabb „2.0-s verziója”, az államok rá lesznek kényszerítve arra, hogy szervezési és igazgatási feladataikhoz igénybe vegyék a platformmechanizmusokat, ahogy a gazdaság szereplői is rákényszerülnek arra, hogy vagy saját platformokat hozzanak létre, vagy egy erős, nagy platformhoz csatlakozzanak.

Az államok alapvetően kétféleképpen használhatják a platformokat. Az egyik módszer, hogy ehhez létező platformokat vesznek igénybe,⁴² sőt, esetleg államosítják

⁴² A magyar kormányzatnak, úgy tűnik, a leglényegesebb kommunikációs csatornája például a Facebook lett. A magyar kormányfő a pandémia alatt nemegyszer itt tette meg a legfontosabb bejelentéseit.

azokat. Ez, bár igencsak szélsőséges véleménynek tűnik, mégis létező felvetés.⁴³ Ugyanakkor, ha el is tekintünk attól az egyáltalán nem lényegtelen kérdéstől, hogy melyik nemzetállam államosítsa, még mindig marad egy sor kérdés, ami miatt ezt nem tartom járható útnak. Semmilyen állam nem lenne jó gazdája egy alapvetően nem állami funkciókra kifejlesztett platformnak, arról nem beszélve, hogy így egy mindenbe belelátó állam milyen alapjogi kérdéseket vetne fel. Ugyanakkor azt is látni kell, hogy Kínában, tekintve a kínai állam befolyását például a WeChatre, éppen ez a helyzet.⁴⁴

A versenyképes szolgáltató állam platformizációját úgy kell kialakítani inkább, hogy az államok maguk alakítanak ki az adminisztratív feladataik ellátásához platformokat. Sőt, egyesek szerint *magának az államnak kellene egy szolgáltató platformmá válnia*.⁴⁵ Hiszen azoknak a funkcióknak a többsége, amelyeket az állam végez, felfogható szolgáltatásként is (információnyújtás, dokumentumok szolgáltatása stb.), amely könnyedén kivihető az online térbe. Ettől a platformizációt (a szolgáltatások egy helyre gyűjtését, az állampolgárok számára felhasználói profilok létrehozását, bizonyos szolgáltatásoknak a viselkedésből történő ajánlását, a szolgáltatások nyújtásának automatizálását, vagy egyenesen mesterségesintelligencia-alapúvá tételét) már csak egy lépés választja el, amelyet ezután végezhetnek külső cégek is. A magyar ügyfélkapu és a rajta elérhető szolgáltatások is egyfajta platformkezdeményt jelentenek.

Nem véletlen, hogy megjelent a GaP (Government-as-Platform) kifejezés is,⁴⁶ bár ez a koncepció kicsit más jelent, mint azt, hogy az állami szolgáltatásokat egy platformon lehessen igénybe venni. O'Reilly, aki már 2011-ben elkezdte propagálni a GaP eszméjét, cikkében a „bazar”-modell mellett érvel.⁴⁷ O'Reilly szerint a kormányzatoknak is „bázarrá” kell változniuk, akik platformként fogják össze a különböző szolgáltatásokat. Példái, a GPS-navigáció vagy az időjárési appok lényege

⁴³ Gianmarco Raddi: Nationalize Facebook. Mark Zuckerberg Can't Protect Our Data. *Politico*, 2018. október 9.; Nick Srniczek: We Need to Nationalise Google, Facebook and Amazon. Here's Why. *The Guardian*, 2017. augusztus 30.

⁴⁴ Gosztonyi „kínai modellnek” nevezi ezt. Gosztonyi (2022): i. m. 157–171.

⁴⁵ Például Vagelis Papakonstantinou: States as Platforms under New EU (Online Platforms') Law. *European Law Blog*, 2022. július 4.

⁴⁶ Tim O'Reilly: Government as a Platform. *Innovations: Technology, Governance, Globalization*, 6. (2011), 1. 13–40.

⁴⁷ A katedrális-bazar hasonlat Eric S. Raymondtól származik, aki azonos című könyvében a régi típusú szoftverfejlesztést, amely egy előre eltervezett szigorú terv szerint épít egy hatalmas épületet, katedrális, egy bazárhoz hasonlítja, ahol sokak erőfeszítéséből alakul ki egy színes kínálat. Eric S. Raymond: *The Cathedral and the Bazaar. Musing on Linux and Open Source by an Accidental Revolutionary*. Beijing, O'Reilly, 1999.

az, hogy az állam bizonyos alapokat, szoftveres megoldásokat, adatokat szolgáltat, és erre a magánvállalkozások építhetnek rá újabb szolgáltatásokat. Itt tehát az állam a platformot mint piacteret biztosítja, amelyre a bázár árusai fejlesztik a saját szolgáltatásaikat.

Az állami szerepvállalás egy másik aspektusa, hogy véleményem szerint jogi és nem jogi eszközökkel minél több európai platform létrejöttét kellene ösztönözni.⁴⁸ Ez nem azt jelenti, hogy létre kell hozni egy Facebook-alternatívát (bár önmagában ezt sem tartanám teljesen butaságnak), hanem azt, hogy az adminisztratív és a bürokratikus akadályok leépítésével kellene a startupokat és más innovatív vállalkozásokat arra ösztönözni, hogy próbálkozzanak új platformok építésével. A platformok világában az USA és Kína túlsúlya annyira nyomasztó, hogy az már bizonyos szempontból csakugyan felvet szuverenitási kérdéseket. Ugyanakkor azt is látni kell, hogy a platformnak, akárcsak minden hálózatos szolgáltatásnak, a kritikus tömeg elérése és fenntartása a lételeme: nem rosszabbul működik, hanem lényegében nem tud működni, ha nincsen kellő mennyiségű felhasználója. És itt a nyelvileg fragmentált európai piac óriási hátránnyal indul. De épp a nagy amerikai platformok sikere bizonyítja, hogy nyelvileg lokalizált változatokkal ez a probléma leküzdhető.

Nemcsak a nemzetállami közigazgatásoknak és közszolgáltatásoknak, hanem magának az EU-nak a platformizációja is elképzelhető, sőt az EU-é sok szempontból könnyebben kivihető is lenne, mint a nemzetállamoké. Azokon a területeken, ahol az EU-jog domináns (adatvédelem, versenyjog stb.), az EU létrehozhatna egy olyan jogi-igazgatási platformot (a jelenlegi szigetszerű alkalmazások helyett), amely a tagállamok koordinációját valósítaná meg. Másrészt a tagállamok a már jelenleg is létező e-kormányzati megoldásaikat integrálhatnák platformokká, és ebben lehetne egy közös fejlesztőbázis és szoftverkomponens-pool felállításával segíteni őket. Európában a Joinup platform a kormányzatoknak már ajánl ingyenes digitális kormányzati szolgáltatásokat,⁴⁹ amelyek középpontjában a geolokációs információk megosztása áll.⁵⁰ A platform mint az online tér koordinációs mechanizmusa sokkal hatékonyabb, mint a papíralapú, ügyközpontú bürokrácia: ezt a hatékonyságot érdemes kihasználni. Általános alkalmazhatósága, amely lehetővé teszi használatát

⁴⁸ Az Európai Unió rengeteget foglalkozik a platformok problematikájával, de soha nem ebben a kontextusban. Az EU inkább az adatgazdaság, és ezen belül az ipari platformok és az adathordozhatóság összefüggésében, például European Commission: Commission Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy. Accompanying the Document Communication Building a European Data Economy. COM(2017)9 végleges (2017. január 10.); és fogyasztóvédelmi szemszögből (például Emma Psaila et al.: *Exploratory Study of Consumer Issues in Online Peer-to-peer Platform Markets*. European Commission, Directorate-General for Justice and Consumers, 2017) tekint a platformokra, illetve újabban mint a demokráciát fenyegető veszélyre, amely a „veszélyes tartalmak” és a szólásszabadság kontextusába helyezi a témát.

⁴⁹ Lásd az EU Bizottsága Joinup platformjának honlapját: European Commission – Joinup.

⁵⁰ European Union Location Framework (EULF) Blueprint.

az államon belüli adatcserére, az állampolgárok ügyeinek az intézésére, az állami erőforrások elosztására (például támogatások, segélyek), az állami vagyonnal való gazdálkodásra, és sok minden másra is, óriási pontenciált rejt. Elképzelhetőnek tartom, hogy az államok fennmaradásának egyik kérdése épp az lesz, hogy „igába tudják-e fogni” a platformok erejét, vagy sem.

Konklúziók

Három dilemmacsoportot érintettem, amelyeket véleményem szerint az új platformjog hatálybalépése sem fog megoldani. Az első dilemma a szabályozás módszerére vonatkozott, és két részproblémát tartalmazott. Az első az ex ante jellegű szabályozás hátulütőit hangsúlyozza. Az ex ante jellegű szabályozással kapcsolatban, amely az új európai platformjog fő módszere, a szakirodalom sok kritikát fogalmaz meg. Ezek közül az a legfontosabb, hogy a kockázatok kikerülésére koncentráló szabályozás a már ismert kockázatokat próbálja kezelni, de nem tud semmit a jövőben felmerülő kockázatokról, és arról sem, hogy a kockázatelkerülésnek milyen mellékhatásai lehetnek, milyen további kockázatokat szül, és milyen költségeket generál. A másik szabályozási kérdés, hogy vajon van-e értelme fenntartani az általános monitorozási kötelezettség hiányát mint főszabályt a platformok esetében, amikor az már egy sor kivétellel és szűkítéssel rendelkezik, és maguk a platformok is folyamatosan monitorozzák a felületükön áramló tartalmakat.

A második dilemmacsoport az adatokhoz történő hagyományos jogi hozzáállással kapcsolatos. Ez is kétféle problémahalmazt takar. Az első az adatvédelmi jog ellehetetlenülése a platformokon, és különösen ennek hozzájárulás-centrikussága, valamint az adattakarékosság és a célhoz kötöttség mint elvek tarthatatlansága. A második dilemma lényege, hogy (részben éppen emiatt) egy új adatjog van kialakulóban, amelyben az adat mint erőforrás nyer szabályozást, és amely a hagyományos magánjoggal és a hagyományos adatvédelmi joggal is nehezen összeegyeztethető, és a jövőben még sok feszültséget fog okozni. Azt, hogy ez a dilemma hogyan fog feloldódni, egyelőre nem lehet tudni, ez a hagyományos adatvédelmi és magánjog visszakozásával, az új adatszemplélet győzelmével is zárulhat, az is elképzelhető, hogy a platformok fűjnek visszavonulót, de az is lehet, hogy valamilyen kompromisszumos megoldás győzedelmeskedik majd.

Végül a harmadik dilemmacsoport az államok és a platformok viszonyával foglalkozott. Itt az első kérdés az volt, hogy az államok hatalmát, szuverenitását mennyire veszélyeztetik a platformok. Erre a válasz az, hogy korántsem annyira, mint azt egyes szerzők vélik. A másik kérdés pedig az volt, hogy az államoknak érdemes-e platformmegoldásokban gondolkodni, platformizálódni. Erre az írás azt a választ adta, hogy az államoknak nemcsak hogy hasznos, hanem előbb-utóbb szükséges is lesz bizonyos területeken platformmegoldásokat alkalmazni.

Felhasznált irodalom

- Article 29 Working Party: *Opinion 2/2010 on online behavioural advertising*. 2010. június 22. Online: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf
- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet). L 119/1 (2016. május 4.)
- Az Európai Parlament és a Tanács (EU) 2019/1150 rendelete (2019. június 20.) az online közvetítő szolgáltatások üzleti felhasználói tekintetében alkalmazandó tisztességes és átlátható feltételek előmozdításáról. L 186/57 (2019. július 11.) (P2B rendelet)
- Az Európai Parlament és a Tanács (EU) 2018/1808 irányelve (2018. november 14.) a tagállamok audiovizuális médiaszolgáltatások nyújtására vonatkozó egyes törvényi, rendeleti vagy közigazgatási rendelkezéseinek összehangolásáról szóló 2010/13/EU irányelvnek (Audiovizuális médiaszolgáltatásokról szóló irányelv) a változó piaci körülményekre tekintettel való módosításáról. L 303/69 (2018. november 28.) (AVMS irányelv)
- Az Európai Parlament és a Tanács (EU) 2019/790 irányelve (2019. április 17.) a digitális egységes piacon a szerzői és szomszédos jogokról, valamint a 96/9/EK és a 2001/29/EK irányelv módosításáról. L 130/92 (2019. május 17.)
- Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (2022. október 19.) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (digitális szolgáltatásokról szóló rendelet). L 277/1 (2022. október 27.)
- Az Európai Parlament és a Tanács (EU) 2022/1925 rendelete (2022. szeptember 14.) a digitális ágazat vonatkozásában a versengő és tisztességes piacokról, valamint az (EU) 2019/1937 és az (EU) 2020/1828 irányelv módosításáról (digitális piacokról szóló jogszabály). L 265/1 (2022. október 12.)
- Az Európai Parlament és a Tanács 2000/31/EK irányelve (2000. június 8.) a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem, egyes jogi vonatkozásairól (Elektronikus kereskedelemről szóló irányelv). L 178/1 (2000. július 17.)
- Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról. L 281/31 (1995. november 23.)
- Az Európai Parlament és a Tanács 96/9/EK irányelve (1996. március 11.) az adatbázisok jogi védelméről. L 77/20 (1996. március 27.)
- Babinet, Gilles: The End of Nation States? Part 1: Technology-Induced Sovereignty Transfers. *Institut Montaigne Blog*, 2018. november 27. Online: www.institutmontaigne.org/en/blog/end-nation-states-part-1-technology-induced-sovereignty-transfers
- Babinet, Gilles: The End of Nation States? Part 2: Meta-Platforms for the Common Good. *Institut Montaigne Blog*, 2019. január 21. Online: www.institutmontaigne.org/en/analysis/end-nation-states-part-2-meta-platforms-common-good
- Balkin, Jack M.: The Fiduciary Model of Privacy. *Harvard Law Review Forum*, 134. (2020), 1. 11–33.
- Barlow, John Perry: A Declaration of the Independence of Cyberspace. *Electronic Frontier Foundation*. Online: www.eff.org/cyberspace-independence

- Berg, Sebastian: Myth #31: The Internet Enables Organizing Without Organization. In Matthias C. Kettmann – Stephan Dreyer (szerk.): *Busted! The Truth about the 50 Most Common Internet Myths*. Hamburg, Verlag Hans-Bredow-Institut, 142–145.
- Bickert, Monika – Brian Fishman: Hard Questions: How We Counter Terrorism. *Facebook News*, 2017. június 15. Online: <https://about.fb.com/news/2017/06/how-we-counter-terrorism/>
- Bonasera, Giulio: Should Consumers Be Able to Sell Their Own Personal Data? *The Wall Street Journal*, 2019. október 13. Online: www.wsj.com/articles/should-consumers-be-able-to-sell-their-own-personal-data-11570971600
- C-682/18 (YouTube) és C-683/18 (Cyando) egyesített ügyek (2021). (EuB)
- Cohen, Julie: *Between Truth and Power. The Legal Constructions of Informational Capitalism*. Oxford, Oxford University Press, 2018.
- Davidow, William H. – Michael S. Malone: *The Autonomous Revolution. Reclaiming Future We've Sold to Machines*. Oakland, CA, Berrett-Koehler Publishers, 2020.
- Elliot, Mark James – Elaine Mackey – Kieron O'Hara – Caroline Tudor: *The Anonymisation Decision-Making Framework*. Manchester, UKAN, 2016.
- European Commission – Joinup. Online: <https://joinup.ec.europa.eu/>
- Európai Bizottság: *Javaslat. Az Európai Parlament és a Tanács rendelete a mesterséges intelligenciára vonatkozó harmonizált szabályok (a mesterséges intelligenciára vonatkozó jogszabály) megállapításáról, és egyes uniós jogalkotási aktusok módosításáról*. COM(2021)206 végleges (2021. április 21.). Online: <https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52021PC0206>
- Európai Bizottság: *Javaslat. Az Európai Parlament és a Tanács rendelete a méltányos adathozzáférése és adatfelhasználásra vonatkozó harmonizált szabályokról (adatmegosztási jogszabály)*. COM(2022)68 végleges (2022. február 23.). Online: <https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52022PC0068&from=EN>
- Európai Bizottság: *Javaslat. Az Európai Parlament és a Tanács rendelete az európai adatkormányzásról (Adatkormányzási rendelet)*. COM(2020)767 végleges (2020. november 25.). Online: <https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52020PC0767&from=EN>
- European Commission: *Commission Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy. Accompanying the Document Communication Building a European Data Economy*. COM(2017)9 végleges (2017. január 10.). Online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017SC0002>
- European Data Protection Board: *8/2020-as állásfoglalása a közösségi média felhasználóinak megcélzásáról*. Online: https://edpb.europa.eu/system/files/2021-11/edpb_guidelines_082020_on_the_targeting_of_social_media_users_hu_0.pdf
- Eva Glawischign-Piesczek v. Facebook ügy (2019) C-18/18 (EuB)
- González-ügy. EuB, Google Spain SL és Google Inc. v. Agencia Española de Protección de Datos (AEPD) és Mario Costeja González (2014) C-131/12
- Gosztonyi Gergely: *Cenzúra Arisztoteléstől a Facebookig. A közösségi média tartalomszabályozási gyakorlatának komplexitása*. Budapest, Gondolat Kiadó, 2022.
- Gunia, Amy: Facebook Tightens Live-Stream Rules in Response to the Christchurch Massacre. *Time*, 2019. május 15. Online: <https://time.com/5589478/facebook-livestream-rules-new-zealand-christchurch-attack/>
- Hildebrandt, Mireille: The Virtuality of Territorial Borders. *Utrecht Law Review*, 13. (2017), 2. 13–27.

- Lechardoy, Lucie – Alena Sokolyanskaya – Francisco Lupiáñez Villanueva: *Study on “Support to the Observatory for the Online Platform Economy”. Monitoring of the implementation of the Platform to Business Regulation*. (h. n.), Observatory of the Online Platform Economy, 2021. Online: <https://platformobservatory.eu/app/uploads/2021/01/P2B-Regulation-monitoring-analysis-January-2021.pdf>
- Lehdonvirta, Vili: *Cloud Empires. How Digital Platforms are Overtaking the State and How We Can Regain Control*. Cambridge, MA, MIT Press, 2022.
- Lessig, Lawrence: *Code 2.0*. New York, Basic Books, 2006.
- Macdonald, Stuart – Sara Giro Correia – Amy-Louise Watkin: Regulating Terrorist Content on Social Media: Automation and the Rule of Law. *International Journal of Law in Context*, 15. (2019), 2. 183–197.
- Mayer-Schönberger, Viktor: *Delete. The Virtue of Forgetting in the Digital Age*. Princeton, NJ, Princeton University Press, 2011.
- Meta adatvédelmi szabályzat. *Meta*, 2022. július 26. Online: www.facebook.com/privacy/policy/?entry_point=data_policy_redirect&entry=0
- O’Reilly, Tim: Government as a Platform. *Innovations: Technology, Governance, Globalization*, 6. (2011), 1. 13–40.
- Ohm, Paul: Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*, 57. (2010), 6. 1701–1777.
- Papakonstantinou, Vagelis: States as Platforms under New EU (Online Platforms’) Law. *European Law Blog*, 2022. július 4. Online: <https://europeanlawblog.eu/2022/07/04/states-as-platforms-under-new-eu-online-platforms-law/>
- Pataki Gábor – Szőke Gergely László: A Google és a Facebook adatvédelmi tájékoztatási gyakorlata a GDPR szabályozásának tükrében. In Polyák Gábor (szerk.): *Algoritmusok, keresők, közösségi oldalak és a jog – A forgalomirányító szolgáltatások szabályozása*. Budapest, HVG-ORAC, 2020. 89–104.
- Posner, Richard A.: Our Domestic Intelligence Crisis. *The Washington Post*, 2005. december 21. Online: www.washingtonpost.com/archive/opinions/2005/12/21/our-domestic-intelligence-crisis/a2b4234d-ba78-4ba1-a350-90e7fbb4e5bb/
- Presentation by Lawrence Lessig on the Impact of Internet Platforms on Democracy. *Eötvös József Kutatóközpont*, 2021. október 21. Online: <https://en.ejkk.uni-nke.hu/hirek/2021/11/09/presentation-by-lawrence-lessig-on-the-impact-of-internet-platforms-on-democracy>
- Psaila, Emma – Sara Fiorentini – Marta Santos Silva – Ana Gomez: *Exploratory Study of Consumer Issues in Online Peer-to-peer Platform Markets*. European Commission, Directorate-General for Justice and Consumers, 2017. Online: https://ec.europa.eu/newsroom/document.cfm?doc_id=45244
- Purtova, Nadezhda: The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law. *Law, Innovation and Technology*, 10. (2018), 1. 40–81. Online: <https://doi.org/10.1080/17579961.2018.1452176>
- Raddi, Gianmarco: Nationalize Facebook. Mark Zuckerberg Can’t Protect Our Data. *Politico*, 2018. október 9. Online: www.politico.eu/article/nationalize-facebook-data-privacy-hackers-advertisement-social-media/
- Raymond, Eric S.: *The Cathedral and the Bazaar. Musing on Linux and Open Source by an Accidental Revolutionary*. Beijing, O’Reilly, 1999.

- Reda, Felix – Joschka Selinger: YouTube/Cyando – an Important Ruling for Platform Liability Part 1 and Part 2. *Kluwer Copyright Blog*, 2021. július 1. Online: <http://copyrightblog.kluweriplaw.com/2021/07/01/youtube-cyando-an-important-ruling-for-platform-liability-part-1/>; <http://copyrightblog.kluweriplaw.com/2021/07/01/youtube-cyando-an-important-ruling-for-platform-liability-part-2/>
- Ressa, Maria – Dmitry Muratov: A 10-point Plan to Address Our Information Crisis. *People vs. Big Tech*, 2022. szeptember 2. Online: <https://peoplevsbig.tech/10-point-plan>
- Shapiro, Robert J.: What Your Data Is Really Worth to Facebook, And Why You Deserve a Cut. *Washington Monthly*, 2019. július 12. Online: <https://washingtonmonthly.com/2019/07/12/what-your-data-is-really-worth-to-facebook/>
- Srniczek, Nick: We Need to Nationalise Google, Facebook and Amazon. Here's Why. *The Guardian*, 2017. augusztus 30. Online: www.theguardian.com/commentisfree/2017/aug/30/nationalise-google-facebook-amazon-data-monopoly-platform-public-interest
- Sunstein, Cass: *Laws of Fear. Beyond the Precautionary Principle*. Cambridge, Cambridge University Press, 2005.
- Van der Sloot, Bart – Frederick Zuiderveen Borgesius: Google and Personal Data Protection. In Aurelio Lopez Tarruella (szerk.): *Google and the Law. Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models*. The Hague, TMC Asser Press – Springer, 2012. 75–112.
- Y2K bug. *Encyclopedia Britannica*. Online: www.britannica.com/technology/Y2K-bug

Vákát

Detrekői Zsuzsa

Az EU szerzői jogi direktívája: segélykiáltás a hazai videómegosztó platformokért



A szerzői jogi irányelv 2019-es implementációja jelentősen befolyásolja a videómegosztó platformok életét, nemcsak a nagy nemzetközi platformokét, hanem a helyi kis szolgáltatók életét is. Mivel az irányelv megszünteti a felhasználói tartalmak esetén a felelősségkorlátozás intézményét, és közvetlenül felelőssé teszi a szolgáltatókat a felhasználók cselekedeteiért, a videómegosztó szolgáltatások élete jelentősen változni fog. A cikk a lehetséges gyakorlati problémákat tárja fel.

Bevezetés

Az Európai Unió 2015-ös Digital Single Market stratégiája jelentős változást hozott az online videómegosztó szolgáltatások életében.

Az internet elterjedésével és a felhasználók által megosztott tartalmak mennyiségének növekedésével a szabályozás is igyekezett megfelelően kezelni a tartalmakért való felelősség kérdését. Tekintettel a nagy mennyiségű tartalomra, és annak belátására, hogy a tartalmak elérhetővé tételében közreműködő szolgáltatók nem tudják ellenőrizni a felhasználók által feltöltött tartalmakat, a szabályozás azon szolgáltatók irányában, amelyek a felhasználók számára tartalommegosztást tettek lehetővé, immunitást biztosítottak a felhasználói tartalmakkal kapcsolatban. Az első ilyen szabályozási modellt természetesen az Amerikai Egyesült Államokban fogadták el, 1998-ban a Digital Millennium Copyright Act (DMCA) keretében.¹ Ezt másolta le és bővítette ki az EU 2000-ben az Elektronikus kereskedelemről szóló irányelvvel.² A szabályozás lényege, hogy „Safe Harbor”-t, azaz úgynevezett biztonságos menedéket biztosítanak a közvetítő szolgáltatók egyes típusai – ideértve a tárhelyszolgáltatókat is – számára, abban az esetben, ha a jogsértő tartalom közzétételére nincs ráhatásuk, vagy azokat értesítés alapján eltávolítják. Tárhelyszolgáltatások esetén, aminek a videómegosztó szolgáltatások is minősülnek, bevezették az úgynevezett

¹ The Digital Millennium Copyright Act of 1998–U.S. Copyright Office Summary. 1998.

² Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (‘Directive on Electronic Commerce’). L 178 (2000. július 17.).

értesítési és eltávolítási eljárást (notice and take down eljárás), amely meghatározott formai kötöttségekkel és határidőkkel folyamatí útra terelte az eltávolítást és így a lehetséges mentesülést.

A Safe Harbor klauzula először az Egyesült Államokban mérettetett meg. A leg-híresebb ügy a Viacom kontra YouTube ügy volt. A valódi kérdés a perben, hogy ki viselje a felhasználók által feltöltött tartalmak (User Generated Content – UGC) figyelésének és a felhasználók által az internetre feltöltött illegális anyagok azonosításának költségeit: a szolgáltatók vagy a szerzői jogok tulajdonosai?

Dióhéjban a per története: 2007 márciusában a Viacom, egy amerikai média-konzern összesen 160 ezer eltávolítási kérelmet küldött az akkor már a Google tulajdonában lévő YouTube-nak. A notice and take down kérelmek többek között a South Parkkal, a Spongyabobbal és a Daily Show-val kapcsolatban érkeztek. Bár a YouTube eleget tett az eltávolítási kérelmeknek, a Viacom egymilliárd dollárra perelte a Google-t a felhasználók által elkövetett szerzői jogsértésekért. A Viacom keresetét számos további kereset követte, sportligák és zenekiadók kezdték perelni a Google-t ugyanezen az alapon. A Viacom egy sajtóközleményében azzal vádolta meg a YouTube-ot, hogy „a technológiát a szerzői jogok szándékos megsértésére használta fel, megfosztva az írókat, zeneszerzőket és előadóművészeket a munkájukért járó jövedelmektől, ezzel csökkentve a kreatív iparág ösztönzőit, illetve a YouTube mások törvénysértéséből profitál”.

2010-ben az elsőfokú bíróság kimondta, hogy a YouTube a Safe Harbor-védelem alatt áll, a szerzői jogsértésekre utaló körülmények ellenére.³ A bíró úgy ítélte meg, hogy bár a cég általánosságban tudomással bírt arról, hogy a felhasználók szerzői jogvédelem alatt álló tartalmakat töltöttek fel az oldalra, azonban azt nem tudhatta, hogy mely tartalmak esetében rendelkeztek az ehhez szükséges engedéllyel. A bíró szerint, ha a videómegosztó oldalakat minden feltöltött videó proaktív ellenőrzésére köteleznék, az „sértené a DMCA működését”. A bíró továbbá megjegyezte, hogy DMCA által meghatározott értesítési rendszer hatékony volt, mivel a YouTube sikeresen kezelte a Viacom által kiadott tömeges eltávolítási kérelmet. Innentől eljárásjogi cselekmények sora következett, a Viacom fellebbezése, amelyet az ügy első fokra történő visszahelyezése követett, majd mivel az ismét a YouTube-nak adott igazat, a Viacom ismét fellebbezett.⁴ Végül, mielőtt jogerős ítélet születhetett volna, a két cég megállapodást kötött az ügyben. Az egyezség részletei ugyan bizalmasak, azonban annyit tudni, hogy nem történt pénzmozgás. Illetve nem sokkal később bevezették a Content ID-t, a Google által kifejlesztett szűrőszoftvert a YouTube-on található szerzői joggal védett tartalmak azonosítására és kezelésére.

³ A YouTube nyerte az összefoglaló ítéletet a Viacom DMCA-perben: Kurt Opsahl: YouTube Wins Summary Judgment in Viacom DMCA Lawsuit. *Electronic Frontier Foundation*, 2010. június 23.

⁴ Viacom Int'l, Inc. kontra YouTube, Inc. – 676 F.3d 19 (2d Cir. 2012.); A New York-i Kerületi Bíróság összefoglaló ítélete: Viacom International Inc. v. YouTube, Inc. no. 1:07-cv-02103-LLS, 2013. április 18.

Az EU 2015-ben, a Digital Single Market Strategy meghirdetésével vágott bele a 20 évig uralkodó jogintézmény felülvizsgálatába.⁵ A Bizottság céljaul tűzte ki, hogy megvizsgálja, „fokozni kell-e az interneten fellelhető jogellenes tartalom elleni védelem szintjét. Az internetes platformok értékelésével egy időben a Bizottság elemzi majd annak szükségességét, hogy a szólásszabadság és a tájékoztatáshoz való jog alapvető jogára gyakorolt hatás tükrében vezessen-e be olyan új intézkedéseket a jogellenes internetes tartalmak kezelésére, mint például – a legális tartalom megőrzése mellett – a jogellenes tartalom eltávolítására vonatkozó szigorú eljárások, vagy megköveteljen-e gondossági kötelezettséget a közvetítőktől, azaz hogy nagyobb felelősséggel és kellő gondossággal járjanak el a hálózat- és rendszerkezelés során.”⁶

2016-ban a stratégia része lett a szerzői jogok kapcsán az úgynevezett „value gap”, azaz értékhiány megszüntetése, amely arra szolgált, hogy a szerzői jog által védett tartalmak jogtulajdonosai is részesedjenek abból a bevételből, amely a felhasználó tartalmak közzétételét lehetővé tévő szolgáltatóknál keletkeznek.⁷

Ennek alapján született meg két fontos irányelv módosítása, amelyek megin-gatták a Safe Harbor intézményét. Az egyik az audiovizuális médiaszolgáltatásokról szóló irányelv (AVMSD) 2018. novemberi módosítása,⁸ a másik a szerzői jogi irányelv 2019. áprilisi módosítása.⁹

Bár mind a két irányelv külön rendelkezik a videómegosztó platformokról, nem sikerült azonos megnevezést használni ugyanarra a szolgáltatásra. Míg az AVMSD a „videómegosztóplatform-szolgáltatás” terminológiát alkalmazza, a szerzői jogi irányelv módosítása az „online tartalommesztó szolgáltató” kifejezést használja. Nemcsak az elnevezésben van diszkrepancia a két irányelv között, hanem a felelősségi rendszer felállításában is.

Egyfelől a szerzői jogi irányelv kötelezővé teszi a szolgáltatók számára, hogy megszerezzék a nyilvánossághoz való közvetítéshez vagy a nyilvánosság számára

⁵ European Commission: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Single Market Strategy for Europe. COM(2015)192 végleges (2015. május 6.).

⁶ Európai Bizottság: A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – Európai digitális egységes piaci stratégia. COM(2015)192 végleges (2015. május 6.).

⁷ European Commission: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Single Market Strategy for Europe. COM(2015)192 végleges (2015. május 6.).

⁸ Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 Amending Directive 2010/13/EU on the Coordination of Certain Provisions Laid Down by Law, Regulation or Administrative Action in Member States Concerning the Provision of Audiovisual Media Services (Audiovisual Media Services Directive) in View of Changing Market Realities. L 303/69 (2018. november 28.).

⁹ Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on Copyright and Related Rights in the Digital Single Market and Amending Directives 96/9/EC and 2001/29/EC. L 130/92 (2019. május 17.).

hozzáférhetővé tételhez szükséges engedélyeket, és ezzel ex ante ellenőrzést vár el a videómegosztó szolgáltatóktól minden felhasználók által feltöltött videó esetében. Másfelől az AVMS kifejezetten kizárja az ex ante kontroll lehetőségét, amikor kijelenti, hogy a videómegosztó szolgáltatók által a jogellenes tartalmak eltávolítására tett intézkedések nem „vezethetnek előzetes ellenőrzési intézkedésekhez vagy a tartalom feltöltésének olyan szűréséhez, amely nem felel meg a 2000/31/EK irányelv 15. cikkének”, ugyanakkor eredményként elvárja, hogy biztosítsák, hogy a nemkívánatos tartalmak ne legyenek elérhetőek a szolgáltatáson.¹⁰

17. cikkely

Közel két évtized után tehát – vélhetően a szerzői jogi lobbi erős nyomására – sikerült megtörni a Safe Harbor klauzulát. A 17. cikkely kimondta, hogy a videómegosztók maguk is nyilvánossághoz közvetítést, illetve nyilvánosság számára hozzáférhetővé tételt valósítanak meg azzal, hogy a felhasználók által feltöltött tartalomhoz hozzáférést biztosítanak. Emiatt szükséges engedélyt beszerezni a jogtulajdonosoktól.

Engedély hiányában akkor mentesülnek a felelősség alól, ha bizonyítják, hogy:

- a) minden tőlük telhetőt megtettek az engedély megszerzése érdekében (licenc);
- b) a szakmai gondosság magas szintű ágazati normáinak megfelelően minden tőlük telhetőt megtettek annak biztosítása érdekében, hogy azon konkrét műveket és más védelem alatt álló teljesítményeket, amelyekre vonatkozóan a jogosultak megadták a szolgáltatóknak a lényeges és szükséges információkat, elérhetetlenné tegyék (szűrőszoftver);
- c) továbbá minden esetben a jogosultak megfelelően indokolt értesítésének kézhezvételét követően haladéktalanul intézkedtek az értesítés tárgyát képező művek vagy más védelem alatt álló teljesítmények hozzáférhetetlenné tétele vagy honlapjaikról történő eltávolítása érdekében, valamint a b) pontnak megfelelően minden tőlük telhetőt megtettek azok jövőbeli feltöltésének megakadályozására (notice and take down eljárás).

Bár a direktíva célja egyértelműen a videómegosztó oldalak kordába terelése volt, de a definíciós hiányosságok nem értek véget azzal, hogy nem sikerült az AVMSD-vel közös meghatározást találni ezekre az oldalakra. A direktíva szerint: „online tartalommesztó szolgáltató”: olyan, az információs társadalommal összefüggő szolgáltatást nyújtó szolgáltató, amelynek fő vagy egyik fő célja a felhasználói által feltöltött, jelentős mennyiségű, szerzői jogi védelem alatt álló mű vagy más védelem alatt álló teljesítmény tárolása és ahhoz hozzáférés biztosítása a nyilvánosság

¹⁰ Giancarlo F. Frosio: Reforming Intermediary Liability in the Platform Economy: A European Digital Single Market Strategy. *Northwestern University Law Review Online*, 112. (2017), 19–46.

számára, amely műveket és más védelem alatt álló teljesítményeket nyereségszerzési céllal összerendezi és promotálja.

Nehéz megbecsülni, hogy a blogbejegyzések mennyiben minősülnek szerzői jogilag védett műnek, nyilván ezeket egyesével kellene vizsgálni. Azonban a blogszolgáltatások ugyanúgy ezeket a bejegyzéseket rendezik össze és promotálják, és mivel valamiből ezeket az oldalakat is fenn kell tartani, reklámokat helyeznek el rajtuk, ami a nyereségszerzés célját szolgálja, így adott esetben kimeríthetik a fenti definíciós kritériumokat. A blogszolgáltatásoknak különös jelentősége van a szólásszabadság biztosítása céljából. Itt jelenhetnek meg kritikus vélemények, amelyek valamely intézményrendszert vonnak kérdőre, és máshol nem kaptak lehetőséget a megjelenésre. A fenti definíciós bizonytalanság tehát súlyos hátrányt jelenthet a szólásszabadság szempontjából.

Összefoglalva, a 17. cikkely három konszekutív feltételt ír elő a felelősség alóli mentesüléshez, a licenc megszerzését, szűrőszoftver használatát, és a notice and take down eljárás alkalmazását. A két első feltétel jelentős problémát okozhat a szolgáltatóknak, az alábbiakban bemutatjuk, miért.

Engedélyezés

Az engedélyezés, azaz a szükséges licencek megszerzése a legösszetettebb folyamat az audiovizuális alkotások, például videók, mémek, filmek, tévémsorok esetében. Minden kreatív résztvevőtől – ideértve a szerzőket, színészeket, rendezőt, zeneszerzőt, operatőrt stb. – engedélyt kell szerezni a kész mű felhasználásához.¹¹ Mindemellett minden egyes felhasználási módra külön engedélyt kell szerezni a licencszerződésekben, ideértve a nyilvánosságához közvetítést és a nyilvánosság számára való hozzáférhetővé tételt.¹² Ezekben a licencszerződésekben a felhasználás időtartamát és területét is meg kell határozni.¹³

A nagy filmstúdiók ezért külön szervezeti egységeket hoznak létre csak azért, hogy egy adott filmhez szükséges jogokat tisztázzák, és az engedélyeket megszerezzék. Ezen filmstúdiók esetében a producerek minden szükséges jogot igyekeznek előzetesen megszerezni a résztvevőktől, hogy ez alapján a filmet terjeszthessék világszerte, és engedélyezhessenek különböző felhasználásokat (például mozivetítést, tévés lejátszást, VOD-letölthetőséget).¹⁴

Általánosságban egy, a művet felhasználni kívánó szolgáltató esetében az engedélyezés két különböző módon történhet, a szerzői jogok tulajdonosától vagy közös jogkezelő szervezetektől. Ez utóbbinak előnye lehet, hogy egyszerűsítik

¹¹ A szerzői jogról szóló 1999. évi LXXVI. törvény 64. §.

¹² A szerzői jogról szóló 1999. évi LXXVI. törvény 16. §.

¹³ A szerzői jogról szóló 1999. évi LXXVI. törvény 43. §.

¹⁴ Cathy Jewell: From Script to Screen: What Role for Intellectual Property? *WIPO*.

a jogkezelést. A jogdíjak egyben történő letárgyalása, az engedélyezés, a monitorozás, a jogdíjak beszedése és elosztása egyes esetekben a kollektív kezeléssel könnyebbnek bizonyul. Példaként egy szerző, egy színész vagy egy producer nem léphet kapcsolatba minden egyes rádióállomással, hogy megtárgyalják a művek felhasználásának engedélyezését és díjazását. Ugyanez igaz fordítva is, nem célszerű és rendkívül időigényes a felhasználók számára is az egyesével történő engedélyezés, például a rádióállomások nem tudnának minden egyes szerzőtől, illetve előadóművészról egyesével engedélyt kérni a dalaik lejátszásához.¹⁵

Magyarországon a közös jogkezelést a jogalkotó két esetre bontotta, az önkéntes közös jogkezelés esetére, illetve a kötelező kiterjesztett közös jogkezelés esetére. A kötelező közös jogkezelés esetén a művészek nem választhatják meg, hogy milyen megállapodási formát szeretnének, mivel az engedélyezés a közös jogkezelő szervezeteken keresztül történik, erre példa a televíziócsatornák kódolatlan terjesztése. Az önkéntes közös jogkezelés ezzel szemben annyi szabadságot enged, hogy az alpból a közös jogkezelő szervezet által képviselt művészeknek évente egyszer lehetőségük van az összes általuk létrehozott mű tekintetében egységesen kilépni a közös jogkezelés rendszeréből.¹⁶

A művészek egyes csoportjait, így a szerzőket, előadóművészeket, a lemezkiadókat, a fotográfusokat külön közös jogkezelő szervezetek képviselik.¹⁷

A közös jogkezelő szervezetek árazási modellje általában elég kártékony. Annak ellenére, hogy a magyar szerzői jogi törvény¹⁸ előírja, hogy a jogdíjaknak az elért bevétellel arányosnak kell lenniük, a közös jogkezelő szervezetek sok esetben minimumdíjakat állapítanak meg felhasználásonként. A hazai video on demand (VOD) szolgáltatások indulásakor például az Artisjus 8%-át kérte a bevételnek letöltésenként. Ezzel szemben az előadóművészeket képviselő EJI-Mahasz a jogdíjat filmperc/napban határozta meg, aminek eredményeként ennek az egy közös jogkezelő szervezetnek az ötszörösét kellett volna fizetni, mint maga a filmletöltés ára, még abban az esetben is, ha senki nem nézte meg.¹⁹ Ezt még ki kell egészíteni azzal, hogy a szolgáltatónak legalább két, illetve három közös jogkezelő szervezetnek kellett volna fizetnie egy adott filmért.²⁰

A magas árak miatt az üzleti modellek kiszámíthatatlanok, a szolgáltatók nem tudnak előre tervezni. Emiatt folyamatos viták alakultak ki a közös jogkezelő

¹⁵ Collective Management of Copyright and Related Rights. *WIPO*.

¹⁶ Collective Management of Copyright and Related Rights. *WIPO*; 2016. évi XCIII. törvény a szerzői jogok és a szerzői joghoz kapcsolódó jogok közös kezeléséről 4. § (6) bekezdése és 17. §; kiterjesztett kollektív joggazdálkodás: Extended Collective Management of Rights. *Előadóművészi Jogvédő Iroda*.

¹⁷ Szellemi Tulajdon Nemzeti Hivatala: *Bejegyzett jogkezelő szervezetek adatai*.

¹⁸ 1999. évi LXXVI. törvény a szerzői jogról.

¹⁹ Lásd az Előadóművészi Jogvédő Iroda honlapját.

²⁰ Online jogdíjak felosztása. *Artisjus*; Lehívások (internet) jogdíjak. *Előadóművészi Jogvédő Iroda*.

szervezetek és a felhasználók között az engedélyezéssel kapcsolatban.²¹ VOD-ok esetében a szerzői jogi törvény szerint az engedélyt közvetlenül az előállítótól vagy a forgalmazótól kellene megszerezni, ennek ellenére az EJI jogdíjat követel a VOD-felhasználások után is, külföldi filmek esetén is (külföldi közös jogkezelő szervezetekkel való kölcsönös megállapodásokra hivatkozva).²² Illusztrációként: ha egy szolgáltató megszerzi a *Bakancslista* című amerikai film video-on-demand letöltésére az engedélyt a Warnertől, és ez alapján online bemutathatja a filmet, az EJI minden letöltés után jogdíjat fog megpróbálni beszedni Jack Nicholson filmbeli előadásáért (bár erről Jack Nicholson nyilván nem is tud), mivel álláspontja szerint a film online lejátszására közös jogkezelésen keresztül szerezhető engedély, nem a jogtulajdonostól vagy annak képviselőjétől.²³

Folyamatosan jelennek meg új közös jogkezelő szervezetek, amelyek azt próbálják bizonyítani, hogy jogosultak valamelyfajta szerzői jogi felhasználás után díjat beszedni.²⁴

A közös jogkezelő szervezetektől való engedélyszerzés feltétele a folyamatos riportolás, amely elég nehéz, időigényes feladat. Audiovizuális műveknél úgynevezett „music cue sheet”-eket kell kitölteni. A music cue sheeteknek tartalmazniuk kell a film címét, a lejátszás időpontját, a műsor hosszát, a lejátszott zenemű hosszát, információkat az előállítóról, a zeneszám címét és szerzőjét, kiadóját, valamint a felhasználás hosszát és időpontját. Ez az elszámolás alapja, ezek nélkül a jogdíjak kifizetése lehetetlen.²⁵

Összességében tehát az engedélyezés egy nagyon összetett, komplex, sokszor kaotikus folyamat sok résztvevővel.²⁶ Ráadásul a fenti jogbizonytalanság és az árázási modellek sem segítik az online szolgáltatások fejlődését.

Szűrőszoftver

Tekintettel az ellenőrizendő videók jelentős mennyiségére, ahhoz, hogy a szolgáltatók minden tőlük telhetőt megtegyenek annak biztosítása érdekében, hogy a jogosultak által jelzett konkrét műveket elérhetetlenné tegyék, szűrőszoftvert kellene használniuk. Egy több millió videót tartalmazó (és a két magyar megosztó bőven itt tart) szolgáltatás esetében manuálisan gyakorlatilag megoldhatatlan a feladat. Egy ilyen szűrőszoftver kifejlesztése és működtetése azonban nehézségeket is okozhat.

²¹ A moderátorokkal készített interjúk és a szerzők saját tapasztalatai alapján.

²² A szerzői jogról szóló 1999. évi LXXVI. törvény 66. §-a; Magyar Színjátszók Társasága (EJI) tarifái: Lehívásos (internet) jogdíjak. *Előadóművész Jogvédő Iroda*.

²³ T-Online Magyarország Kft. v. 8.P.24.159/2006.

²⁴ Koi Tamás: Új jogdíj miatt fájhat a feje a tévéseknek. *HWSW*, 2015. december 23.

²⁵ BBC Academy: Silvermouse (for Production Paperwork) Reporting Music in the BBC Cue Sheet.

²⁶ Christina Angelopoulos – Joao Pedro Quintais: Fixing Copyright Reform. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 10. (2019), 2. 147–172.

A már említett Google Content ID fejlesztése több mint 50 ezer munkaórát vett igénybe, és legalább 60 millió dollárba került. A Google-nak ugyan megvannak az ehhez szükséges forrásai, de a kis hazai videómegosztó oldalak nyilván nem engedhetnek meg maguknak egy ekkora fejlesztést.²⁷

További probléma az eltávolítandó tartalom azonosítása. Az egyes tartalmak szűréséhez a szolgáltatóknak mintákra van szükségük a tartalomból, hogy ellenőrizni tudják a feltöltött videókat.²⁸ A jogtulajdonosoknak még a film premierje előtt hozzáférést kellene biztosítani a még le nem vetített film részletéhez, hogy ezt megosszák a videómegosztó szolgáltatókkal a szűrés érdekében. Nyilván a premier előtti filmeket a stúdiók a legnagyobb titokban kezelik. Bár a magyar szerzői jogi törvény lehetővé teszi a film online megosztásának közvetlen engedélyezését, a copyright direktíva implementációjának hazai nyilvános konzultációján 2019 novemberében az EJI jelezte, hogy a filmek kiszivárgásától való félelem miatt nem támogatják a mintamegosztás lehetőségét. A mintamegosztás megszervezése amúgy egy hatalmas adminisztratív feladat lenne sok nehézséggel, mivel az EU-s videómegosztó szolgáltatásoknak a világ minden táján megjelenő filmekből mintát kellene kapniuk, hogy szűrni tudjanak ez alapján. Nem beszélve arról, hogy a szoftver is hibázhat, ennek példája volt a YouTube-on a fehér zajos videók jogsértő tartalomként való azonosítása.²⁹

Notice and take down eljárás

A 2000-es e-kereskedelmi irányelv³⁰ által bevezetett notice and take down eljárás eddig hatékony szabályozási eszköznek tűnt. Ez az eljárás megfelel a 17. cikk (4) c) pontjában előírt eltávolítási kötelezettségnek. Két hazai videómegosztó, az Indavideo és a Videamoderátor szerint a szerzői jogi irányelv hazai implementálása előtti időben legalább havonta 1000 videót távolítottak el. Mind a két szolgáltatás az e-kereskedelmi törvény³¹ által előírt notice and take down eljárásnál jóval egyszerűbb módon lehetőséget biztosít a felhasználóknak a szerzői jogilag védett tartalmak

²⁷ Thomas Spoerri: On Upload-Filters and other Competitive Advantages for Big Tech Companies under Article 17 of the Directive on Copyright in the Digital Single Market. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 10. (2019), 2. 173–186.

²⁸ A moderátorokkal készült interjúk alapján.

²⁹ Chris Baraniuk: White Noise Video on YouTube Hit by Five Copyright Claims. *BBC News*, 2018. január 5.

³⁰ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market ('Directive on Electronic Commerce'). L 178 (2000. július 17.).

³¹ 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről.

jelzésére, és a jelzés alapján általában a törvényben meghatározott határidő előtt a moderátorok törölték a videókat. A videómegosztó szolgáltatások ellenőrzésének terhe azonban eddig a jogtulajdonosokat terhelte.

Szabad felhasználás

A szabad felhasználás vagy a DMCA szerinti fair use a szerzői jog korlátozása, amely lehetővé teszi a szerzői joggal védett anyagok korlátozott felhasználását anélkül, hogy előzetesen engedélyt kellene szerezni a szerzői jog tulajdonosától. Célja, hogy egyensúlyt teremtsen a szerzői jogok tulajdonosainak érdekei, illetve a kreatív alkotások szélesebb körű felhasználásához fűződő érdekek között azáltal, hogy lehetővé tesz bizonyos felhasználásokat, amelyek a törvény által biztosított engedély hiányában jogsértésnek minősülnének. A magyar szerzői jogi törvény szerint: „Természetes személy magáncélra a műről másolatot készíthet, ha az jövedelemszerzés vagy jövedelemfokozás célját közvetve sem szolgálja, feltéve, hogy a felhasználással érintett műhöz jogszerűen fért hozzá.”

A 17. cikkely új eseteket határoz meg (például idézés, kritika, ismertetés; paródia vagy pastiche céljára történő felhasználás), de a 17. cikkely szövegéből nem derül ki egyértelműen, hogy csak ezen felhasználások jelentik-e a szerzői jog szabad felhasználás alapján történő kizárólagos korlátozását, vagy a szerzői jogi törvény korábbi rendelkezései alapján egy ennél általánosabb körre is érvényes lenne a korlátozás. Mindenesetre az online tartalommesztó szolgáltató definíciója eleve kizárja a szabad felhasználás lehetőségét, mivel a definíció feltételül szabja a nyereségszerzési célt, míg a szabad felhasználás kizárja a jövedelemszerzés vagy -fokozás célját.³²

Felmerülő gyakorlati problémák

A 17. cikkely kimondja, hogy alkalmazása nem vezethet általános nyomkövetési kötelezettséghez. A gyakorlatban azonban a moderátoroknak minden feltöltött videónál meg kellene határozniuk azt, hogy a videó tartalmaz-e szerzői jogilag védett művet.³³ Ezt sok esetben nehéz megállapítani. Zenei tartalmaknál könnyebbnek tűnik, bár itt is nehéz eldönteni, hogy az adott videóra – esetleg csak pár másodperc zenénél – vonatkozik-e a szabad felhasználás, illetve az Egyesült Államokban fair use (ha van ilyen) valamely esete.³⁴ Az elhíresült *Lenz v. Universal*

³² Act LXXVI of 1999 on copyright (2018. május 13.): a szerzői jogról szóló 1999. évi LXXVI. törvény 35. §.

³³ Christina Angelopoulos – Joao Pedro Quintais: Fixing Copyright Reform. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 10. (2019), 2. 147–172.

³⁴ Angelopoulos–Quintais (2019): i. m.

(avagy a „Dancing Baby”) ügyben egy anya egy 29 másodperces videót töltött fel a YouTube-ra, amelyen a kisgyermek a *Let's Go Crazy* című Prince-dalra táncol. A Prince-dalok szerzői jogait birtokló Universal Music Publishing Group emiatt egy notice and take down kérelmet küldött a YouTube-nak, és felszólította, hogy távolítsa el a kérdéses videót. Emiatt több mint 10 év pereskedés követte a kérelmet, amelyben végül nem született valódi döntés, mert a felek megegyeztek.³⁵ És ez csak egy viszonylag könnyen felismerhető zenei tartalom esete. Annak eldöntése például, hogy egy demonstráció során egy felszólaló beszéde vagy előadása, amelyet feltöltenek valamely videómegosztó oldalra, szerzői jogvédelem alá esik-e, rendkívül időigényes, ha nem lehetetlen.

A szerzői jog tulajdonosa

Még abban az egyszerűnek tűnő esetben is, ha egy televíziós csatorna logója megjelenik egy feltöltött videón, a moderátorok nem lehetnek biztosak abban, hogy a tartalom jogosultja a televíziós csatorna, hiszen a műsor felhasználása alapulhat felhasználási szerződésen is.³⁶ Jelentős problémát jelent tehát, hogy hogyan lehet információt szerezni egy adott mű valódi szerzői jogi jogosultjáról. Előfordulhat, hogy a videót feltöltő felhasználók nem adnak információt a szerzői jogosultról, főleg ha a videót nem ők rögzítették. Esetleges szerzői jogot sértő videók esetén pedig jobbra direkt nem nyújtanak információt az azt feltöltő felhasználók.³⁷

A felhasználási engedély megszerzése

A videók nyilvánossághoz közvetítésének, illetve nyilvánosság számára hozzáférhetővé tételének kizárólagos joga a jogtulajdonost, illetve azt illeti meg, akinek erre a jogtulajdonos vagy az általa felhatalmazott személy vagy szervezet engedélyt adott. Ha a jogtulajdonos személye nem ismert, a közvetlen engedély megszerzése lehetetlen. Még abban az esetben is, ha a jogtulajdonos beazonosítható, személye ismert, a kapcsolattartó személy vagy szervezeti egység elérhetőségi adatainak megszerzése óriási kihívás. Ha esetlegesen a moderátoroknak sikerül felvenniük a kapcsolatot a megfelelő személlyel, és azok nem adnak engedélyt a mű felhasználására, a helyzet egyértelmű. A kérdés azonban az, hogy a folyamat során fel kell-e függeszteni a videó elérhetőségét, vagy sem. Illetve mi van, ha nem válaszolnak?

A közös jogkezelés lehetősége is kérdéseket vet fel. A közvetlen engedélyezési modell (zeneszerzők kivételével) ellenére a szerzői jogi irányelv implementációja

³⁵ Lenz v. Universal. *Electronic Frontier Foundation*.

³⁶ A moderátorokkal készült interjúk alapján.

³⁷ A moderátorokkal készült interjúk alapján.

kapcsán tartott nyilvános konzultáción számos közös jogkezelő szervezet jelent meg. Annak ellenére, hogy az irányelv lehetőséget biztosít az úgynevezett egyablakos jogosításra, amely esetben egy közös jogkezelő szervezet szedi be a jogdíjakat, és osztja szét a többi közös jogkezelő szervezet között, ahogy ez a televíziós csatornák egyidejű változatlan továbbközvetítése esetében történik, a konzultáción jelen lévő legalább három közös jogkezelő szervezet jelezte, hogy külön kívánnak jogdíjat szedni.³⁸ A korábban jelzett árazási modellek mellett lehetetlen megállapodni az összes közös jogkezelő szervezettel anélkül, hogy a szolgáltatások lényege sérülne.

Sőt, fennáll annak a lehetősége, hogy a közös jogkezelés ellenére a valódi jogtulajdonos jelenik meg a szolgáltatónál, és kártérítést követel az engedély hiánya miatt, mert a jogtulajdonos nem tud például arról, hogy magyar közös jogkezelő szervezetek járnak el a nevükben. A jogrendszerek közötti különbségek miatt például egy amerikai filmstúdió jogosan nyújthat be olyan esetben igényt, amikor egy feltöltött tartalomra hiányzik tőle az engedély, nem tudva, hogy közös jogkezelő szervezetek képviselik.

Riportolási kötelezettségek teljesítése

A jogtulajdonosok általában tisztában vannak munkájuk pontos tartalmával, így számukra elegendő a megtekintések számát jelenteni. A videómegosztó szolgáltatások esetében is a közös jogkezelő szervezeten keresztül engedélyezés feltétele, hogy a szolgáltatók részletes jelentést – például a korábban már bemutatott music cue sheetek alapján – nyújtsanak a közös jogkezelő szervezetek számára, mivel ez a jogdíjak elosztásának alapja. A moderátorok vélhetően nem tudják az összes videóban felhasznált összes művet feltérképezni, és erről jelentést készíteni.

Sőt a fent leírt négy gyakorlati probléma megoldása minden egyes feltöltött videó esetében teljesen irreális. A szolgáltatóknak minden tőlük telhetőt meg kell tenniük az engedély megszerzése érdekében, illetve annak biztosítása érdekében, hogy azon konkrét műveket és más védelem alatt álló teljesítményeket, amelyekre vonatkozóan a jogosultak megadták a szolgáltatóknak a lényeges és szükséges információkat, elérhetetlenné tegyék; továbbá minden esetben. Az azonban nem egyértelmű, hogy mit jelent pontosan a „minden tőlük telhető” kritérium. Elegendő megpróbálni felvenni a kapcsolatot a jogtulajdonossal? Mi van, ha nem válaszol? Végül mi történik, ha a szolgáltatók minden erőfeszítésük ellenére nem tudnak megállapodni a közös jogkezelő szervezetekkel? Vagy csak az egyikükkel? Például, ha a kártékony árazási modellek vagy egy irreális riportolási kötelezettség miatt nem tudnak megállapodni, akkor a szolgáltatók megtették minden tőlük telhetőt? Ezek retorikai kérdéseknek tűnhetnek, de valószínűleg a moderátorok mindennap szembesülnek velük.

³⁸ Ahogy azt a közös jogkezelő szervezetek képviselői a nyilvános konzultáción jelezték.

Egy másik gyakorlati probléma a jogdíjak felosztása. Ha a közös jogkezelő szervezetek engedélyeket adnak, és beszedik a jogdíjakat, hogy tudják azokat felosztani megfelelő információ nélkül? Még ha a magáncélú másolás után történő felosztás rendszerét próbálják meg érvényesíteni, akkor sem rendelkeznek információval számos olyan videó készítőjéről, akiknek videója amúgy nagyon népszerű egy oldalon, például mémek esetében, pedig ők is ugyanúgy jogosultak lennének jogdíjra. Nem beszélve a szerzői joggal nem védett videókról, amelyeket nem lehet megkülönböztetni az elszámolás során a szerzői joggal védett videóktól, így a szolgáltatók ezek után is kénytelenek lennének fizetni.

Epilógus

Eredetileg a szöveg végén itt egy következtetésnek kellett volna szerepelnie, amely kitér arra, hogy a fent említett gyakorlati problémák mennyire megnehezítik a hazai videómegosztó szolgáltatók életét, a különbségekre a globális és a hazai szolgáltatók erőforrásai között, illetve hogy milyen kimenetelei lehetnek ezeknek a problémáknak, onnantól kezdve, hogy a tartalom jelentős része eltűnik, mert ellenőrizhetetlen, odáig, hogy az engedélyszerzés a közös jogkezelő szervezetektől olyan drága, hogy fenntarthatatlanná teszi a hazai videómegosztó szolgáltatások működtetését, ne adj isten azok becsukásához vezethet.

Azonban az a furcsa helyzet állt elő, hogy a nyilvános konzultáción részt vevő és jelentős lobbitevékenységet folytató közös jogkezelő szervezetek eddig még nem jelentek meg a videómegosztó szolgáltatásoknál, illetve ha azok megkeresték az általuk illetékesnek tartott szervezetet, az nem válaszolt. A jelenlegi helyzet tehát olyan, mintha meg sem született volna a 17. cikkely.

Felhasznált irodalom

2016. évi XCIII. törvény a szerzői jogok és a szerzői joghoz kapcsolódó jogok közös kezeléséről
- Angelopoulos, Christina – Joao Pedro Quintais: Fixing Copyright Reform. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 10. (2019), 2. 147–172.
- Baraniuk, Chris: White Noise Video on YouTube Hit by Five Copyright Claims. *BBC News*, 2018. január 5. Online: www.bbc.com/news/technology-42580523
- BBC Academy: *Silvermouse (for Production Paperwork) Reporting Music in the BBC Cue Sheet*. Online: http://downloads.bbc.co.uk/academy/academyfiles/bs_silvermouse_indies_cue_sheet.pdf
- Collective Management of Copyright and Related Rights. *WIPO*. Online: www.wipo.int/copyright/en/management/
- Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 Amending Directive 2010/13/EU on the Coordination of Certain Provisions Laid Down by Law, Regulation or Administrative Action in Member States Concerning the Provision of Audiovisual Media Services (Audiovisual Media Services Directive) in View of Changing

- Market Realities. L 303/69 (2018. november 28.). Online: <https://eur-lex.europa.eu/eli/dir/2018/1808/oj>
- Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on Copyright and Related Rights in the Digital Single Market and Amending Directives 96/9/EC and 2001/29/EC. L 130/92 (2019. május 17.). Online: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019L0790&rid=1>
- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market ('Directive on Electronic Commerce'). L 178 (2000. július 17.). Online: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0031&from=EN>
- Európai Bizottság: *A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – Európai digitális egységes piaci stratégia.* COM(2015)192 végleges (2015. május 6.). Online: <https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52015DC0192&from=EN>
- European Commission: *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Single Market Strategy for Europe.* COM(2015)192 végleges (2015. május 6.). Online: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52015DC0192&from=EN>
- Extended Collective Management of Rights. *Előadóművészi Jogvédő Iroda.* Online: https://eji.hu/cikk/extended_collective_management_of_rights
- Frosio, Giancarlo F.: Reforming Intermediary Liability in the Platform Economy: A European Digital Single Market Strategy. *Northwestern University Law Review Online*, 112. (2017), 19–46.
- Jewell, Cathy: From Script to Screen: What Role for Intellectual Property? *WIPO.* Online: www.wipo.int/pressroom/en/stories/ip_and_film.html
- Koi Tamás: Új jogdíj miatt fájhat a feje a tévéseknek. *HWSW*, 2015. december 23. Online: www.hwsz.hu/hirek/54953/jogdij-tevecsatorna-tv-digitalfilm-teveszolgtato-filmjus-artistjus.html
- Lehívásos (internet) jogdíjak. *Előadóművészi Jogvédő Iroda.* Online: https://eji.hu/cikk/lehivasos_internet_jogdijak
- Lenz v. Universal. *Electronic Frontier Foundation.* Online: www.eff.org/cases/lenz-v-universal
- Online jogdíjak felosztása. *Artistjus.* Online: www.artistjus.hu/wp-content/uploads/2020/01/I20tarifa.pdf
- Opsahl, Kurt: YouTube Wins Summary Judgment in Viacom DMCA Lawsuit. *Electronic Frontier Foundation*, 2010. június 23. Online: www.eff.org/deeplinks/2010/06/YouTube-wins-summary-judgment-viacom-dmca
- Spoerri, Thomas: On Upload-Filters and other Competitive Advantages for Big Tech Companies under Article 17 of the Directive on Copyright in the Digital Single Market. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 10. (2019), 2. 173–186.
- Szellemi Tulajdon Nemzeti Hivatala: *Bejegyzett jogkezelő szervezetek adatai.* Online: https://kjk.sztnh.gov.hu/en/szervezetek_nev_szerint_angol
- The Digital Millennium Copyright Act of 1998. U.S. Copyright Office Summary.* 1998. Online: www.copyright.gov/legislation/dmca.pdf
- Viacom International Inc. v. YouTube, Inc. no. 1:07-cv-02103-LLS*, 2013. április 18. Online: www.docketalarm.com/cases/New_York_Southern_District_Court/1—07-cv-02103/Viacom_International_Inc._et_al_v._YouTube_Inc._et_al/452/
- Viacom Int'l, Inc. kontra YouTube, Inc. – 676 F.3d 19 (2d Cir. 2012.).* Online: www.lexisnexis.com/community/casebrief/p/casebrief-viacom-int-l-inc-v-YouTube-inc

Vákát

Klein Tamás

Az újmédia szabályozásának új iránya? – A Digital Services Act alapjogvédelmi mechanizmusa



A modern technológiák által a demokráciával szemben támasztott kihívások között kiemelt jelentőségű az újmédia szolgáltatóinak működése, különös tekintettel a szolgáltatásoknak a demokratikus nyilvánosságra és eljárásokra gyakorolt felforgató hatására. A tudományos diskurzusban évek óta élénken jelen van a szolgáltatók közérdekű kötelezettséggel való megterhelésének lehetősége, még-hozzá elsősorban a felhasználók alapjogainak védelme érdekében. Az alapjogvédelem eredeténél fogva klasszikusan az állami jogsértéssel szembeni alkotmányos védelemként jelenik meg: az államot kötelezi a jogok tiszteletben tartására (egyes esetekben a jogok érvényesülésének biztosítására), és/vagy az egyénnek alanyi jogi jogosultságot biztosít a jog kikényszerítésére. Ugyanakkor az alapjogoknak a magánjogviszonyokban, nem az állammal szemben érvényesíthető (horizontális hatályú) védelme mellett egyre erősebb, meggyőző érvek hozhatók fel. A Digital Services Act összetett eszközrendszerrel nyúl a digitális szolgáltatások szabályozásához, amelyben egy jövőendő horizontális hatályú alapjogvédelmi mechanizmus alapjai kontúrozódnak. Ennek az alapjogvédelmi mechanizmusnak a szükségességéről, tartalmáról (a kiolvasható alapjogi tesztről) és érvényesülésének várható nehézségeiről szól az alábbi tanulmány.

Az alapjogvédelem új megközelítésének szükségessége

Az alkotmányjogi gondolkodásnak vannak olyan évszázados alapvetései, amelyeket az idő, a társadalmi vagy akár a technológiai fejlődés vasfoga nem kezdhet ki. Az alapjogok védelmével kapcsolatban például az alapjogok katalógusába felvett jogosultságok száma gyarapodott, illetve a már elismert alapjogok tartamukban gazdagodtak, de az alapjogvédelem általános dogmatikája csak igen lassan módosul (fejlődik), és e fejlődés a revolúció helyett a lassú, alkotmányos tradíciókhoz szervesen illeszkedő evolúcióval jellemezhető. Az alapjogvédelem sajátossága (volt) az is, hogy az alapjogi jogviszonyok klasszikusan vertikális szerkezetűek, a közhatalmat gyakorló állam és a közhatalomnak kiszolgáltatott egyén közötti jogviszonyokban érvényesül, ahol az egyén védelmét szolgálja az állami önkénnyel szemben. Az állam és egyén viszonyrendszerében értelmezett alapjogok tehát egyfelől az egyén szabadságának, autonómiájának védelme érdekében az állam hatalma elé állítanak

garanciális, közjogi korlátokat, másfelől bizonyos állami szolgáltatások iránti igényeket alapoznak meg.¹

Az alapjogok dogmatikáját – mind általánosan (alapjog-korlátozás elvei, mércéi stb.), mind pedig az egyes alapjogok tekintetében – a nemzeti alkotmányos rendszerekben évszázados tradíció formálta. Ez az alkotmányjogi hagyomány hatja át a nemzetközi emberi jogi mechanizmusokat csakúgy, mint a tagállamok közös európai alkotmányos értékein alapuló Alapjogi Chartát is.² A véleménynyilvánítás szabadsága (anyajog) és a kommunikációs jogcsoportba tartozó alapjogok, mint a szólás- és a sajtószabadság magas alkotmányjogi értéktartalma és kitüntetett védelme is mélyen gyökerezik az alkotmányos tradícióban. A technológiai evolúció (néha revolúció) azonban a jogi szabályozást és a jogalkalmazást rendre a régi szabályok újragondolására, megújítására, az új társadalmi környezethez való igazítására készíti.³ A Gutenberg- és a Marconi-galaxisok hatása a társadalmi nyilvánosságra a maguk korában nem volt kisebb jelentőségű, mint az újmédia társadalmi diskurzusokat „felforgató” ereje.

A diskurzív-deliberatív demokrácia elméletének vezérgondolata, hogy a nyílt, szabad és szélesre tárt társadalmi vita (vagyis a demokratikus diskurzusok működése) a demokratikus eljárások elengedhetetlen előfeltétele. Az újmédia kora a technológia hozzáférhetőségéből fakadóan – sok tekintetben – a minden korábbinál plurálisabb nyilvánosság működésének lehetőségét ígérte és részben be is teljesítette. Ugyanakkor az újmédia nyilvánossága számos vonatkozásban hordozza a hagyományos nyilvánosság mintázatait, amelyek a látszólagos korlátlanság ellenére is szűkösseget eredményeznek. Ebben a jelenségben, amely valójában a platformtechnológia sajátos jellemzője, egyszerre van benne a korlátlanság ígérete és a szűkösség valósága. Az újmédia nyilvánosságának legjelentősebb szereplői, a közösségimédia-platformok magánnormaképzésük és magánnorma-érvényesítésük eredményeként rendkívüli hatást gyakorolnak nem csupán a véleménynyilvánítási szabadság alanyi oldalának érvényesülésére, az egyéni alapjogra, hanem az anyajog objektív, kollektív oldalára, a közviták alakulására, a demokratikus diskurzusok összetételére is, anélkül, hogy az alapjog-korlátozás alkotmányos követelményeinek érvényesítéséről számot kellene adniuk. Ennek a felismerésnek a hatására az alapjogi gondolkodásban megfogalmazódott az az igény, hogy az alapjogok, különösen a véleménynyilvánítás szabadságának védelme a platformok mint magánjogi jogalanyok tevékenységének közérdekű korlátjaként is érvényesüljenek.⁴

¹ Sári János – Somody Bernadette: *Alapjogok. Alkotmánytan II.* Budapest, Osiris Kiadó, 2008. 33.

² Az Európai Unió Alapjogi Chartája. 2016/C 202/02 (2016. június 7.).

³ A technológia médianyilvánosságra gyakorolt hatásának elméleti kérdéseiről lásd Udvary Sándor: *Media Revolution – Effects of Technological Development on Freedom of Expression.* In Kapa Mátyás (szerk.): *Studia Iuridica Caroliensia 2.* Budapest, KRE Állam- és Jogtudományi Kar, 2007. 197–215.

⁴ A magyar irodalomban erről lásd Koltay András: *Az új média és a szólásszabadság. A nyilvánosság alkotmányos alapjainak újragondolása.* Budapest, Wolters Kluwer, 2019; Török Bernát: *A szólásszabadság*

A közösségimédia-platformok és a nyilvánosság ökoszisztémájának átalakulása

A közösségimédia-platformok tevékenységének demokratikus hozzáadéka

A közösségimédia-platformok megjelenése és széles körű elterjedése kezdetben azzal a felfokozott várakozással kapcsolódott össze, hogy a minden korábbinál szélesebb körben hozzáférhető (korlátlan) infrastruktúrának köszönhetően elhozza a véleménynyilvánítás szabadságának aranykorát, hiszen a korábbi szűkös infrastruktúrákhoz való korlátozott hozzáférés helyett a közvetlen hozzáférés révén bárki szabadon és azonos eséllyel oszthatja meg gondolatait, véleményét másokkal, és vehet részt a szélesre tárt, minden álláspontot becsatornázni képes közvitában. A közvetlen hozzáférés lehetőségének megvalósulása mint demokratikus hozzáadék (az egyéni véleménynyilvánítás és a demokratikus diskurzusok pluralizálódása révén) kétségtől olyan pozitív technológiai következményként értékelendő, amely az új platformnyilvánosság-tér megőrzendő értékei közé tartozik.

A tartalom és a szolgáltatók viszonya – passzív vagy aktív szereplők?

A közösségimédia-platformok tevékenységével kapcsolatban használt narratívák a platformnyilvánosság kapuőreit többnyire az információáramlás passzív szereplőiként azonosították, olyanokként, akik nem alakítói a közbeszédnek, csupán az online nyilvánosságban kialakuló diskurzusok elengedhetetlen technológiai hátterét biztosítják, de nem befolyásolják annak összetételét, struktúráját, az egyes vélemények, álláspontok, tartalmak láthatóságát. A kezdeti narratívák tehát olyan passzív szereplőként tekintettek a közösségimédia-platformokra, amelyeknek a tevékenysége nincs hatással a felhasználók szólásszabadságára és tájékozódáshoz való jogára. A platformszolgáltatók a valóságban azonban csakhamar aktív tartalommenedzselési szerepet vállaltak, amelynek során egyes (jogellenes) tartalmak hozzáférhetőségét megszüntették (törölték), láthatóságát mérsékeltek, a tartalmakat különböző szempontok alapján rangsorolták, és az egyes felhasználók (vélelmezett) igényeihez igazították (személyre szabták).

A közösségimédia-platformoktól – bár tartalommenedzselési tevékenységük kezdetben dominánsan a magánérintkezésekre irányult – soha nem állt távol a szabad véleménynyilvánítás jogának legvédelettebb központi magját képező politikai, közéleti

a közösségi platformokon és a Digital Services Act. In Török Bernát – Zódi Zsolt (szerk.): *Az internetes platformok kora*. Budapest, Ludovika Egyetemi Kiadó, 2022. 195–207; Papp János Tamás: *A közösségi média szabályozása a demokratikus nyilvánosság védelmében*. Budapest, Wolters Kluwer, 2022; Gosztönyi Gergely: *Cenzúra Arisztoteléstől a Facebookig. A közösségi média tartalomszabályozási gyakorlatának komplexitása*. Budapest, Gondolat Kiadó, 2022; Klein Tamás: *Sajtószabadság és demokrácia*. Budapest, Gondolat – Dialóg Campus, 2020.

diskurzust érintő tartalommenedzselés, akár a politikai diskurzusokban megfogalmazott tartalmak elérésének korlátozása, megszüntetése (moderálás), akár láthatóságának csökkentése révén. Az elmúlt néhány évben azonban talán nem túlzás azt állítani, hogy a demokratikus diskurzusokban való aktív szerepvállalásuk oly mértékben fokozódott, ami a tudományos közösség mellett a közvélemény figyelmét is ráirányította a közösségimédia-platfórmok hatalmára. Gondoljunk bármit is Donald Trump politikusi, elnöki teljesítményéről, vagy éppen a 2020-as elnökválasztás utáni megszólalásairól, különösen a Capitolium ostromában játszott szerepéről, a volt amerikai elnökről alkotott szubjektív véleményünk független attól a ténytől, hogy Trump kitiltása az egyes közösségimédia-platfórmokról történeti és alkotmányossági jelentőségű fejlemény volt,⁵ olyan, amely ismételten ráirányította a figyelmet a kivételesen robusztus cselekvési szabadságot biztosító hatalommal rendelkező szolgáltatók alkotmányos elvek, jogok alá rendelésének – haladékot nem engedő – szükségességére. A konkrét példával összefüggésben felmerülő elvi kérdés mindazonáltal nem az, hogy vajon Trump (időleges vagy „örök időkre” szóló végleges) kitiltása⁶ az első alkotmánykiegészítés betűjével és szellemével összhangban történt-e, hanem az, hogy az ilyen döntés mögött azonosíthatók-e ezek az alkotmányos követelmények, és ha igen, azok miként érvényesülnek? Másként megfogalmazva a közösségimédia-platfórmok demokratikus diskurzusokban betöltött aktív szerepét és annak a véleményszabadság hagyományos tartalmára gyakorolt hatását érzékelve azt kell eldönteni, hogy feladjuk az évszázados alkotmányos hagyományban gyökerező alapjogi tartalmat és védelmi szintet, vagy a közösségimédia-platfórmokat terheljük meg olyan alkotmányos kötelezettségekkel, amelyek tevékenységük megváltoztatására kényszerítik a szolgáltatókat, és garantálják a véleménynyilvánítás szabadságából fakadó klasszikus alkotmányos követelményeknek esetükben is megvalósuló érvényesülését.⁷ A közösségimédia-platfórmok tehát érzékelhetően az egyszerű postás, könyvtáros passzív pozíciójából a közbeszéd aktív alakítóivá, mi több mindenható bíráivá váltak, oly módon, hogy az alapjogok védelmét szolgáló közjogi garanciák tevékenységekre nem vonatkoztak.

⁵ Vö. Szikora Tamás: A platformszabályozás egy új iránya Donald Trump Facebookról való kitiltásának példáján keresztül. In Török Bernát – Zódi Zsolt (szerk.): *Az internetes platformok kora*. Budapest, Ludovika Egyetemi Kiadó, 2022. 209–226.

⁶ Azóta a Twitter, amely a volt elnök kedvenc közösségimédia-platfórmja volt, nem függetlenül a szolgáltató tulajdonosváltásától, bejelentette az „örök időkre” kitiltott Trump visszaengedését a platformra. Ennek ellenére a kézirat lezárásakor a legfrissebb bejegyzés a @realDonaldTrump oldalon 2021. január 8-i, és Trump „foglalkozásaként” az szerepel, hogy az USA 45. elnöke. Úgy tűnik tehát, hogy a volt elnök nem siet vissza a platformra, inkább saját Truth Social nevű oldalán osztja meg gondolatait.

⁷ Vö. Török (2022): i. m. 200.

A szemünk előtt kibontakozó új nyilvánosság-ökoszisztéma jelenségei a társadalmi nyilvánosság működésére olyan jelentőségű felforgató hatást gyakoroltak, amely válaszok adására késztette mind a jogtudományt, mind a jogalkotást és a jogalkalmazást. Az alapvető dilemma adott. A fentebb már körvonalazott szabályozási utak két irányba vezethetnek. Az egyik szabályozási koncepció szerint a közösségimédia-platformok okozta új, az egyéni szólásszabadságra és a demokratikus társadalmi nyilvánosságra veszélyt hordozó jelenségek felforgató hatásától tartva újra kell gondolni az anyajog, valamint a szólás- és sajtószabadság hagyományos tartalmát, és azokat hozzá kell igazítani az új technológiai követelményekhez, akár a korábbi széles körű szabadság és fokozott alapjogi védelem szűkítése árán is. Ezzel szemben sokan – így e sorok szerzője is – amellett érvelnek, hogy az új kihívások ellenére sem szabad feladni a szabadságjogok egyszer már elért védelmi szintjét, az alapjogi vívmányokat, nem a gyereket kell kiönteni a fürdővízzel, hanem a már létező alkotmányjogi keretek megőrzése mellett kell adekvát szabályozási megoldásokat találni. Nézetem szerint a – később röviden bemutatott – Digital Services Act (DSA) elfogadásával az európai jogalkotó éppen erre a szabályozási útra talált rá.

A demokratikus hozadék árnyékos oldala?

Bármennyire is üdvözlendő az újmédia – fentebb jelzett – demokratikus hozadéka, önmagában a sokak megszólalásának lehetősége is aggodalomra adhat okot, különösen akkor, ha a kapuőrök nem megfelelően látják el a tevékenységüket, és az általuk nyújtott szolgáltatás szabályozatlansága és a tartalmak moderálatlansága miatt a jogellenesség táptalajává válnának, sértve a demokratikus társadalom szövetét és az egyének alapjogait. Ugyanakkor álláspontom szerint ebben az esetben is az egyensúlyi állapot megtalálása lehet az üdvözítő szabályozási cél, amelyben a platformszolgáltatókat olyan közérdekű kötelezettségekkel kell terhelni, amelyek képesek biztosítani az egyének alapjogainak védelmét és a nyílt, szabad és szélesre tárt demokratikus közvita érvényesülését. Másként megfogalmazva, Török Bernáttal egyetértve azt is mondhatnánk, hogy „bármilyen legyen a véleményünk sokak megszólalásának lehetőségéről és ennek kockázatairól, ameddig a szabad vélemény nyilvánításra mint a demokrácia legfontosabb legitimációs és részvételi alapjára tekintünk, addig nem zúzhatjuk szét ezt a lehetőséget, hanem jó gyakorlatainak kialakításán kell fáradoznunk”.⁸ A jó gyakorlatok kialakításának, a piaci érdekek és az alapjogok összebékítésének egy ígéretes eszköze lehet az Európai Unió digitális

⁸ Török (2022): i. m. 197.

szolgáltatásokról szóló rendelete,⁹ amelynek végleges szövege 2022. október 19-én jelent meg az Európai Unió Hivatalos Lapjában.¹⁰

Az európai szabályozás a Digital Services Actig

Mielőtt rátérnék a napjainkban igencsak kurrens új szabályozás, a DSA alapjogi mechanizmusának rövid bemutatására, szükségesnek látszik felvillantani azt a két évtizedes szabályozási időszakot, amely az európai harmonizációs szabályozás 2000-ben megalkotott újszerű megoldásaitól a szabályozás inadekvitásáig és fragmentálódásáig vezetett.

Az újmédia legjelentősebb szereplői, a közösségimédia-platformok napjainkig, a hatályos európai harmonizációs joganyag szerint alapvetően az internetes közvetítő szolgáltatók, azon belül a tárhelyszolgáltatók kategóriájába tartoznak, amelyek tevékenységére csupán néhány kötelezettséget előíró szabály vonatkozik. Az európai jogalkotó a tárhelyszolgáltatók szabályozása körében abból indult ki, hogy ezek a jó szándékú, önzetlen, az egyének és a társadalom érdekeit szem előtt tartó szolgáltatók nem alakítói az online nyilvánosság összetételének, csupán a korlátlan infrastruktúra passzív fenntartói, az interperszonális és társadalmi diskurzus mennyiségi és minőségi bővülésének elősegítői. Erre utalnak a jogalkotók által is használt korabeli – és már korábban említett – metaforák, amelyek passzív szereplőként látatják a közvetítő szolgáltatókat, köztük a közösségimédia-platformokat (vö. postás, könyvtár metaforával). Ebből fakadóan az európai harmonizációs szabályokat bevezető irányelv¹¹ vonatkozó rendelkezései az online platformokkal szemben csak igen kevés és szűk körű közérdekű kötelezettséget állapítottak meg, a tartalomért való felelősségüket pedig limitálták.

Az elektronikus kereskedelemről szóló irányelv és válsága

Az európai jogalkotás több mint húsz éve helyesen érezte meg az online nyilvánosság technológiavezérelt átalakulásának jelentőségét, az információs társadalom sajátosságaiból fakadó szabályozási igényt. Az elektronikus kereskedelemről szóló 2000/31/EK irányelv (a továbbiakban: Eker. irányelv), a vonatkozó tagállami

⁹ Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (2022. október 19.) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (digitális szolgáltatásokról szóló rendelet). L 277/1 (2022. október 27.).

¹⁰ Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (2022. október 19.) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (digitális szolgáltatásokról szóló rendelet). L 277/1 (2022. október 27.).

¹¹ Lásd a következő pontban.

szabályozásokat harmonizáló európai jogharmonizációs keret az újszerű szolgáltatások okozta kihívásokra elfogadásakor kifejezetten előremutató és felelős válaszokat adott. Az Eker. irányelv leglényegesebb vonatkozó rendelkezései az általános nyomkövetési kötelezettség hiánya és a harmadik személyek jogellenes tartalmaiért viselt limitált felelősség, illetve a felelősség alóli mentesülést biztosító notice and take down eljárás. A szolgáltatók tartalmakhoz való passzív viszonyának szabályozására ezek a rendelkezések megfeleltek, ugyanakkor az értesítési és eltávolítási eljárás, bár általánosságban szintén helyeselhető szabályozási megoldás volt, önmagában is számos alkotmányossági problémát generált.¹² Az online platformok kímélete a súlyosabb kötelezettségektől nagyrészt azon a várakozáson is alapult, hogy ez a szabályozási hozzáállás járulhat hozzá eredményesen az innovációhoz, a demokratikus hozadék szolgáltatóktól remélt kiteljesedéséhez. A valóságban azonban ezek a szolgáltatók nem a sokszávos autópálya üzemeltetőihez hasonlítottak, akik – az infrastruktúra minőségét karbantartva, a közlekedés biztonságára veszélyt jelentő helyzeteket orvosolva – a biztonságos közlekedés feltételeit biztosítják a sebességhatár-mentes szupersztrádán, sokkal inkább olyan tevékenységet végeztek, amely a forgalom irányát, dinamikáját, a közlekedés szabályait meghatározó, a szabályszegőket szankcionáló, egyes közlekedőket akár a forgalomból kitiltó közlekedésrendészeti szerv jellegzetességeit mutatta.

A fenti példa is jól mutatja, hogy két évtized alatt a technológiai változások szélesebben erodálták az irányelv adekvátságát, hiszen az információs társadalommal összefüggő szolgáltatások 2000-ben történt szabályozását követően olyan „új és innovatív (digitális) szolgáltatások jelentek meg, amelyek nagymértékben megváltoztatják az uniós polgárok mindennapi életét, befolyásolva és átalakítva a kommunikáció és kapcsolattartás, a fogyasztás és az üzletkötés módját. Ezek a szolgáltatások nagymértékben hozzájárultak az uniós és globális társadalmi és gazdasági átalakuláshoz.”¹³ A technológiavezérelt társadalmi, gazdasági változások, bár kétségtől számos előnnyel jártak, a piaci szabadság és az alapjogok, különösen a nyilvánosság szélesedésével az egyéni önkifejezés szabadsága (véleménynyilvánítás szabadsága) tekintetében, az új nyilvánosságszcénák sajátos működési modellje miatt új kockázatok és kihívásokat is kitermeltek a társadalom és az egyén vonatkozásában egyaránt, a piaci verseny, a fogyasztói jogok mellett nem utolsósorban az egyéni szabadság

¹² Az értesítési-eltávolítási eljárás mentesülési szabálya kifejezetten abban tette érdekeltté a szolgáltatókat, hogy az értesítéssel érintett, jogellenesnek jelentett tartalmakat érdemi vizsgálat nélkül törölje, hiszen ezzel biztosíthatta, hogy a jogellenesség megállapítása esetén mentesül a felelősség alól. Ez a mechanizmus szemernyt sem vette figyelembe az eltávolított tartalom közzevetőjének alapjogait, különös tekintettel a szólásszabadság jogára, hiszen az alapjogsérelmet szenvedett személyek jogvédelméről nem gondoskodott.

¹³ Európai Bizottság: *Javaslat. Az Európai Parlament és a Tanács rendelete a digitális szolgáltatások egységes piacáról (digitális szolgáltatásokról szóló jogszabály) és a 2000/31/EK irányelv módosításáról*. COM(2020)825 végleges (2020. december 15.). (Digitális szolgáltatásokról szóló rendelettervezet, Digital Services Act, röviden: DSA) Indokolás 1.

kiteljesedésének potenciális korlátozásával. A kilencvenes években megfogalmazott elveken nyugvó, 2000-ben elfogadott szabályozás és a társadalmi valóság azonban egy évtized múltával oly mértékben eltávolodtak egymástól, hogy – Zódi Zsolt erőteljes, ám a helyzetet hűen leíró kifejezését kölcsönözve – a vonatkozó joganyag válságba került,¹⁴ a korábbi technológiai megoldásokra szabott szabályozási fogalmak és eszközök, valamint a valóság között tátongó szakadékot a jogalkalmazás sem tudta áthidalni.

A harmonizált joganyag fragmentálódása

A platformnyilvánosságban tapasztalható rendkívüli változások, a szolgáltatók tevékenységének mennyiségi és minőségi átalakulása, különösen a tartalmakhoz való viszonyuk radikális megváltozása a közös európai szabályozás gyors avulását eredményezték. A technológiai alapú, de az európai polgárok alapjogait is érintő kihívásokat az EU bár igen hamar érzékelte, a gyors, hatékony és adekvát válaszok megadásával hosszú ideig adós maradt. A közös európai szabályozási folyamat lassúsága és a platformok növekvő hatalma több tagállamot arra bátorított, hogy az online platformok által generált kihívásokra saját, egyedi válaszokat adjanak. Az úttörőnek számító, 2018. január 1-jén hatályba lépett német törvény (NetzDG)¹⁵ után több tagállam is olyan szabályokat alkotott, amelyek a közösségimédia-platformok működésének egyes vonatkozásait szabályozták. A NetzDG után megszületett a francia,¹⁶ az osztrák¹⁷ platformokat érintő szabályozás is. A tagállami szabályozások sok tekintetben hasonlóak (voltak) egymáshoz, abban mindenképpen, hogy nemzeti keretek között próbáltak választ találni az ilyen keretrendszerben nehezen értelmezhető, globális jelenségekre. A tagállami szabályozások mellett, hogy az online platformszolgáltatások globális jellegére tekintettel csupán korlátozottan lehettek eredményesek, az európai belső piacon olyan szabályozási fragmentációt okoztak, amelyet már nem tudtak egyben tartani a harmonizációs célú jogalkotás eredményei, különösen az Eker. irányelv egykor haladó rendelkezései.

¹⁴ Zódi Zsolt: *Platformjog*. Budapest, Ludovika Egyetemi Kiadó, 2023. 71.

¹⁵ Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG).

¹⁶ LOI no 2020-766 du 24 juin 2020 visant à lutter, contre les contenus haineux sur internet.

¹⁷ Bundesgesetz über Maßnahmen zum Schutz der Nutzer auf Kommunikationsplattformen (Kommunikationsplattformen-Gesetz – KoPl-G).

Az audiovizuális médiaszolgáltatásokról szóló irányelv módosítása, mint az első fecske

Az audiovizuális médiaszolgáltatásokról szóló 2010/13/EU irányelv¹⁸ (a továbbiakban: AVMS irányelv) 2018/1808 irányelvvel¹⁹ történő, 2018-as módosítása (a továbbiakban: AVMSM) az online nyilvánosság egy meghatározó jelentőségű szolgáltatástípusának tagállamokban harmonizált szabályozását tűzte ki célul. Az AVMSM nagy újdonsága volt, hogy az irányelv tárgyi hatályát, amely korábban kizárólag az audiovizuális médiaszolgáltatásokra vonatkozott, kiterjesztette a videómegosztó platformokra is, azzal, hogy nem minősülnek klasszikus értelemben vett médiaszolgáltatóknak. A videómegosztóplatform-szolgáltatást az AVMSM irányelv ugyan változatlanul a tárhelyszolgáltatók körében helyezte el, ám kötelezettség szabásuk mértékének meghatározása során tekintettel volt arra, hogy az információáramlás online kapuőreiként sokkal jelentősebb hatást gyakorolnak a tartalomszolgáltatás dinamikájára és a fogyasztók valóságérzékelésére, mint az egyszerű tárhelyszolgáltatók, hiszen tevékenységük sajátos, a tartalmak szabad áramlását befolyásoló forgalomirányításként jellemezhető, vagyis nem pusztán a technikai feltételeket biztosító passzív résztvevői a nyilvánosságnak, hanem aktív információmenedzselési szerepet vállalnak. A videómegosztóplatform-szolgáltatások irányelvi fogalma sajátos módon nem csupán a klasszikus videómegosztókat vonta az AVMS hatálya alá, hiszen a szolgáltatás akkor is videómegosztó szolgáltatásnak minősül, ha a videómegosztási funkció a szolgáltatásnak csupán egy eleme, amely a főtevékenységtől elválasztható, vagy ha nem különválasztható eleme a teljes szolgáltatásnak, de olyan alapvető funkcióval rendelkezik, amely a teljes szolgáltatás vonatkozásában meghatározó jelentőségű. Ebből fakadóan a közösségimédia-platformok is videómegosztóplatform-szolgáltatásnak minősülnek a felhasználók által közzétett audiovizuális tartalmak tekintetében, függetlenül attól, hogy a platformnak egyébként nincs kifejezetten az audiovizuális tartalmak megosztására fenntartott részszerkeztetése, hanem az csupán a főszolgáltatás részeként jelenik meg.

Az AVMSM bár jó irányba mutató szabályozási lépésként értékelhető, csupán a platformszolgáltatások egy speciális típusára állapított meg kötelezettséget.

¹⁸ Az Európai Parlament és a Tanács 2010/13/EU irányelve (2010. március 10.) a tagállamok audiovizuális médiaszolgáltatások nyújtására vonatkozó egyes törvényi, rendeleti vagy közigazgatási rendelkezéseinek összehangolásáról (Audiovizuális médiaszolgáltatásokról szóló irányelv). L 95/1 (2010. április 15.). 1–24.

¹⁹ Az Európai Parlament és a Tanács (EU) 2018/1808 irányelve (2018. november 14.) a tagállamok audiovizuális médiaszolgáltatások nyújtására vonatkozó egyes törvényi, rendeleti vagy közigazgatási rendelkezéseinek összehangolásáról szóló 2010/13/EU irányelvnek (Audiovizuális médiaszolgáltatásokról szóló irányelv) a változó piaci körülményekre tekintettel való módosításáról. L 303/69 (2018. november 28.). 69–92.

Az alapjogok horizontális hatályú védelmének elméleti lehetőségei

A horizontális hatályú alapjogvédelem elméleti igényű, dogmatikai elemzésére jelen tanulmány keretei között nem vállalkozhatok, ugyanakkor a későbbiekben bemutatott konkrét szabályozás hatásainak elemzéséhez röviden szükséges kitérni legalább annak alapvonalaira. Amint arra a bevezető gondolatokban már utaltam, az alapjogok védelmét történetileg a közhatalmat birtokló állammal mint a (történelmi) tapasztalat szerint az egyén szabadságát elnyomni képes hatalommal szemben fogalmazták meg az első kartális alkotmányok alapjogi katalógusaiban. Amennyiben az alapjogok esztörténeti előzményeit felelevenítjük, szintén a közhatalom és az egyén viszonyrendszere tárul elénk, hol az isteni jog, vagy éppen a (társadalmi) szerződés korlátozza a közhatalmat az egyén jogainak, szabadságának védelme érdekében. Az alkotmánytörténet híres jognyilatkozatai különböző terjedelemben és hatókörben szintén az állam hatalmát voltak hivatottak korlátozni. Az alapjogok védelme az alkotmánytörténet bő két évszázada során szinte kizárólag vertikális hatályú volt, az egyén és az állam közjogi, vertikális viszonyában volt értelmezhető, az egyén jogait deklarálta és látta el alkotmányos garanciákkal az állammal mint az egyénre nézve közjogi túlhatalommal rendelkező potenciális jogsértővel szemben. A vertikális hatályú alapjogvédelem tehát az alapjogok történetileg kialakult, klasszikus hatalomkorlátozó funkciójából következik, hiszen a liberális alkotmányok egyik legfőbb rendeltetése az egyén jogainak védelme a közhatalmat birtokló állammal szemben. Egyáltalán nem (volt) evidens tehát, hogy ezek a jogok kiterjeszthetők a magánosok egymás közötti, a kölcsönös egyenlőség elvén nyugvó, horizontális magánjogi jogviszonyaira.

Az elmúlt évtizedekben azonban egyre világosabb igény rajzolódott ki a társadalmakban, és vált elfogadottá az alkotmányjog-tudományban is, hogy az alapjogok nem csupán az egyén és a közhatalommal rendelkező állam vertikális, közjogi jogviszonyában értelmezhetők, hanem magánjogi jogviszonyokban horizontálisan is érvényesülniük kell. Az alapjogok horizontális hatályú érvényesülésének széles körű elismerése ugyanakkor az egyre intenzívebb tudományos diskurzus ellenére²⁰ is megosztó tudományos kérdés maradt. Bár az alkotmánybíróságok²¹ is egyre szélesebb körben ismerik el az alapjogok védelmét a magánjogi jogviszonyokban, a horizontális hatályú alapjogvédelem dogmatikai alapjai, az egyes alapjogok esetében

²⁰ A magyar irodalomból lásd Gárdos-Orosz Fruzsina: Alapjogok alkalmazása a magánjogi jogvitákban az Európai Unióban és ennek lehetséges hatásai a magyar jogra. *Állam- és Jogtudomány*, 51. (2010a), 3. 225–258; Gárdos-Orosz Fruzsina: Az alkotmányjog a magánjogi jogviszonyokban. *Rendészeti Szemle*, 58. (2010b), 4. 19–35; Bedő Renáta: Az alapjogok érvényesülése magánviszonyokban Magyarországon – fókuszban a fórumrendszer. *Fundamentum*, 22. (2018), 1. 58–69; Gárdos-Orosz Fruzsina – Bedő Renáta: Az alapvető jogok érvényesítése a magánjogi jogviták során – az újabb alkotmányjogi gyakorlat (2014–2018). *Alkotmánybírósági Szemle*, (2018), 1. 3–15.

²¹ A magyar Alkotmánybíróság gyakorlatából elsőként említhető: 8/2014. (III. 20.) AB határozat, ABH 2014. 174.

érvényesülő mércéi közel sem olyan kidolgozottak, mint az egyén és az állam viszonyrendszerében érvényesülő vertikális hatályú alapjogvédelem évszázados alkotmányos követelményrendszere.

Az a szabályozási megoldás, hogy egy alapjog nem csupán az államot, hanem a magánfeleket is kötelezi, ugyanakkor nem lehet automatizmus, minden esetben alkotmányos igazolásra szorul. Ilyen alkotmányos igazolás lehet, hogy a magánjogi jogalany olyan erősen kötődik a közhatalomhoz, hogy cselekvése az állam cselekvéseként értelmezhető. Ennek példaként említhető az USA Legfelsőbb Bírósága által kidolgozott állami cselekvés tana (*state action doctrine*), ez alapján az alkotmány csak akkor alkalmazható közvetlenül, ha megállapítható, hogy az alapjogi jogszerelem bekövetkezése állami szervnek tulajdonítható, vagy magánszemély állami kötelezettségének teljesítésére vezethető vissza. Európában széles körben elfogadott felfogás a közvetett horizontális hatály tana. Ennek értelmében az alapjogi normák egy objektív alkotmányos értékrendet is kirajzolnak, amelynek a jogrendszer egészét át kell hatnia, annak a jogrendszer egészében érvényesülnie kell. Ezt az alkotmányos értékrendet elsősorban a jogági kódexekben megfogalmazott generálklauzulák hivatottak képviselni. Az alkotmányos megalapozottságú generálklauzulákat a bíróságoknak ítélezésük során figyelembe kell venniük, és a jogszabályi rendelkezéseket az alkotmányos normákban megfogalmazott (alapjogi) értékrenddel összehangban kell értelmezniük. A közvetett horizontális hatály elmélete mellett ismert az alapjogvédelem magánjogviszonyokban való közvetlen érvényesülésének felfogása is, ám annak elfogadottsága ma még az irodalomban is csupán kivételes álláspontnak minősül. Ugyanakkor sajátosságaikra tekintettel ma is vannak olyan alapjogok, amelyek esetében közvetlenül érvényesül az alapjogvédelem a magánjogi jogviszonyokban. E körben említhető az egyenlő bánásmódhoz való jog, illetve legújabban az európai adatvédelmi rendszerben – a GDPR rendelkezései révén – a személyes adatok védelméhez való jog.

A horizontális hatályú alapjogvédelemnek amellet, hogy vannak alkotmányosági standardjai, érvényesülése jelentékeny mértékben azon múlik, hogy a rendes bíróságok jogalkalmazói tevékenységük során mennyire hajlandóak vagy képesek az egyes ügyekben érvényesíteni.

A rendes bíróságok alapjogi bíráskodását, vagy mértékletesebben fogalmazva, az alapjogok védelmére figyelmet fordító igazságszolgáltatási gyakorlatának alkotmányos alapját hazánkban az Alaptörvény 28. cikke határozza meg, amely szerint „[a] bíróságok a jogalkalmazás során a jogszabályok szövegét elsősorban azok céljával és az Alaptörvénnyel összhangban értelmezik”.²² A magyar Alkotmánybíróság is egyértelműen elfogadja a közvetett hatály érvényesülését: „Az a vita, hogy az alapjogok [...] a magánjogra hatással vannak-e, ma már csak arról folyik, hogyan van hatással az alkotmány-törvény a magánjogi viszonyokra. Vagyis a behatás módszerei és intenzitása a vita tárgya. A közvetett hatály tana értelmében

²² Magyarország Alaptörvényének 28. cikke.

az alkotmány-törvény érvényesülésével együtt a polgári jogviszonyok azonban továbbra is polgáriak maradnak. Az Alaptörvényben foglalt jogok a magánjog generálklauzuláin keresztül képesek beszűrődni a magánjog rendszerébe.”²³

A digitális szolgáltatásokról szóló rendelettervezet alapjogi elköteleződése és a horizontális hatály érvényesítésének esélye

Az Európai Unió új digitális jogszabálysomagja bár több rendelet(tervezet)ből áll,²⁴ az alapjogok és különösen a véleménynyilvánítás szabadsága horizontális hatályú védelmével összefüggésben a digitális szolgáltatások egységes piacáról szóló rendelet (*Digital Services Act*, a továbbiakban: DSA vagy Rendelet] kiemelkedő jelentőségű. A tanulmány vizsgálati fókuszára tekintettel a továbbiakban kizárólag a DSA vonatkozó rendelkezéseivel és az azokból levezethető általános következtetésekkel foglalkozom.

A DSA tervezetét 2020 decemberében mutatta be az Európai Bizottság, és nem egészen két év múlva, 2022. október 19-én kihirdették. Rendelkezéseit főszabályként 2024. február 17-től kell alkalmazni, de egyes, a platformokra és óriásplatformokra vonatkozó szabályait már 2022. november 16-tól érvényesíteni kell. A DSA ugyan az Eker. irányelv egyes rendelkezéseit hatályon kívül helyezi és újraszabályozza,²⁵ az irányelvet teljes egészében nem helyezi hatályon kívül, éppen ellenkezőleg, épít annak megoldásaira, és nem érinti az ÁVMSM vívmányait sem.²⁶

A DSA alapjogi szemlélete – európai nézőpont

A Rendelet számos ponton hivatkozik az Európai Unió Alapjogi Chartájára és az abban foglalt alapvető jogokra, még hozzá nem csupán formális módon, így egy sajátos, új alapjogvédelmi mechanizmus normatív alapjait fekteti le. Bár minőségi következtetésekre közel sem alkalmas mennyiségi mutató, de mégiscsak jelzi a DSA alapjogi elkötelezettségét, hogy az „alapvető jog” kifejezés mindösszesen 43 alkalommal szerepel a textusban.²⁷ Az üdvözlendő deklaráción túl azonban a valódi

²³ 8/2014. (III. 20.) AB határozat, ABH 2014. 174. 185.

²⁴ DSA (digitális szolgáltatásokról szóló rendelet), DMA (digitális piacokról szóló rendelet), MFA (az európai tömegtájékoztatás szabadságáról szóló rendelet).

²⁵ Az Eker. irányelv 12–15. cikkeit a DSA 4–6. és 8. cikkei tartalmazzák.

²⁶ Bár e tanulmány szűken vett tárgyának nem része, de azt érdemes jelezni, hogy az egyes jogszabályok egyes rendelkezései nem minden ponton látszanak harmonizáltnak, ami a későbbi jogalkalmazás során még nehézségeket okozhat.

²⁷ Az Eker. irányelvben az alapvető jog kifejezés nem szerepelt, csupán a (9) preambulumbekfezdés hivatkozik a véleménynyilvánítás szabadságára: „Az információs társadalommal összefüggő szolgáltatások szabad mozgása sok esetben egy általánosabb elv egyedi megnyilvánulása lehet a közösségi

kérdés az, hogy a platformszolgáltatók és a szolgáltatásukat igénybe vevő felhasználók magánjogi jogviszonyait szabályozó Rendelet alapjogvédelmi mechanizmusa miként érvényesül majd a gyakorlatban, hiszen a platformszolgáltatókkal szemben megfogalmazott alapjogi követelmények gyakorlati érvényesülése számos, ma még pontosan nem prognosztizálható körülménytől függ. Teljesen egységes gyakorlat várhatóan csak az EU-s intézmények részéről valósulhat meg, amelyet erőteljes ecsetvonásokkal fog színeezni a tagállami bíróságok (és alkotmánybíróságok) várhatóan széttartó gyakorlata.

A digitális szolgáltatásokról szóló rendelet az online platformok szabályozási kihívásait tehát félre nem érthető nyíltsággal alapjogi kérdésként kezeli, a szabályozás megközelítése a belső piaci szabályozás legfontosabb céljaként is az alapjogok védelmére hivatkozik: a „rendelet célja, hogy hozzájáruljon a közvetítő szolgáltatások belső piacának megfelelő működéséhez, az olyan biztonságos, kiszámítható és megbízható online környezetre vonatkozó harmonizált szabályok meghatározásával, amely elősegíti az innovációt, és amelyben a Chartában rögzített alapvető jogok [...] hatékony védelmet élveznek”.²⁸ A DSA – a címében is megjelenő piaci működés szabályozása mellett – hangsúlyosan veszi figyelembe a Chartában foglalt alapvető jogok védelmét. Az alábbiakban röviden azt szeretném bemutatni, hogy ezek az alapjogi hivatkozások merőben nem csupán formálisak, hanem nagyon is valóságosak, mögöttük kellően kidolgozott jogvédelmi mechanizmus és az érvényesülésüket szolgáló garanciarendszer áll.

Az általános alapjogi hivatkozások konkretizálásaként a DSA néhány alapjogot külön is nevesít: „A közvetítő szolgáltatók felelősségteljes és kellően gondos magatartása elengedhetetlen [...] ahhoz, hogy az uniós polgárok és más személyek gyakorolhassák az Európai Unió Alapjogi Chartájában (a továbbiakban: Charta) biztosított alapvető jogokat, különösen a véleménynyilvánítás és a tájékozódás szabadságát, a vállalkozás szabadságát, a megkülönböztetésmentességhez való jogot és a fogyasztóvédelem magas szintjének elérését.”²⁹ Azzal, hogy a szabályozás mely alapjogokat emelte ki, a jogalkotó nyilvánvalóvá tette, hogy a platformgazdaság kulcsszereplői, a közvetítő szolgáltatók, különösen pedig az online platform- és óriásplatform-szolgáltatók működése meghatározó jelentőségű a demokratikus diskurzusok szabad alakulása és védelme szempontjából. Az óriásplatformok tekintetében pedig ennél is határozottabban fogalmaz az (56) preambulumbekkezdés,

jogban, nevezetesen a véleménynyilvánítás szabadságáé, amelyről a minden tagállam által ratifikált, az Emberi jogok és alapvető szabadságok védelméről szóló egyezmény 10. cikkének (1) bekezdése rendelkezik; ezért az információs társadalommal összefüggő szolgáltatások nyújtására vonatkozó irányelveknek biztosítaniuk kell, hogy ez a tevékenység szabadon gyakorolható legyen az említett cikk értelmében, és e tevékenységre csak az említett cikk (2) bekezdésében és a Szerződés 46. cikkének (1) bekezdésében megállapított korlátozások vonatkozhatnak; ennek az irányelvnek nem célja, hogy érintse a véleménynyilvánítás szabadságával kapcsolatos alapvető nemzeti szabályokat és elveket.”

²⁸ DSA 1. cikk (1) bekezdés.

²⁹ DSA (3) preambulumbekkezdés.

elismeri azok jelentékeny befolyásolási potenciálját a közvélemény és a közbeszéd alakulására. Az így kialakuló társadalmi kockázatok enyhítése érdekében olyan szabályozási megoldásokra és jogérvényesítésre van szükség, amely közvetlenül az alapvető jogok védelmére épül.³⁰

A DSA a kiemelt védelemben részesített alapjogok mellett azonosítja az alapvető jogokat fenyegető legjelentősebb – elsősorban az óriásplatformok működésével összefüggő – veszélyeket is, úgymint „a jogellenes tartalmak online terjesztését és azokat a társadalmi kockázatok, amelyeket a dezinformáció vagy más tartalmak terjesztése okozhat [...]”,³¹ ezekkel a veszélyekkel összefüggésben a Rendelet preambulumának ígérete szerint a Chartában rögzített alapvető jogok oly módon részesülnek hatékony védelemben, hogy egyúttal elősegítik a platformokon jelentkező innovációt is.

A DSA többszintű és differenciált szabályozási modellje

A DSA egy többszintű és differenciált szabályozási modellt vezet be, amely annak alapján tipizálja az egyes szolgáltatókat, hogy milyen mértékben befolyásolják a piacot és az alapjogok érvényesülését. A különböző hatással bíró szolgáltatók típusaira különböző mértékű kötelezettségeket és felelősségi mércéket állapít meg. A kötelezettségszabás annál szélesebb körű, minél intenzívebb az adott közvetítőszolgáltató-típus működésének hatása az egyéni jogok érvényesülésére és a demokratikus nyilvánosság alakulására. A közvetítő szolgáltatók típusán belül a DSA megkülönbözteti a tárhelyszolgáltatókat, az online platformokat³² és az óriásplatformokat, valamint a nagyon népszerű online keresőprogramot üzemeltető szolgáltatókat (továbbiakban: óriásplatformok)³³ mint az alapjogok érvényesülésére fokozott befolyással bíró szolgáltatókat. Néhány alapvető szabály valamennyi közvetítő szolgáltatóra egységesen vonatkozik, amelyeknél egyre szigorodóbb rendelkezések vonatkoznak a tárhelyszolgáltatókra, az online platformokra, valamint az óriásplatformokra.

³⁰ DSA (56) preambulumbekkezdés.

³¹ DSA (9) preambulumbekkezdés.

³² „[O]lyan tárhelyszolgáltatás, amely a szolgáltatás igénybe vevőjének kérésére információkat tárol és nyilvánosan terjeszt, kivéve, ha ez a tevékenység egy másik szolgáltatás kisebb vagy kizárólag kiegészítő eleme, vagy a fő szolgáltatás kisebb funkcionálitása, amely objektív és technikai okokból nem használható az említett másik szolgáltatás nélkül, és az ilyen elem vagy funkcionálitás másik szolgáltatásba való integrációja nem a rendelet alkalmazhatóságának elkerülésére szolgál [...]”.

³³ Olyan online platformok és online keresőprogramok, amelyek havonta átlagosan legalább 45 millió, a szolgáltatást aktívan igénybe vevővel rendelkeznek az unióban, és amelyeket online óriásplatformnak vagy nagyon népszerű online keresőprogramoknak minősítettek [vö. DSA 33. cikk (1) bekezdés].

Moderálás és navigálás mint azonosított alapjogi kockázatok

A közösségimédia-platformoknak a nyilvánosság és a közviták összetételére gyakorolt hatásáról fentebb már volt szó. A platformok tartalomszervező tevékenységével összefüggésben a DSA a két legjelentősebb és a felhasználók alapjogait, különösen a véleményszabadságot veszélyeztető jellegzetességeként – nézetem szerint helyesen – a tartalmak moderálását és a forgalom irányítását (tartalomnavigálás) azonosítja.³⁴ A DSA a tartalommoderálás fogalmát kellően tágan határozza meg, beleértve mindazon szolgáltatói tevékenységet, amelyek a tagállami jogba ütköző (jogellenes) vagy a magánjogi jogviszony alapját képező szerződési feltételekkel ellentétes tartalmakra irányulnak, a legenyhébb láthatóságot csökkentő intézkedésektől a legszigorúbb eszközök alkalmazásának biztosításáig.³⁵ A DSA a tartalommoderálási tevékenységet valamennyi platform esetében olyan szabályok közé szorítja, amelyek megfelelő garanciákat nyújtanak a szolgáltatást igénybe vevők alanyi jogainak a védelmére.

Az ajánlórendszerekre³⁶ vonatkozó szabályok az óriásplatformok kockázatértékelési és kockázatsökkentési kötelezettségei körében jelennek meg, hiszen a figyelemnavigálás ezen a szolgáltatói szinten jelent érdemi alapjogi kockázatot. A transzparenciakövetelmények és az alapértelmezett rangsorolási paraméterektől való eltérést biztosító (nem profilozáson alapuló) beállítási alternatíva elérhetővé tétele olyan szabályozási követelmények, amelyek ugyan nem biztosítanak alanyi jogi igényt a felhasználók számára, ugyanakkor a demokratikus közvélemény intézményes védelmét teremtik meg.

³⁴ A DSA az algoritmikus tartalommenedzsmentet ugyan nem tekinti az online platformok fogalmi elemének, ám a tartalommoderálás és navigálás szabályozásának kiemelt jelentőséget tulajdonít, amelyeken keresztül az online platformok viselkedése a jog alá rendelhető. Vö. Török (2022): i. m. 203–206. és Zódi Zsolt: A platform mint elméleti konstrukció és mint narratív keret – A platformfogalom kialakulásának története. In Török Bernát – Zódi Zsolt (szerk.): *Az internetes platformok kora*. Budapest, Ludovika Egyetemi Kiadó, 2022. 35.

³⁵ „Tartalommoderálás”: a közvetítő szolgáltató olyan automatizált vagy nem automatizált tevékenysége, amely különösen a szolgáltatás igénybe vevője által közzétett jogellenes tartalom vagy a közvetítő szolgáltató szerződési feltételeivel összeegyeztethetetlen információ észlelésére, azonosítására és kezelésére szolgál, ideértve az ilyen jogellenes tartalom vagy információ elérhetőségét, láthatóságát és hozzáférhetőségét érintő intézkedéseket, például annak hátrасorolását, a demonetizálását, az ahhoz való hozzáférés megszüntetését vagy annak eltávolítását, vagy a szolgáltatás igénybe vevője általi információközlés lehetőségét érintő intézkedéseket, például a fiókja megszüntetését vagy felfüggesztését.

³⁶ „Ajánlórendszer”: teljes mértékben vagy részben automatizált rendszer, amelyet az online platform arra használ, hogy az online interfészen konkrét információkat javasoljon, vagy ezeket az információkat rangsorolja a szolgáltatás igénybe vevője számára, többek között a szolgáltatás igénybe vevője által indított keresés alapján vagy egyéb módon meghatározva a megjelenített információk relatív sorrendjét vagy elsőbbségét.

Szerződési feltételek, transzparenciakövetelmények és az alapjogi generálklauzula

A valamennyi közvetítő szolgáltatót érintő, az alapvető jogok védelmét szolgáló közös rendelkezések sorában témánk szempontjából kiemelkedő jelentőségű a szerződési feltételekről rendelkező 14. cikk, amely amellett, hogy szigorú transzparenciakövetelményeket és tájékoztatási kötelezettséget³⁷ állapít meg,³⁸ az alapvető jogok védelmének valamennyi közvetítő szolgáltatóra vonatkozó általános generálklauzuláját is a szabályozás részévé teszi. Amint arra fentebb már utaltam, a generálklauzulák az alapjogok (közvetett) horizontális hatályú védelmének hagyományos és széles körben elismert jogalkotástani megoldásai.

A 14. cikk (4) bekezdése rögzíti, hogy a közvetítő szolgáltatók kellő gondossággal, objektíven és arányosan járnak el a szerződési feltételekben meghatározott korlátozások alkalmazása és érvényesítése során, kellően figyelembe véve valamennyi érdekelt fél jogait és jogos érdekeit, beleértve a szolgáltatás igénybe vevőit megillető alapvető jogokat, mint a véleménynyilvánítás szabadságát, a tömegtájékoztatás szabadságát és sokszínűségét, valamint a Chartában foglaltak szerinti más alapvető jogokat és szabadságokat.³⁹ Ez a rendelkezés minden kétséget kizárva helyezi a DSA valamennyi rendelkezését alapjogi kontextusba,⁴⁰ hiszen az alapvető jogok biztosítékainak figyelembevétele nélkül nem értelmezhetők, nem alkalmazhatók.

Az óriásplatformokra vonatkozó fokozott alapjogvédelmi kötelezettség

Az óriásplatformoknak jelentős befolyása van a platformon zajló demokratikus diskurzusokra és az egyéni jogokra: a véleménynyilvánításhoz való jog szubjektív és objektív oldalára, amely „adott esetben erősen befolyásolhatja az online biztonságot, a közvélemény és a közbeszéd alakulását”.⁴¹ Az óriásplatformok platformhatalmának korlátozása és az alkotmányos értékek és jogok védelme érdekében a DSA kockázatmenedzselési kötelezettséget ír elő számukra, amelynek során „értékelniük kell a szolgáltatásaik kialakításából, működéséből és használatából, illetve a szolgáltatások igénybe vevői általi esetleges visszaélésekből származó rendszerszintű kockázatokat, és az alapvető jogokra figyelemmel megfelelő kockázatsökkentési intézkedéseket kell hozniuk”.⁴²

³⁷ Meg kell határozni a szolgáltatás használatával kapcsolatban megállapított korlátozásokat, vagyis a tartalommoderálás részletes szabályait, eljárásrendjét, az alkalmazható intézkedéseket és eszközöket, a belső panaszkezelési rendszer eljárási szabályait.

³⁸ DSA 14. cikk (1) bekezdés.

³⁹ Vö. DSA 14. cikk (4) bekezdés.

⁴⁰ Török (2022): i. m. 204.

⁴¹ DSA (79) preambulumbekkezdés.

⁴² DSA (79) preambulumbekkezdés.

A DSA tehát az óriásplatformok kötelezettségévé teszi egy olyan kockázatértékelési mechanizmus működtetését, amelyben „gondosan azonosítaniuk, elemezniük és értékelniük kell a szolgáltatásaik és a kapcsolódó rendszerek – többek között az algoritmikus rendszerek – kialakításából vagy működéséből vagy a szolgáltatásaik használatából eredő rendszerszintű kockázatokat”.⁴³ A négy általánosan azonosított rendszerszintű kockázattípus között a DSA másodikként jelöli meg az alapvető jogok gyakorlására, érvényesülésére gyakorolt hatást. A Rendelet e körben azonosítja az alapvető jogok legszélesebb körét. A vonatkozó felsorolás nem taxatív ugyan, de érdemes idézni, melyek azok a Chartában védett alapvető jogok, amelyeknek sérelmét különösen prognosztizálja a jogalkotó az óriásplatformok működése során: emberi méltósághoz való jog (Charta 1. cikk), a magán- és a családi élet tiszteletben tartásához való alapvető jog (Charta 7. cikk), a személyes adatok védelméhez való alapvető jog (Charta 8. cikk), a véleménynyilvánítás és a tájékozódás szabadságához való alapvető jog, a tömegtájékoztatás szabadságát és sokszínűségét is beleértve (Charta 11. cikk), valamint a megkülönböztetés tilalmához való alapvető jog (Charta 21. cikk), a gyermekek jogainak védelméhez való alapvető jog és a magas szintű fogyasztóvédelemhez való alapvető jog.

A rendszerszintű kockázatok között szerepel továbbá „a polgári közbeszédre, valamint a választási folyamatokra és a közbiztonságra gyakorolt bármely tényleges vagy várható negatív hatás”.⁴⁴ A közvetlen demokrácia intézményeinek gyakorlásába és a népakarat szabad kialakulásának és kifejezésének folyamatába való beavatkozás veszélye a véleménynyilvánítás szabadságának objektív oldalán, a demokratikus diskurzusok működésével összefüggésben megkerülhetetlen kérdés, hiszen a platformnyilvánosság szélesre tárt hozzáférési infrastruktúrája számos veszélyt hordoz a demokratikus diskurzusokra és azokon keresztül a demokratikus döntéshozatalra. Ezért az óriásplatformok ez irányú kötelezettségekkel való megterhelése – bár nem szorosan e tanulmány tárgya – szintén üdvözlendő fejlemény. Nem hallgatható el ugyanakkor, és kritikaként szükséges hangsúlyozni, hogy az elnagyolt normatív textus bizonyos értelmezési keretben rendkívül leszállítja a szóláskorlátozás mércéjét, amely esetben a nyilvánvaló és közvetlen veszély tényleges fennállása helyett a várható negatív hatás is elégséges (veszély önmagában) korlátozási mérceként alkalmazható.

Az alapvető jogok érvényesülését veszélyeztető, rendszerszinten azonosítható tényezőként az óriásplatformoknak vizsgálniuk kell a figyelemnavigálás során alkalmazott ajánlórendszereiknek és bármely más releváns algoritmusuknak a kialakítását, a tartalommoderálási szabályokat és gyakorlatot, a szolgáltatás igénybevételére vonatkozó szerződési feltételeket és azok érvényesítését, a hirdetések kiválasztását és megjelenítését végző rendszereket, valamint a szolgáltatásuk adatokkal kapcsolatos gyakorlatát. A kockázatértékelések dokumentációját legalább három évig meg

⁴³ DSA 34. cikk (1) bekezdés b) pont.

⁴⁴ DSA 34. cikk (1) bekezdés c) pont.

kell őrizniük, és kérésre közölniük kell az Európai Bizottsággal, illetve a tagállami hatáskörrel rendelkező hatósággal (digitális szolgáltatási koordinátor).⁴⁵ A kockázatértékelés eredményének elemzése alapján az azonosított rendszerszintű kockázatok csökkentése érdekében az óriásplatformoknak „észszerű, arányos és hatékony kockázatsökkentési intézkedéseket kell bevezetniük a[z] [...] egyes rendszerszintű kockázatokra szabva, kiemelt figyelmet fordítva az ilyen intézkedéseknek az alapvető jogokra gyakorolt hatásaira”.⁴⁶

Az óriásplatformokat terhelő kockázatmenedzselési rendelkezések a demokratikus diskurzusok alkotmányos értékének, a platformon megvalósuló plurális közvélemény védelmének sajátos intézményvédelmi eszközeinek tekinthetők.

A DSA alapjogi tesztje

A DSA az alapjogi generálklauzulában és az óriásplatformok kockázatsökkentési intézkedései körében is olyan rendelkezéseket tartalmaz, amelyek a magánfelek közötti alapjogi jogviszonyok alapjogi tesztjeiként értelmezhetők. A közvetítő szolgáltató a szerződési feltételek meghatározása során – gondossági kötelezettsége részeként – csupán objektív és arányos szólásszabadsági korlátozásokat állapíthat meg, ami megfeleltethető egy szükségességi-arányossági mérlegelést alkalmazó alapjogi tesztnek is.⁴⁷

Az óriásplatformoknak a kockázatsökkentési intézkedéseik keretében észszerű, arányos és hatékony megoldásokat kell alkalmazniuk, amelyek kiemelten veszik figyelembe az alapvető jogokra gyakorolt hatásukat. Ez a rendelkezés a generálklauzulával egyezően alapjogkorlátozási tesztként is tekinthető, ahol az észszerűség a szükségességi, az arányosság az arányossági, a hatékonyság pedig az alkalmassági kritériumelemnek feleltethető meg.⁴⁸

Az alapjogi tesztek alkalmazása során érvényesített arányossági mérce tehát az alapjogi mérlegelés lehetőségét teremti meg, ahol a mérleg egyik serpenyőjében a szolgáltatás igénybe vevőjének védelemben részesülő alapvető joga, míg a másokban harmadik személyek alapvető jogai (például jó hírnévhez való jog, magánélet védelméhez fűződő jog stb.), illetve a szolgáltatók sajátos érdekei mérettetnek meg. Az egyes alapvető jogok korlátozhatósága, az egymással ütköző alapvető jogok

⁴⁵ DSA 34. cikk (3) bekezdés.

⁴⁶ DSA 35. cikk (1) bekezdés.

⁴⁷ Ugyanakkor ebben a tekintetben ellenérvként tűri a vitát, hogy ha valóban egy klasszikus arányossági teszt bevezetése volt a jogalkotó szándéka, akkor alkalmazhatta volna annak klasszikus terminológiáját.

⁴⁸ Az előző lábjegyzeti hivatkozáshoz hasonlóan ez az értelmezés is vita tárgyává tehető, különösen az észszerűség kritérium szempontjából, mivel az észszerűség szükségességgként való értelmezése vitatható, hiszen nem vitásan lehetséges olyan eset, amelyben az egyébként akár észszerűnek is tekinthető alapjog-korlátozási szabály nem fogadható el szükségesnek.

kollíziójának feloldása során alkalmazandó mércék kialakítása szintén a jogalkalmazás feladata lesz. E tekintetben pontos prognózist adni nyilvánvalóan nem lehetséges, ám a szolgáltatók sajátos helyzetére és a „platformhatalomnak”⁴⁹ a közhatalomtól különböző természetére is tekintettel kiemelendő – egyetértve Török Bernáttal –, hogy az állam tekintetében alkalmazott mércéket nem lehet automatikusan a magánjogviszonyokban alkalmazni.⁵⁰

A DSA alapjogi mechanizmusának alkalmazási kérdései és korlátai

A fenti rövid elemzésből kitűnik, hogy a DSA megteremtette a platformokon zajló kommunikáció, a szolgáltatás igénybe vevőinek szólásszabadsághoz való jogának horizontális hatályú védelmét. A közösségimédia-platformoknak tehát jogi kötelezettségük keletkezett arra, hogy működésüket a szolgáltatásukat igénybe vevő európai polgárok alapvető jogainak tiszteletben tartásához igazítsák. A DSA alapjogi mechanizmusa ugyanakkor annyit fog érni, amennyit a szolgáltatók abból betartanak, illetve amennyit a hatáskörrel rendelkező szervek betartatnak velük.

Az alanyi jogi igények tekintetében a tagállami bíróságokon lesz a felelősség, hogy egy, a szolgáltató és a szolgáltatást igénybe vevő közötti magánjogi jogvitában miként érvényesíti a DSA alapjogi követelményeit, illetve érvényesíti-e egyáltalán. Ebben a kérdésben vélhetően széttartó gyakorlat lesz megfigyelhető az egyes tagállamok között. Az alapjogi megalapozottságú alanyi jogi igények elbírálása tekintetében a tagállami bíróságok gyakorlata – a saját szerepfelfogásuk, hatáskör-értelmezésük mentén – a DSA alapjogvédelmi mechanizmusának szigorú számonkérésétől a figyelmen kívül hagyásáig terjedhet. A tagállami bíróságok joggyakorlatában tapasztalható különbségeket várhatóan leginkább az az alkotmányelméleti felfogásbéli különbség határozza majd meg, miként viszonyulnak a nemzeti alkotmányok a horizontális hatályú alapjogvédelemhez, és annak végső intézményi garanciáit milyen hatásköri szabályokkal támasztják alá.

A horizontális hatályú alapjogvédelemnek szélesebb körű érvényesítése prognosztizálható az egyes alapjogok intézményvédelmi oldalán, amely leginkább az EU hatáskörrel rendelkező szerveitől várható, különösen a felügyeleti és végrehajtási hatáskörökkel rendelkező Európai Bizottságtól. A tagállami hatásköröket gyakorló hatóságok delegáltjaiból álló Digitális Szolgáltatások Európai Testülete is értékes módon járulhat hozzá a közös alapjogi sztenderdekből fakadó, a felhasználók alapvető jogait tiszteletben tartó, jó szolgáltatói gyakorlatok kialakulásához, a tagállami hatóságok várhatóan széttartó gyakorlatának harmonizációjához.

⁴⁹ Zódi (2023): i. m.

⁵⁰ Török (2022): i. m. 205.

Az Európai Unió Alapjogi Chartájából fakadó alkalmazási bizonytalanságok

A DSA 1. cikke a szabályozás tárgyaként az alapvető jogok hatékony védelmét jelöli meg, az alapvető jogokat érintő szabályozást közvetlenül összekapcsolja az Alapjogi Chartával, hiszen a védelem tárgyaként a Chartában rögzített alapvető jogokra hivatkozik. Ez azon túl, hogy kijelöli a védendő alapvető jogok körét, az egyes jogok tartalmát, a jogvédelmi mechanizmus jellegét és hatókörét is meghatározza.

Az Európai Unió Alapjogi Chartája preambulumban azokra a társadalmi változásokra és haladásra, valamint a tudományos és technológiai fejlődésre hivatkozik, amelyek a 21. században végbementek, amikor az alapvető jogok egy chartában való megerősítésének szükségességét megindokolja.⁵¹ A DSA szabályait éppen egy ilyen, technológiavezérelt társadalmi változás hívta életre, és ennek a társadalmi változásnak az alapjogi kihívásaira kíván adekvát választ adni.

A DSA az alapvető jogok (közvetett) horizontális hatályú védelmét – helyeseltetően – a leghatékonyabb módon, generálklauzulaként fogalmazza meg, és így általánosan, valamennyi alapvető jogra kiterjeszti, jelentőségük folytán azonban külön is kiemeli a véleménynyilvánítás szabadságát, valamint a tömegtájékoztatás szabadságát és sokszínűségét, amelyeket az Alapjogi Charta 11. cikke is együttesen kezel: „Mindenkinek joga van a véleménynyilvánítás szabadságához. Ez a jog magában foglalja a véleményalkotás szabadságát, valamint az információk és eszmék megismerésének és közlésének szabadságát anélkül, hogy ebbe hatósági szerv beavatkozhatna, továbbá országhatárookra való tekintet nélkül. A tömegtájékoztatás szabadságát és sokszínűségét tiszteletben kell tartani.”⁵²

Érdeemes e helyütt rámutatni, hogy a Chartának a szabad véleménynyilvánítás jogának biztosítását deklaráló rendelkezése kifejezetten a vertikális alapjogvédelem követelményét fogalmazza meg, amikor rögzíti, hogy a szabadság gyakorlásához mindenkinek joga van „anélkül, hogy ebbe hatósági szerv beavatkozhatna,” a tömegtájékoztatás szabadsága kapcsán pedig csak általános tiszteletben tartási kötelezettséget fogalmaz meg. Az Alapjogi Chartából tehát önmagában nem vezethető le a véleménynyilvánítás szabadságának a DSA-ban már *expressis verbis* megfogalmazott, magánjogi jogviszonyokban érvényesülő védelme, a másik oldalról azonban nem is zárja ki az alapjogvédelem kiterjesztését a horizontális hatályú jogviszonyokra.

Az Európai Unió Alapjogi Chartájának elfogadása, amely a tagállamok közös alkotmányos hagyományain alapult, a tagállamok részéről nem csupán egy szimbolikus deklaráció volt, hiszen a Chartát valódi jogi kötőerővel is felruházták. Az Alapjogi Charta elfogadása és jogi kötelező ereje ugyanakkor nem eredményezte az Európai Unió (intézményei) és a tagállamok közötti hatáskörmegosztási status quo megváltozását, hiszen a Charta 51. cikke szerinti alkalmazási körre vonatkozó garanciális szabályok ezt egyértelműen rögzítik. Az alapjogi rendelkezések

⁵¹ Vö. Charta preambulum.

⁵² Charta 11. cikk (1)–(2) bekezdés.

címzettjei az EU intézményei, szervei és hivatalai, a tagállamok pedig csak annyiban, amennyiben uniós jogot hajtanak végre,⁵³ míg az uniós jog alkalmazási körét nem terjeszti ki az EU hatáskörein túlra, új hatásköröket, feladatokat nem hoz létre az EU számára,⁵⁴ vagyis nem jár az alapító szerződésekben rögzített közösségi hatáskörök kiterjesztésével. A Charta tehát nem helyettesíti, csupán kiegészíti az egyes tagállamok alapjogvédelmi rendszereit. A tagállamok változatlanul a saját alkotmányaik alapjogi rendelkezéseiből következő védelmi szintnek és teszteknek megfelelően biztosítják az alapjogok védelmét, azzal, hogy nem kerülhetik meg a Charta rendelkezéseit azokban az esetekben, amikor uniós jogot alkalmaznak. Az Alapjogi Charta alkalmazási köre ugyan csak közvetetten kapcsolódik a DSA-ban foglalt alapjogvédelmi követelményekhez, hiszen a platformszolgáltatókat terhelő alapjogvédelmi követelményeket közvetlenül a Rendelet állapítja meg. A tagállami alkalmazás során ugyanakkor az alkalmazási kör kérdésének kiemelt jelentősége lesz akkor, amikor a tagállami bíróság a szolgáltatást igénybe vevő alanyi jogáról ítél. Az alkotmányjog-tudományban bár vannak, akik a Charta teljes körű, közvetlen tagállami alkalmazása mellett érvelnek,⁵⁵ mi több ezen álláspontok mellett erős indokok hozhatók fel, különösen a Charta jelentőségére, hatására és szoros kapcsolatára az Európai Unió általános értékeivel,⁵⁶ ennek a közeljövőben történő tagállamok általi elfogadása és megvalósulása reálisan nem várható.

A fenti szabályok összevetéséből – nézetem szerint – arra lehet következtetni, hogy a DSA alapjogi követelményei az Európai Unió intézményei és szervei tekintetében egyértelműen (intézményvédelmi) kötelezettséget keletkeztetnek a tekintetben, hogy ellenőrizték, hogy a DSA-ban foglalt közérdekű kötelezettségek teljesítése során a platformszolgáltatók tiszteletben tartják-e a szolgáltatás igénybe vevőinek vagy harmadik feleknek az alapvető jogait. Annak az esélye, hogy az egyes jogsérelmet szenvedő felhasználók közvetlenül a tagállami bíróságok előtt, a DSA-ra és a Chartára hivatkozva eredményesen fel tudnak lépni, közvetlenül hivatkozva az e rendelkezésekből fakadó horizontális hatályú alapjogvédelemre, sokban függ majd az egyes tagállami bíróságok ma még megjósolhatatlan gyakorlatától.

Összegző megállapítások és prognózis

A DSA elfogadásával az európai jogalkotó adekvát választ adott az online platformoknak a demokratikus nyilvánosságot torzító és az alapvető jogok platformokon

⁵³ Vö. Charta 51. cikk (1) bekezdés.

⁵⁴ Vö. Charta 51. cikk (2) bekezdés.

⁵⁵ Például Chronowski Nóra: Az Európai Unió Alapjogi Chartája hatályának kiterjesztéséről – alkotmánypolitikai megfontolások. In Blutman László – Homoki-Nagy Mária (szerk.): *Ünnepi kötet dr. Bodnár László egyetemi tanár 70. születésnapjára*. Szeged, SZTE AJTK, 2014. 85–98.

⁵⁶ Vö. Chronowski (2014): i. m. 86.

való érvényesülését egyre jelentősebben veszélyeztető működésére. Ugyanakkor ez a tanulmány nem vállalkozhatott a DSA teljes körű elemzésére, csupán a Rendeletben bevezetett alapjogvédelmi mechanizmus rövid értékelését végezte el. Üdvözlendő, hogy a DSA sajátos, az európai alkotmányos hagyományokra építő, európai megoldást talált, és olyan szabályozást alkotott, amely amellett, hogy a belső piac működési elveit is figyelembe veszi, az alapvető jogok védelmét is előtérbe helyezi – nemcsak a deklaráció szintjén, hanem egy hatékonynak remélt mechanizmus bevezetésével. Azt, hogy a DSA alapvető jogok érvényesülését biztosítani hivatott megoldásai mennyire lesznek hatékonyak, a rendelet alkalmazhatóságának a kezdete előtt nem lehet megjósolni. Az mindenestre bizonyos, hogy a kívánt alapjogvédelmi hatás több szinten, több fórumon és intézmény közvetítésével fog megvalósulni. A platformokkal szemben megkövetelt alapjogvédelem alanyi jogi jogosultsággént és intézményvédelmi eszközök segítségével is érvényesülhet. A DSA a véleményszabadság horizontális hatályú védelmének bevezetésével olyan mértéktartó megoldást talált, amely megőrzi az alapjogvédelem klasszikus értékeit, és egyúttal bátran terjeszti ki annak hatályát azokra a magánjogi viszonyokra, amelyekben az online platformok az egyének szólásszabadságát korlátozni és a demokratikus diskurzusokat torzítani képes hatalomra tettek szert.

A DSA szabályozási megoldásai alkalmasnak látszanak a platformokon tapasztalható alapjogi kihívások kezelésére. Az alapjogvédelmi szabályok hatékonysága azonban nagymértékben attól függ, hogy a tagállami és EU-s jogalkalmazók mennyire lesznek érzékenyek ezekre az alapjogi követelményekre. A legoptimistább várakozás mellett is fontos azonban kellő visszafogottsággal tudatosítanunk magunkban, hogy a DSA bár számos komoly társadalmi problémára reményteli megoldást kínál, nem csodaszer, a szabályozástól nem várható, hogy varázssütsére a platformnyilvánosság valamennyi társadalmi kihívását kezelni tudja.

Felhasznált irodalom

- 8/2014. (III. 20.) AB határozat az Alaptörvény M) cikk (2) bekezdésének, valamint ezzel összefüggésben az Alaptörvény II. cikkének és a B) cikk (1) bekezdésének értelmezéséről
- Az Európai Parlament és a Tanács (EU) 2018/1808 irányelve (2018. november 14.) a tagállamok audiovizuális médiaszolgáltatások nyújtására vonatkozó egyes törvényi, rendeleti vagy közigazgatási rendelkezéseinek összehangolásáról szóló 2010/13/EU irányelvnek (Audiovizuális médiaszolgáltatásokról szóló irányelv) a változó piaci körülményekre tekintettel való módosításáról. L 303/69 (2018. november 28.)
- Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (2022. október 19.) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (digitális szolgáltatásokról szóló rendelet). L 277/1 (2022. október 27.)
- Az Európai Parlament és a Tanács 2010/13/EU irányelve (2010. március 10.) a tagállamok audiovizuális médiaszolgáltatások nyújtására vonatkozó egyes törvényi, rendeleti vagy közigazgatási

- Az újmédia szabályozásának új iránya? – A Digital Services Act alapjogvédelmi mechanizmusa rendelkezéseinek összehangolásáról (Audiovizuális médiaszolgáltatásokról szóló irányelv). L 95/1 (2010. április 15.)
- Az Európai Unió Alapjogi Chartája. 2016/C 202/02 (2016. június 7.)
- Bedő Renáta: Az alapjogok érvényesülése magánviszonyokban Magyarországon – fókuszban a fórumrendszer. *Fundamentum*, 22. (2018), 1. 58–69.
- Bundesgesetz über Maßnahmen zum Schutz der Nutzer auf Kommunikationsplattformen (Kommunikationsplattformen-Gesetz – KoPl-G). Online: www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20011415
- Chronowski Nóra: Az Európai Unió Alapjogi Chartája hatályának kiterjesztéséről – alkotmánypolitikai megfontolások. In Blutman László – Homoki-Nagy Mária (szerk.): *Ünnepi kötet dr. Bodnár László egyetemi tanár 70. születésnapjára*. Szeged, SZTE ÁJTK, 2014. 85–98.
- Európai Bizottság: *Javaslat. Az Európai Parlament és a Tanács rendelete a digitális szolgáltatások egy-egyes piacáról (digitális szolgáltatásokról szóló jogszabály) és a 2000/31/EK irányelv módosításáról*. COM(2020)825 végleges (2020. december 15.)
- Gárdos-Orosz Fruzsina: Alapjogok alkalmazása a magánjogi jogvitákban az Európai Unióban és ennek lehetséges hatásai a magyar jogra. *Állam- és Jogtudomány*, 51. (2010a), 3. 225–258.
- Gárdos-Orosz Fruzsina: Az alkotmányjog a magánjogi jogviszonyokban. *Rendészeti Szemle*, 58. (2010b), 4. 19–35.
- Gárdos-Orosz Fruzsina – Bedő Renáta: Az alapvető jogok érvényesítése a magánjogi jogviták során – az újabb alkotmányjogi gyakorlat (2014–2018). *Alkotmánybírószági Szemle*, (2018), 1. 3–15.
- Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG). Online: www.gesetze-im-internet.de/netzdg/BJNR335210017.html
- Gosztonyi Gergely: *Cenzúra Arisztoteléstől a Facebookig. A közösségi média tartalomszabályozási gyakorlatának komplexitása*. Budapest, Gondolat Kiadó, 2022.
- Klein Tamás: *Sajtószabadság és demokrácia*. Budapest, Gondolat – Dialóg Campus, 2020.
- Koltay András: *Az új média és a szólásszabadság. A nyilvánosság alkotmányos alapjainak újragondolása*. Budapest, Wolters Kluwer, 2019.
- LOI n° 2020-766 du 24 juin 2020 visant à lutter, contre les contenus haineux sur internet. Online: www.legifrance.gouv.fr/download/pdf?id=CP05NSqcPl5IPNu3MsP2PSu1fmt64dDetDQxhvJZNM6
- Papp János Tamás: *A közösségi média szabályozása a demokratikus nyilvánosság védelmében*. Budapest, Wolters Kluwer, 2022.
- Sári János – Somody Bernadette: *Alapjogok. Alkotmánytan II*. Budapest, Osiris Kiadó, 2008.
- Szikora Tamás: A platformszabályozás egy új iránya Donald Trump Facebookról való kitiltásának példáján keresztül. In Török Bernát – Zódi Zsolt (szerk.): *Az internetes platformok kora*. Budapest, Ludovika Egyetemi Kiadó, 2022. 209–226.
- Török Bernát: A szólásszabadság a közösségi platformokon és a Digital Services Act. In Török Bernát – Zódi Zsolt (szerk.): *Az internetes platformok kora*. Budapest, Ludovika Egyetemi Kiadó, 2022. 195–207.
- Udvary Sándor: Media Revolution – Effects of Technological Development on Freedom of Expression. In Kapa Mátyás (szerk.): *Studia Iuridica Caroliensia 2*. Budapest, KRE Állam és Jogtudományi Kar, 2007. 197–215.
- Zódi Zsolt: A platform mint elméleti konstrukció és mint narratív keret – A platformfogalom kialakulásának története. In Török Bernát – Zódi Zsolt (szerk.): *Az internetes platformok kora*. Budapest, Ludovika Egyetemi Kiadó, 2022. 17–38.
- Zódi Zsolt: *Platformjog*. Budapest, Ludovika Egyetemi Kiadó, 2023.

Vákát

Papp János Tamás

A szűrőbuborék kipukkasztása – Gondolatok az online szűrőbuborékok és visszhangkamrák koncepciójának újraértelmezéséhez



A tanulmány az online szűrőbuborékok és visszhangkamrák koncepcióival és azok empirikus alátámasztásának hiányával foglalkozik. A mára már szinonimává vált két kifejezés által fémjelzett jelenség arra utal, hogy az online térben a felhasználók kizárólag vagy túlnyomó többségében csak olyan hírekkel vagy információkkal találkozhatnak, amelyek érdeklődési körüket, véleményüket és hiedelmeiket tükrözik, vagyis hogy „visszhangkamrákban” élnek a közösségi médiában. Ezt azonban nem támasztják alá az empirikus kutatások, ugyanis egy nagy választékú médiakörnyezetben csak a lakosság egy nagyon kis része találhatja magát visszhangkamrában. Ennek ellenére a buborékok vagy visszhangkamrák léteznek, társadalmi jelentőségük és az általuk okozott lehetséges társadalmi károk valódiak, azonban az a gondolat, amely az online platformokat hibáztatja ezek kialakulásáért, nem igazolható tudományos kutatásokkal. A napjainkban is egyre inkább tapasztalható társadalmi polarizálódás a hagyományos és az online média kölcsönös együttthatásaként jött létre: az internetnek köszönhetően kialakult figyelemalapú médiakörnyezetben a hagyományos média egyre inkább véleményalapúvá vált, ezáltal megnőtt a személyes perszonalizáció lehetősége, amely folyamatot tovább erősített a közösségi média, aminek következtében a sajtó még inkább a kevésbé minőségi, de nagyobb interakciót eredményező, polarizált tartalom-előállítás irányába mozdult el. Az így létrejött ördögi kör nagyon nehezen kezelhető, a legalkalmasabb eszköz talán a minőségi, objektív újságírói tartalmak előállításának támogatása lehet, amely által nehezebbé válik a párhuzamos nyilvánosságok elkülönítésének fenntartása.

Az online perszonalizáció különböző formái

Talán nem túlzó kijelentés, hogy az online platformok – és azon belül a közösségi média – alapjaiban változtatták meg a nyilvánosság szerkezetét. A 20. század második felétől meghatározó szerepű tömegtájékoztatást javarészt felváltotta az egyéniesített, személyre szabott tartalomfogyasztás. A tömegkommunikáció korábban csak kevesek számára nyitva álló lehetősége szinte bárki számára elérhetővé vált, ezzel pedig korábban elképzelhetetlen mennyiségű szöveg kerül bele a napi cirkulációba. Csak a YouTube-ra percenként több mint 500 órányi videót töltenek fel,¹ vagyis olyan mennyiségű tartalom keletkezik percenként egy-egy közösségi

¹ Hours of Video Uploaded to YouTube Every Minute. *Statista*, 2022. április 4.

oldalon, hogy amennyiben ezt valamiféle előzetes, a platform által üzemeltetett tartalomrendező elv nélkül próbálná megtekinteni a felhasználó, káoszba fulladna a felhasználói élmény. A közösségi oldalak tehát némiképp a felhasználói élmény javítása érdekében, de mindenképpen a platform érdekeinek megfelelően optimalizálják a tartalomrendező algoritmusait, aminek fő célja, „hogy a felhasználó minél több (hirdetések megnézésére is fordítható) időt töltsön a felületükön, ennek érdekében pedig a korábbi kereséseinek, preferenciáinak megfelelő tartalmakat szűr és tár elé az algoritmus”.²

A platformok által ajánlott tartalom tehát mindenki részére személyre szabott, és az adott felhasználó ismerősi vagy érdeklődési köréhez, valamint az adott platformon, sőt azon kívüli online tevékenységéhez van igazítva.³ A közösségi oldalak viszont a perszonalizáció két különböző megjelenési formáját okozhatják. Először is, a fent említett módon, egy átláthatatlan algoritmus határozza meg, hogy milyen tartalom jelenjen meg a felhasználó hírfolyamában. Másodszor azonban, bár az emberek különféle típusú ismerősökkel (barátokkal, családdal, kollégákkal stb.) lépnek kapcsolatba az ilyen oldalakon, sokan többnyire olyan emberekkel tartják azt fent, akik hasonlítanak rájuk. Ha valakinek az adott platformon kialakított személyes és egyéb érdeklődési hálózata meglehetősen homogén, az azt jelenti, hogy az ismerősök vagy az általa követett oldalak által megosztott tartalom is összhangban van az illető preferenciáival.⁴ A személyre szabott tartalommegjelenítésnek – más szóval perszonalizációnak – tehát két fő típusát különböztetjük meg: a felhasználó által egyénileg beállított perszonalizációt, valamint az algoritmusok és egyéb ajánlórendszerek által kialakított perszonalizációt. Ezeket más néven hívhatjuk önkéntes vagy előzetes személyre szabásnak,⁵ vagy megint másképpen „explicit” vagy „implicit” perszonalizációnak is.⁶

Utóbbi, vagyis az algoritmusok által végzett perszonalizáció régóta képezi az online platformokkal kapcsolatos tudományos vizsgálódások meghatározó fókuszát. Az mára talán mindenki számára egyértelmű, hogy a közösségimédia-platformok nem csupán inaktív szereplőként működnek, hanem aktívan „navigálják a felhasználókat az általuk meghatározott tartalmakhoz”.⁷ A tartalmakkal kapcsolatban ugyanis nem csupán moderálási tevékenységet végeznek, vagyis az illegális tartalmak szűrését, hanem a rengeteg felhasználói tartalom között egyfajta „kurátorként”

² Veszelszki Ágnes: deepFAKEnews: Az információmanipuláció új módszerei. In Balázs László (szerk.): *Digitális kommunikáció és tudatosság*. Budapest, Hungarovox Kiadó, 2021. 96.

³ Birgit Stark et al.: Are Algorithms a Threat to Democracy? The Rise of Intermediaries: A Challenge for Public Discourse. *Algorithm Watch*, 2020. 12.

⁴ Frederik J. Zuiderveen Borgesius et al.: Should We Worry About Filter Bubbles? *Internet Policy Review*, 5. (2016), 1. 7.

⁵ Richard Fletcher: The Truth Behind Filter Bubbles: Bursting Some Myths. *Reuters Institute for the Study of Journalism*, 2020. január 24.

⁶ Borgesius (2016): i. m. 3.

⁷ Tarleton Gillespie: The Politics of ‘Platforms’. *New Media & Society*, 12. (2010), 3. 348.

tevékenykedve állítják össze a felhasználó egyéni idővonalát.⁸ Ezen két tevékenységet választja külön Sofia Grafanaki, nevezetesen a „tárhely legalitása céljából” történő és a „navigálás érdekében” történő kurátori tevékenységet.⁹ Előbbi annak eldöntését jelenti, hogy a tartalom egyáltalán maradhat-e a platformon, míg az utóbbi arról dönt, hogy mely tartalmakra hívja fel a felhasználók figyelmét, mely tartalmakat soroljon előrébb és hátrébb.¹⁰ Utóbbi tevékenység folytán tehát a felhasználók idővonalai kivétel nélkül valamilyen egyedi összeállítás alapján jönnek létre, vagyis egyediesített módon jelennek meg. Az „egyediesített” pedig Paul Bernal szerint egyet jelent a „manipulálttal”, hiszen akár pénzügyi-gazdasági, akár marketing-, akár politikai célok mentén alakítják ki a felhasználók idővonalát, semmiképp sem nevezhető semleges, befolyástól mentes tartalomszolgáltatásnak.¹¹ 2021. január 11-én Adam Mosseri, az Instagram vezetője írta azt a Twitteren, hogy „nem vagyunk semlegesek. Egyetlen platform sem semleges, mindannyiunknak vannak értékei, és ezek az értékek befolyásolják a döntéseinket.”¹² Egyesek nevet is adtak a jelenségnek, számítógépes propagandának (*computational propaganda*) hívják, amely szerintük a politikai manipuláció új formája, amely az interneten keresztül zajlik, és a közösségimédia-platformok, botok és algoritmusok együttes működésével igyekszik befolyásolni a közvéleményt.¹³

A szűrőbuborékok és visszhangkamrák koncepciója

Ezen perszonalizáció kapcsán gyakran hallunk a szűrőbuborék vagy visszhangkamra kifejezésről, amelyet legfőképpen a platformok által a felhasználókra gyakorolt (káros) befolyás vonatkozásában szoktak emlegetni. A visszhangkamra metaforáját először 2001-ben Cass Sunstein fogalmazta meg, amikor leírta, hogy a csoportdinamikus véleményformálási folyamatok hogyan haladnak a személyre szabott információk környezetekben, amelyek következetesen tükrözik az egyén saját magáról alkotott véleményét, mint a visszhang.¹⁴ Így a visszhangkamra kifejezés a kizárólagosan hasonló véleményeknek való kitettségre utal az online környezetben. Sunstein

⁸ Tarleton Gillespie: The Relevance of Algorithms, in Media Technologies. In Tarleton Gillespie – Pablo J. Boczkowski – Kirsten A. Foot (szerk.): *Media Technologies. Essays on Communication, Materiality, and Society*. Cambridge, MA, The MIT Press, 2014. 167.

⁹ Sofia Grafanaki: Platforms, the First Amendment and Online Speech Regulating the Filters. *Pace Law Review*, 39. (2018), 1. 119.

¹⁰ Grafanaki (2018): i. m. 126.

¹¹ Paul Bernal: *The Internet, Warts and All*. Cambridge, Cambridge University Press, 2018. 92.

¹² Idézi: Seth Oranburg: Social Media and Democracy after the Capitol Riot, or, A Cautionary Tale of the Giant Goldfish. *Mercer Law Review*, 73. (2022), 2. 594.

¹³ Samuel C. Woolley – Philip N. Howard (szerk.): *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*. New York, Oxford University Press, 2018. 2–5.

¹⁴ Lásd Cass R. Sunstein: *Republic.com*. Princeton, Princeton University Press, 2001.

szerint egy demokratikus társadalomban az embereknek olyan információkkal kell találkozniuk, amelyek eltérnek a saját véleményüktől, annak érdekében, hogy teljes mértékben meg tudják formálni saját álláspontjukat. Ellenkező esetben az emberek beléphetnek az „attitűdök megerősítésének spiráljába”, és szélsőségesebb nézőpontok felé sodródhatnak.¹⁵ Az Európai Unió egy szakértői csoportja által készített jelentés is megemlíti, hogy „egyesek attól tartanak, hogy az internetes szűrőmechanizmusok, tekintettel növekvő személyre szabási lehetőségükre, egyre elszigeteltebb és kevésbé elkötelezett társadalmi közösségeket hozhatnak létre a nagyközönségen belül”.¹⁶ A jelenség tehát arra utal, hogy az emberek kizárólag vagy túlnyomó többségben csak olyan hírekkel találkoznak, amelyek érdeklődési körüket, véleményüket és hiedelmeiket tükrözik, vagyis hogy „visszhangkamrákban” élnek a közösségi médiában.¹⁷ Ezen kutatások szerint azok az emberek, akik ismétlődő módon ki vannak téve részrehajló tartalmaknak, amelyek egy sajátjukhoz közel álló politikai álláspontot részesítenek előnyben, végül szélsőségesebb álláspontot alakítanak ki, és kevésbé lesznek toleránsak az ellenkező nézőpontokkal szemben.¹⁸

A visszhangkamrák melletti másik gyakran elhangzó kifejezés a szűrőbuborék. A szűrőbuborék egy Eli Pariser¹⁹ által alkotott fogalom, amely egyfajta szellemi elszigeteltség állapotát jelenti, amely személyre szabott keresésekből származhat, amikor egy weboldal algoritmusa a felhasználóval kapcsolatos információk (például a tartózkodási hely, a korábbi kattintási viselkedés és a keresési előzmények) alapján kitalálja, hogy milyen információkat szeretne látni. Ennek eredményeként a felhasználók nem, vagy nagyon keveset találkoznak azokkal az információkkal, amelyek nem illeszkednek a látásmódjukba, hatékonyan elszigetelve őket saját kulturális vagy ideológiai buborékjaikban.²⁰ Bizonyos kutatások azt mutatták, hogy a felhasználók inkább azokat a híreket választják, amelyek jó érzésekkel töltik el őket, és megerősítik meglévő véleményüket és elfogultságukat.²¹ A közösségi oldalak működése és az a lehetőségünk, hogy gyorsan és egyszerűen tömegekkel oszthatjuk meg rajtuk keresztül nézeteinket, tovább növeli az egyes társadalmi csoportok megosztottságát, és mindennap újabb és újabb buborékok jönnek létre.²² Egyes szerzők

¹⁵ Cass R. Sunstein: The Law of Group Polarization. *The Journal of Political Philosophy*, 10. (2002), 2. 178.

¹⁶ Vaira Viķe-Freiberga et al.: *A Free and Pluralistic Media to Sustain European Democracy*. The Report of the High Level Group on Media Freedom and Pluralism, 2013. 31.

¹⁷ Katrina Lee: Your Honor, on Social Media: The Judicial Ethics of Bots and Bubbles. *Nevada Law Journal*, 19. (2019), 3. 808.

¹⁸ Borgesius (2016): i. m. 8.

¹⁹ Lásd Eli Pariser: *The Filter Bubble. How the New Personalized Web Is Changing What We Read and How We Think*. New York, Penguin Publishing, 2012.

²⁰ Cass R. Sunstein: *Republic.com 2.0*. Ford. Veres Péter. Budapest, Wolters Kluwer, 2013. 18.

²¹ Cass R. Sunstein: *#Republic: Divided Democracy in the Age of Social Media*. Princeton, Princeton University Press, 2017. 104–108.

²² Neill Fitzpatrick: Media Manipulation 2.0: The Impact of Social Media on News, Competition, and Accuracy. *Athens Journal of Mass Media and Communications*, 4. (2018), 1. 56.

szerint ezáltal a szűrőbuborékok létezése magát a demokráciát is fenyegeti.²³ Daniel Maggen három fő megítélást fogalmaz meg a szűrőbuborékokkal kapcsolatban. Kiindulópontként rögzíti, hogy a témával foglalkozó tudósok nagy része pusztán az algoritmusok lehetséges hibáira koncentrálnak, így figyelmen kívül hagyják az algoritmusok átlagos működésében rejlő veszélyeket. Másrészt arra mutat rá, hogy a szűrőbuborékok hatására a politikai döntéshozók is szűkebb körű információkkal rendelkeznek, így sokszor döntéseiket is merőben befolyásolják a szűrőbuborékok. Végül pedig kiemeli, hogy a szűrőbuborékok két fő tevékenysége, vagyis az adott világnézetnek megfelelő tartalmak ajánlása és az azzal ellentétesen ható információk kizárása közül utóbbi a sokkal nagyobb probléma.²⁴ Egyes tanulmányok pedig Maggenhez hasonlóan arra mutatnak rá, hogy az online szűrőbuborékok jelensége még a bírói pártatlanságra is negatív hatással lehet.²⁵

Bár Pariser eredetileg főként a keresőmotorokra vonatkoztatva fogalmazta meg tételeit, az utóbbi időben ő is egyre inkább a közösségi oldalak kapcsán beszél a jelenségről.²⁶ Ebben az új, közösségi médiára összpontosító inkarnációban azonban szerinte a szűrőbuborék-konceptió egyre inkább összefonódik a visszhangkamrák fogalmával. Számos tudományos cikk is ma már lényegében felcserélhető módon használja a két kifejezést.²⁷ Ahogy arra Axel Bruns is rámutat, annak ellenére, hogy meglehetősen sokat írtak róla, Sunstein és Pariser sem határozta meg egyértelműen a szűrőbuborékok és a visszhangkamrák fogalmát, így az azt követő kutatások során vagy szinonimaként, vagy meglehetősen zavaros meghatározásokkal használták a fogalmakat.²⁸ Véleménye szerint ezért „az olyan átgondolatlan metaforákról folytatott viták, mint a visszhangkamrák és a szűrőbuborékok, olyan figyelemelterelés, amelyet már nem engedhetünk meg magunknak, mert megakadályozza, hogy sokkal fontosabb ügyekkel szembesüljünk”.²⁹ Még ha nem is tekintjük teljes mértékben „figyelemelterelésnek” a szűrőbuborékok és visszhangkamrák jelenségét, annyit mindenképpen meg kell jegyeznünk, hogy a két fogalom mára a tudományos és a laikus diskurzusokban is voltaképpen ugyanazt a jelenséget írja le, így jelen tanulmány is szinonimaként kezeli a két kifejezést.

²³ Sara J. Benson: @PublicForum: The Argument for a Public Forum Analysis of Government Officials' Social Media Accounts. *Washington University Jurisprudence Review*, 12. (2019), 1. 109.

²⁴ Daniel Maggen: Law In, Law Out: Legalistic Filter Bubbles and the Algorithmic Prevention of Nonconsensual Pornography. *Cardozo Law Review*, 43. (2022), 5. 1751–1753.

²⁵ Lee (2019): i. m. 790.

²⁶ Eli Pariser: Did Facebook's Big Study Kill My Filter Bubble Thesis? *Wired*, 2015. május 7.

²⁷ Axel Bruns: Filter Bubble. *Internet Policy Review*, 8. (2019a), 4.

²⁸ Axel Bruns: *It's Not the Technology, Stupid: How the 'Echo Chamber' and 'Filter Bubble' Metaphors Have Failed Us*. Brisbane, Digital Media Research Centre (QUT), 2019b. 3.

²⁹ Bruns (2019b): i. m. 9.

A koncepció gyakorlati igazolásának hiánya

A szűrőbuborékokkal kapcsolatos tudományos ellentmondás abból fakad, hogy nagyon nehéz empirikus módon vizsgálni a szűrőbuborékok és visszhangkamrák valódi hatását, ezért az ebből levonható következtetések is sokszor vitatottak.³⁰ Egyes kutatók a politikai nézetek mentén magas szintű klaszteresedéstről számolnak be, ami a közösségi média platformjait visszhangkamraként jellemezte, míg mások azt találták, hogy az online ideológiai szegregáció abszolút értelemben alacsony, és az online térre inkább jellemző a nyílt ideológiai eszmecsere és az ideológiai sokféleségnek való kitettség.³¹ Egy kutatás során például internethasználókat kérdeztek arról, hogy hogyan használják a különböző keresőoldalakat, a közösségi médiát és más egyéb médiát politikai információszerzés céljából. Az eredmények azt mutatták, hogy a közösségi oldalak használata vagy az internetes keresés csupán csak egy mozzanata a politikai információszerzésnek, vagyis a politika iránt érdeklődők nincsenek buborékba zárva az online portálok által. Ezzel párhuzamosan a kutatás vezetői a visszhangkamrák jelenségére sem találtak empirikus bizonyítékot, a megkérdezettek többsége ugyanis ellenőrzi a problémás vagy meghökkentő politikai információkat, így különböző nézőpontoknak teszi ki saját magát. Így a kutatók szerint a közösségi oldalakkal és a buborékokkal kapcsolatos bizonyos nézetek nemcsak túlbecsülik a technikai értelemben determináló tényezőket, hanem alábecsülik az internet, a közösségi média és a keresőprogramok tudatos használatának társadalmi elterjedését is.³²

Egy 2015-ben készült tanulmány, amely 3,8 millió Twitter-felhasználó megkérdezésén alapult, arra a következtetésre jutott, hogy túlbecsülték a közösségi médiában jelen lévő „ideológiai szegregációt”. A kutatók kimutatták, hogy a közösségi médiának mint kommunikációs eszköznek az interperszonális hálózatokon belüli használatát nem feltétlenül korlátozzák ideológiai elköteleződések, különösen, ha nem politikai kérdésekről és eseményekről van szó. A kutatás eredményei azt mutatták, hogy bár a liberális beállítottságú felhasználók hajlamosak más liberális felhasználók tweetjeit retweetelni, a konzervatívok pedig különösen nagy valószínűséggel más konzervatívok tweetjeit, a nem politikai témákról, például a bostoni maratoni robbantásról, a 2014-es Super Bowlról vagy a 2014-es téli olimpiáról szóló retweetek azonban mind átlépték az ideológiai határokat.³³ Katrina Lee szerint még ha egy tudományos vizsgálat – amely például csak a Twitter-t vizsgálja – bizonyítékokat

³⁰ Judith Moeller – Natali Helberger: *Beyond the Filter Bubble: Concepts, Myths, Evidence and Issues for Future Debates*. Amsterdam, University of Amsterdam, 2018.

³¹ Pablo Barberá et al.: Tweeting From Left to Right: Is Online Political Communication More Than an Echo Chamber? *Psychological Science*, 26. (2015), 10. 1532.

³² William H. Dutton et al.: *Social Shaping of the Politics of Internet Search and Networking: Moving Beyond Filter Bubbles, Echo Chambers, and Fake News*. Quello Center Working Paper No. 2944191. 1.

³³ Barberá (2015): i. m. 1537.

is talál a visszhangkamrákra és a politikai polarizációra, ez nem feltétlenül jelenti azt, hogy egy adott felhasználó mindenképp visszhangkamrában él. Rámutat arra, hogy sok tanulmány nem vett figyelembe más információforrásokat, amelyekhez a felhasználó hozzáférhet, például a személyes beszélgetéseket, újságokat vagy a televíziót. Ebből kifolyólag szerinte kijelenthető, hogy a közösségi média kisebb szerepet játszott a politikai polarizációban, mint ahogyan attól a közösségi oldalak kezdeti évei idején tartottak.³⁴

A témával foglalkozó kutatások nagy része mindemellett figyelmen kívül hagyja a korábban említett explicit perszonalizációt, vagyis hogy a közösségi médiában és a való életben az egyének olyan információkkal és perspektívákkal is találkoznak, amelyek akár változatosak is, azonban a megjelenő tartalmak közül ők maguk választják ki, hogy mely információkat olvassák el részletesen, így egy saját visszhangkamrahatást alakíthatnak ki algoritmusok nélkül is. Egy, a Michigani Egyetem által végzett kutatás szintén azt hangsúlyozta, hogy az egyének beállítottságának megfelelő információknak való kitettségét nem az algoritmusok által keltett buborékok, hanem a felhasználók saját döntései okozzák.³⁵ Az implicit személyre szabás hatásait ugyanis más erők is ellensúlyozhatják. Például azok az emberek, akik saját maguk választanak ki tartalmat egyes blogokon, és emellett sok előre kiválasztott tartalommal találkoznak a Facebook-hírfolyamukban, továbbra is lelkes felhasználói lehetnek a nem személyre szabott híroldalaknak is.³⁶ Más szerzők is azon a véleményen vannak, hogy ma, egy nagy választékú médiakörnyezetben valószínűleg csak a lakosság egy nagyon kis része találhatja magát visszhangkamrában, ezért a visszhangkamrákat és szűrőbuborékokat vizsgáló tanulmányok többsége hibás, mivel nem tesztelik az elméletet a nagy választékú médiakörnyezet reális összefüggésében.³⁷

Gálik Mihály cikkében jelen sorok írójánál sokkal részletesebben és mélyrehatóbban veszi sorra a témában készült kutatásokat, és rengeteg releváns tanulmányt elemezve mutatja be, hogy az empirikus kutatások egyáltalán nem támasztják alá az online szűrőbuborékokkal kapcsolatos aggályokat. Arra a következtetésre jut, hogy „a hagyományos, a tömegmédia korából megörökölt hírmédia erős hálózati jelenléte, az online hírmédiában jelen lévő nagyszámú szereplő, valamint az a tény, hogy a közönség jó része több forrásból tájékozódik, hatékonyan állja útját már az online hírmédiában is a visszhangkamrák kialakulásának, nem beszélve a hírmédia egészéről”.³⁸

³⁴ Lee (2019): i. m. 809.

³⁵ Eytan Bakshy et al.: Exposure to Ideologically Diverse News and Opinion on Facebook. *Science*, 348. (2015), 6239.

³⁶ Borgesius (2016): i. m. 10.

³⁷ Elizabeth Dubois – Grant Blank: The Echo Chamber Is Overstated: The Moderating Effect of Political Interest and Diverse Media. *Information, Communication & Society*, 21. (2018), 5. 744.

³⁸ Gálik Mihály: Visszhangkamrák és szűrőbuborékok. A hírfogyasztásról szóló vita a digitális hálózati média-ökoszisztéma világában. *Médiakutató*, 21. (2020), 1. 32.

Mindezek ellenére annyi azonban legalább biztosan kijelenthető, hogy az algoritmusok útján való információrendezés mindenképpen hatással lehet a felhasználókra, és ezáltal a demokratikus nyilvánosságra. Az empirikus kutatásokkal is igazolható, hogy a közösségi oldalakon megjelenő tartalmak az egyének szempontjából sokkal kevésbé sokszínűek és kiegyensúlyozottak,³⁹ ennek pedig egyik eredménye, hogy nagyon hatékonyan polarizálják a társadalmat.⁴⁰ Veszelszki Ágnes is azon az állásponton van, hogy bár a szűrőbuborék jelenségét empirikus adatok alapján egyes kutatások megkérdőjelezzik, annyi mindenképpen állítható, hogy az online felületek mögött működő algoritmusok befolyással bírnak arra, milyen információkkal találkozik a böngésző személy az interneten. Szerinte még ha nem is fogadjuk el a szűrőbuborék-jelenség meglétét, abban az esetben is működik az úgynevezett ismétlési hatás, vagyis ha ugyanazzal az információval többször, akár ugyanolyan forrásból, redundáns módon találkozunk a felhasználó, az az ismétlés révén sokkal meggyőzőbb lesz számára.⁴¹

Azt láthatjuk tehát, hogy a szűrőbuborékok jelensége bár teoretikus szempontból logikusnak tűnik, gyakorlati jelenléte a valóságban mégsem igazolható. Ennek egyik oka a felhasználó saját autonóm szűrőtevékenysége (vagyis az explicit perszonalizáció), másik oka pedig a tájékozódás céljából széles körben rendelkezésre álló diverz médiakörnyezet. Persze sokak szerint önmagában már az is vitatott kérdés lehet, hogy a politikai döntések tekintetében vajon mekkora befolyásoló ereje van ténylegesen az egyes médiumoknak – köztük a közösségi médiának is. Bajomi-Lázár Péter szerint például annak, hogy a média csak korlátozott mértékben és áttételesen képes befolyásolni a közönséget, az az oka, hogy a média csak egy az embereket befolyásoló számos tényező között: ott van mellette egyebek között a család, a kortárs csoport, az iskola, az egyház és – nem utolsósorban – a személyes tapasztalás.⁴²

A média és az online platformok polarizáló hatása

Ha viszont a személyes tapasztalás leszűkül a közösségi médiára, annak befolyásolási képessége jóval nagyobbat nő. Ha a felhasználó a társadalmi életének jelentős részét a közösségi oldalakon keresztül éli meg, vagyis itt tartja a kapcsolatot a barátaival, családtagjaival, innen tájékozódik, itt fogyaszt szórakoztató tartalmakat, akkor a közösségi oldal befolyásoló ereje is vélhetően sokkal nagyobb. Ez a jelenség pedig már úgy tűnik, kibontakozóban van, ugyanis az online platformok egyre inkább

³⁹ Giovanni Luca Ciampaglia – Filippo Menczer: Misinformation and Biases Infect Social Media, Both Intentionally and Accidentally. *The Conversation*, 2018. június 20.

⁴⁰ Political Bias on Social Media Emerges from Users, Not Platform, IU Study Says. *Indiana University*.

⁴¹ Veszelszki (2021): i. m. 96.

⁴² Bajomi-Lázár Péter: Manipulál-e a média? *Médiakutató*, 18. (2017), 4. 74.

a hírolvasás elsődleges színtereivé válnak.⁴³ Egy 2019 végén végzett kutatásból az olvasható ki, hogy a hazai „facebookozó” lakosság háromnegyede legalább heti rendszerességgel használja hírfogyasztásra a szolgáltatást, és főként az elé kerülő hírekből tájékozódik.⁴⁴ Ebből pedig egyenesen következik, hogy az online platformok átalakítják a hír- és az információáramlás módját, közvetlen hatást gyakorolva az újságírássra és a tömegtájékoztatásra, meghatározva ezzel azok működési gyakorlatát.⁴⁵ Bár sokan úgy gondolnak a platformok által alkalmazott algoritmusokra, mint egyszerű matematikai műveleteken alapuló, elfogulatlan rendezőeszközökre, ezek mögött emberi tényezők vannak, alkotók, akik így tevékenységükkel komolyan befolyásolják az újságírást, vagyis a nyilvánosság számára egyfajta „kidobóként” szolgálnak, akik saját döntéseik alapján döntenek el, hogy milyen információ juthat be a „közösségi házibuliba”. Mike Ananny és Kate Crawford ezt a jelenséget úgy írja le, hogy a platformok és az algoritmusok tervezői egyfajta „küszöbön álló sajtóként” (*liminal press*) működnek.⁴⁶

Ahogy az információs kapuőr szerepe kezd átkerülni a hírügynökségek újságíróiról a kódolókra és a tervezőkre, a sajtó és az általa készített hírek természete is megváltozik.⁴⁷ Ahogyan a televízió sem közvetlenül, direkt módon befolyásolja a nézők tevékenységét, hanem hosszú távon, sokkal finomabb módon,⁴⁸ így az algoritmusok sem azonnal fejtik ki hatásukat. Lam Tuy Vo ezen a téren három új trendet azonosít az online platformok tevékenységének következményeként: (1) információs szegregáció, vagyis hogy az információk nem azonosan jutnak el mindenkihez, minden felhasználóhoz csupán egy személyre szabott, szűkített kör jut; (2) az információfogyasztás politikai megnyilvánulássá vált, mert a platform annak megfelelően alakítja ki a profilunkat, ahogyan fogyasztjuk az információkat, vagy ahogy reagálunk rá, így minden egyes reakció (vagy annak hiánya) a politikai véleményünket közvetíti a platform irányába; (3) mindezek következményeként a felhasználók közötti párhuzamos valóságok kialakulása.⁴⁹

Napjainkra a hírekkel kapcsolatos sajtó és a kábeltelevíziók is egyre inkább véleményalapúvá váltak, vagyis a hagyományos médiában is megfigyelhető a polarizáció

⁴³ Erin C. Carroll: Making News: Balancing Newsworthiness and Privacy in the Age of Algorithms. *Georgetown Law Journal*, 106. (2017), 1. 82.

⁴⁴ Török Bernát – Rab Árpád – Szikora Tamás: *Internetes attitűdök – Régióink és a világháló*. Budapest, NKE Információs Társadalom Kutatóintézet, 2020.

⁴⁵ Carroll (2017): i. m. 86.

⁴⁶ Mike Ananny – Kate Crawford: A Liminal Press: Situating News App Designers within a Field of Networked News Production. *Digital Journalism*, 3. (2015), 2. 192–208.

⁴⁷ Carroll (2017): i. m. 71.

⁴⁸ Kimberlianne Podlas: Reconsidering the Nomos in Today's Media Environment. *Touro Law Review*, 37. (2022), 4. 2219–2220.

⁴⁹ Lam Tuy Vo: How the Internet Created Multiple Publics. *Georgetown Law Technology Review*, 4. (2020), 2. 412.

jelensége.⁵⁰ A sajtóban mindig is jelen volt, a televíziózás világában pedig a kábel-televíziók térnyerése óta megvan a lehetőség az explicit perszonalizációra. A nézők saját döntéseik alapján tudják kiválasztani azokat a tartalmakat, amelyeket nézni vagy olvasni szeretnének, és elkerülni azokat a csatornákat vagy fórumokat, amelyek az övékével ellentétes véleményeket fogalmaznak meg.⁵¹ A kutatások pedig alátámasztják, hogy a nézők élnek is ezzel a lehetőséggel, és sokkal inkább a saját nézeteiknek megfelelő csatornákat néznek.⁵²

A felelősség tehát nem csak az online platformokat terheli. Ahhoz, hogy a felhasználók politikailag vagy ideológiailag elfogult tartalmak buborékjába kerüljenek, ezeket a tartalmakat valakinek elő is kell állítani. Az internet térnyerése egyelőre nem jelentette a televíziós és sajtón keresztüli hírfogyasztás végét, a kutatások azt mutatják, hogy a közösségi oldalakon és az interneten keresztül történő hírfogyasztás nem váltotta fel, csupán kiegészíti a televíziós hírfogyasztást.⁵³ Ennek következtében ma több hírt fogyasztunk, mint bármikor korábban, azonban sokkal kevesebb és kevésbé változatos forrásból.⁵⁴ A felhasználók ezért úgy gondolják, hogy mivel ők rengeteg hírt olvasnak, ezért jól informáltak, ez pedig a gondolatok piacának illúzióját kelti bennük.⁵⁵ A kutatások alapján a felhasználók túlnyomó többsége felismeri az elfogultságot egy-egy hír vagy hírforrás kapcsán, és annak figyelembevételével kezeli az így megszerzett információkat, vagyis következetesen „szelektív” hírmegosztásban vesznek részt a közösségi oldalakon. Ez azt jelenti, hogy gyakrabban olvasnak és osztanak meg olyan híreket, amelyek saját ideológiájuknak kedveznek, vagyis nem igaz a „naiv hírolvasók” mintaképe, akik minden újtjukba kerülő információt megosztanak.⁵⁶ Ezáltal a közösségi média társadalmi polarizáltságra gyakorolt lehetséges negatív hatásai főként akkor mutatkoznak meg, ha maga a kérdéses hír(forrás) is elfogult.⁵⁷

A helyzet tehát az, hogy nem csupán az internetes vagy a közösségi oldalakon történő hírfogyasztás lesz polarizált, hanem az egész „hírmédia” is átalakul, a televíziós csatornák, a sajtótermékek és az online sajtó is ideológiák által meghatározott módon működnek.⁵⁸ Ez azonban nem menti fel az online platformokat a felelősség alól, a közösségi médiában található robotok és buborékok ugyanis olyan potenciálisan példátlan kockázatokat jelentenek, amelyekkel más típusú médiában – televízióban

⁵⁰ Podlas (2022): i. m. 2240.

⁵¹ Podlas (2022): i. m. 2232.

⁵² Podlas (2022): i. m. 2241.

⁵³ Podlas (2022): i. m. 2238.

⁵⁴ Podlas (2022): i. m. 2247.

⁵⁵ Madhura Bhandarkar: Legality of Social Media Algorithms: How They Shape Our Minds and Democracy. *International Journal of Law Management & Humanities*, 4. (2021), 1. 1919.

⁵⁶ Kirill Pogorelskiy – Matthew Shum: *News We Like to Share: How News Sharing on Social Networks Influences Voting Outcomes*. 2019. 3.

⁵⁷ Pogorelskiy – Shum (2019): i. m. 5.

⁵⁸ Podlas (2022): i. m. 2243.

vagy rádióban – nem találkozhatunk. Ezek a megnövekedett kockázatok abból adódnak, hogy a közösségimédia-hálózatok milyen sebességgel és gyakorisággal képesek terjeszteni és felerősíteni a rossz minőségű tartalmakat és pontatlan információkat.⁵⁹ A Facebook, a Twitter és más platformok rangsorolásának, moderálásának, szűrésének, eltávolításának és monetizálási politikájának mértéke egyértelműen szerkesztői felelősséghez kezd hasonlítani, ennek eredményeként pedig a hírek egyre inkább polarizáltak, mivel a meghökkentő, sokkoló hírek és az ezek által létrejött interakciók az online platformokon tartják az embereket.⁶⁰ Az újságíróknak ma már inkább az az érdekük, hogy minél több interakció legyen egy cikkhez kapcsolódóan, nem az, hogy az a cikk minőségi újságírás terméke legyen.⁶¹ A legtöbb interakció, komment azonban a legtöbbször a hatásvadász, sokszor pontatlan cikkekre érkezik, amelyek pont úgy vannak megfogalmazva, hogy heves érzelmi reakciókat váltsanak ki.⁶² Mindezek mellett pedig az is egyértelműen azonosítható, hogy az emberek médiába vetett bizalma folyamatosan csökken, köszönhetően annak, hogy ma már voltaképpen bárki lehet újságíró,⁶³ ennek kapcsán pedig vannak olyan újságírók, akik szerint egyenesen az van veszélyben, hogy valaha beszélhetünk-e még tényszerűen tájékoztatható közönségről.⁶⁴

Mit tehetünk a buborékok ellen?

Viszonylag széles körben elterjedt nézet, hogy az internet párhuzamos nyilvánosságokat hozott létre.⁶⁵ Ennek egyik eredménye, hogy a felhasználók különböző csoportjai merőben eltérő tartalmakat látnak, ezáltal egyre kevesebb a megjelenő információk közötti átfedés, és egyre kevesebb lesz a közös társadalmi tapasztalat. Ezek nélkül pedig egy heterogén társadalomnak sokkal nehezebb dolga lesz a társadalmi problémák kezelésében. Az emberek egymást különbözőnek, idegennek, sőt akár ellenségnek is tekinthetik emiatt, ezáltal pedig még mélyebb szakadék alakulhat ki a társadalmon belül.⁶⁶

Még ha a fent kifejtettek alapján nem is teljesen igaz, hogy mindez az online platformoknak köszönhető – hiszen nem csupán az internet hozta létre a párhuzamos nyilvánosságokat –, az semmiképp sem jelenthető ki, hogy az internet és az online

⁵⁹ Lee (2019): i. m. 791.

⁶⁰ Oranburg (2022): i. m. 610.

⁶¹ Carroll (2017): i. m. 70.

⁶² Vo (2020): i. m. 405.

⁶³ Carol Pauli: The “End” Of Neutrality: Tumultuous Times Require a Deeper Value. *Cardozo Journal of Conflict Resolution*, 23. (2022), 3. 566.

⁶⁴ Pauli (2022): i. m. 557.

⁶⁵ Vo (2020): i. m. 400.

⁶⁶ Cass Sunstein: Is Social Media Good or Bad for Democracy? *International Journal on Human Rights*, 15. (2018), 27.

platformok pusztán tétlen és ártatlan szemtanúi lettek volna ennek a folyamatnak. Az online platformok ugyanis, még ha nem is maguk hozták létre, mélyítik és fenn tartják a társadalmi polarizálódás folyamatát, és jogosan elvárható, hogy a rendelkezésükre álló eszközökkel fellépjenek ez ellen. Az online platformok és a közösségi média szabályozásának kérdése komplex, összetett kérdés,⁶⁷ ezen a helyen pusztán a szűrőbuborékok és visszhangkamrák folyamata elleni fellépésről kívánok írni.

A közösségi oldalak, mint új városközpontok, amelyeken minden egyes felhasználónak saját kis szónoki emelvénye (az amerikai szóhasználatban „szappanos doboza”) van,⁶⁸ merőben új szabályozást és felfogást igényelnek. Tekintettel arra, hogy globálisan működő platformok, a hatékony szabályozást – főként, de nem kizárólag – országokon átívelő formában kell keresni. Az Európai Unió az utóbbi években felismerte az online platformok jelentette veszélyeket, és különböző eszközökkel igyekszik orvosolni a problémát. Ezek között az eszközök között találunk önszabályozó kódexeket,⁶⁹ irányelveket⁷⁰ és rendeleteket⁷¹ is, de a legjelentősebb változást a digitális szolgáltatásokról szóló rendelet⁷² jelenti. A jogszabály különböző átláthatósági és garanciális szabályok bevezetésével számos ponton jelent előrelépést a jelenlegi helyzethez képest, és mindenképp üdvözlendő erőfeszítésnek tekinthető.

A DSA szövege nem tartalmazza a szűrőbuborék vagy visszhangkamra kifejezéseket, azonban azonosítja és bizonyos mértékben szabályozza az online platformok tartalomajánló rendszereit. A rendelet értelmében ajánlórendszernek minősül minden „teljes mértékben vagy részben automatizált rendszer, amelyet az online platform arra használ, hogy az online interfészén konkrét információkat javasoljon vagy ezeket az információkat rangsorolja a szolgáltatás igénybe vevője számára, többek között a szolgáltatás igénybe vevője által indított keresés alapján vagy egyéb módon meghatározva a megjelenített információk relatív sorrendjét vagy elsőbbségét”.⁷³ Mindezek alapján tehát a felhasználókat buborékba záró algoritmusok ilyen

⁶⁷ Erről lásd részletesen: Papp János Tamás: *A közösségi média szabályozása a demokratikus nyilvánosság védelmében*. Budapest, Wolters Kluwer, 2022.

⁶⁸ Rachel Casey: John Stuart Mill and Social Media: Evaluating the Ethics of De-Platforming. *University of Central Florida Department of Legal Studies Law Journal*, 4. (2021). 33.

⁶⁹ Például Európai Bizottság: *A dezinformáció visszaszorítását célzó uniós gyakorlati kódex megerősítése*.

⁷⁰ Például Az Európai Parlament és a Tanács (EU) 2017/541 irányelve (2017. március 15.) a terrorizmus elleni küzdelemről, a 2002/475/IB tanácsi kerethatározat felváltásáról, valamint a 2005/671/IB tanácsi határozat módosításáról. L 88/6. (2017. március 31.); Az Európai Parlament és a Tanács (EU) 2019/790 irányelve (2019. április 17.) a digitális egységes piacon a szerzői és szomszédos jogokról, valamint a 96/9/EK és a 2001/29/EK irányelv módosításáról. L 130/92. (2019. május 17.).

⁷¹ Például P2B–Az Európai Parlament és a Tanács (EU) 2019/1150 rendelete (2019. június 20.) az online közvetítő szolgáltatások üzleti felhasználói tekintetében alkalmazandó tisztességes és átlátható feltételek előmozdításáról. L 186/57. (2019. július 11.).

⁷² Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (2022. október 19.) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (digitális szolgáltatásokról szóló rendelet). L 277/1. (2022. október 27.) (DSA).

⁷³ DSA 3. cikk s) pont.

ajánlórendszernek minősülnek, akár keresési találatokról, akár konkrét tartalmak kiajánlásáról, akár csak bármilyen tartalom megjelenítésének relatív sorrendjéről van szó. Az ilyen ajánlórendszerek paramétereit világosan és minden felhasználó számára érthetően meg kell határozni a felhasználási feltételekben,⁷⁴ ha pedig több ilyen ajánlási módszert is alkalmaz a platform, biztosítani kell a felhasználó számára a választási lehetőséget.⁷⁵ Vagyis a felhasználók rendelkezésére kell bocsátani azokat az információkat, amelyek magyarázatot adnak arra, hogy miért az adott információt ajánlják számára, azaz hogy mik azok a kritériumok, amelyek az ajánlások szempontjából a legjelentősebbek.⁷⁶ Az online óriásplatformot üzemeltető szolgáltatóknak pedig mindezekon felül biztosítaniuk kell egy olyan opciót is, amely mindenféle profilkészítés és tartalomrendezési folyamat nélkül közvetíti az információkat a felhasználóknak.⁷⁷ Mindezekon kívül a platformoknak biztosítaniuk kell az algoritmusaik⁷⁸ és hirdetési rendszereik átláthatóságát,⁷⁹ valamint bizonyos akkreditált kutatóknak hozzáférést kell adniuk további adatokhoz az ajánlórendszerekkel (is) kapcsolatban.⁸⁰ Mindezek közvetlen hatást nem tudnak gyakorolni, ezáltal nem is jelenthetnek egyértelmű megoldást a buborékhatások jelenségére, mégis hozzájárulhatnak a tudatos, tájékozott felhasználók hatékonyabb információfogyasztásához, valamint a kutatók számára a különböző ajánlási folyamatok megismeréséhez.

A DSA azonban más módon is igyekszik garantálni a kevésbé tudatos felhasználók tartalomfogyasztási lehetőségeit. Külön kikötés, hogy az online platformot üzemeltető szolgáltatók nem alakíthatják ki vagy üzemeltethetik felületeiket oly módon, amely „megtéveszti vagy manipulálja a szolgáltatásaikat igénybe vevőket, vagy más módon lényegesen torzítja vagy gyengíti a szolgáltatásaikat igénybe vevők szabad és tájékozott döntéshozatalra való képességét”.⁸¹ Az online óriásplatformoknak észszerű, arányos és hatékony kockázatcsökkentési intézkedéseket kell bevezetniük az általuk azonosított rendszerszintű kockázatok kezelése érdekében,⁸² amelyekbe beletartozhat akár a társadalmi polarizáltság vagy radikalizálódás esete is.

Mindezek mellett különösen érdekesek a DSA azon rendelkezései is, amelyek az óriásplatformok tömegtájékoztatásra vonatkozó szerepével kapcsolatosak. Az online óriásplatformot üzemeltető szolgáltatóknak például „különösen kellő figyelmet kell fordítaniuk a véleménynyilvánítás és a tájékozódás szabadságára, beleértve

⁷⁴ DSA 27. cikk (1) bekezdés.

⁷⁵ DSA 27. cikk (3) bekezdés.

⁷⁶ DSA 27. cikk (2) bekezdés.

⁷⁷ DSA 38. cikk.

⁷⁸ DSA 69. cikk.

⁷⁹ DSA 26. cikk.

⁸⁰ DSA 40. cikk.

⁸¹ DSA 25. cikk.

⁸² DSA 35. cikk.

a tömegtájékoztatás szabadságát és sokszínűségét is”,⁸³ valamint kockázatelemzéseik során „azonosítani kell és fel kell lépni a tömegtájékoztatás szabadságát és sokszínűségét veszélyeztető körülmények ellen” is.⁸⁴ Ezen rendelkezések tehát a tömegtájékoztatás sokszínűségének megőrzését és garantálását követelik meg a platformoktól, biztosítva ezzel többek között a kiegyensúlyozott tömegtájékoztatás eléréséhez szükséges eszközöket. Ez a megoldási javaslat azon az elven nyugszik, amely szerint sokszínű tartalmakkal csökkenthető a polarizáció.⁸⁵ Sok e témával foglalkozó kutató azon az állásponton van, hogy az egyéni szűrőbuborék „kipukkasztása” szükségszerűen javítja a társadalom helyzetét azáltal, hogy informatívabb egyéni döntéseket tesz lehetővé. A hagyományos média elfogultságát is figyelembe véve azonban az összkép bonyolultabbá válik, és a fenti következtetés nem biztos, hogy megállja a helyét. Ez ugyanis figyelmen kívül hagyja az úgynevezett ellenséges hírrel szembeni elfogultság (*hostile news bias*) jelenségét, amely alapján hiába létezik az elképzelés, mely szerint a szűrőbuborékokat úgy lehet semlegesíteni, hogy bejuttatunk beléjük másfajta híreket, a kutatások szerint a felhasználók azokat az egyébként semleges, objektív információkat, amelyek ellentmondanak a világnézetüknek, ellenségesnek tekintik, és elutasítják azokat.⁸⁶

Kiindulópontként a legalapvetőbb előírás az lehet, ha a platformoknak tartózkodniuk kell a nyilvánosság algoritmusok útján történő befolyásolásától. Ezáltal némiest csökkenthető az implicit perszonalizáció az online térben, kérdéses azonban, hogy mit lehet kezdeni az explicit perszonalizáció jelenségével. Elvárható-e, hogy egy online platform akár a felhasználó saját preferenciái és beállításai ellenére is sokszínű tartalmat ajánljon fel a felhasználónak? A sokszínű tájékoztatás kérdése a hagyományos média kapcsán is rendszeres viták alapját képezi, az online térben pedig meghatározódnak az ehhez kapcsolódó gyakorlati jellegű problémák. Mi alapján mérhető a sokszínűség? Melyek azok az indikátorok, amelyek egy online platform kapcsán segítenek eldönteni azt a kérdést, hogy vajon az általa nyújtott szolgáltatás megfelel-e a sokszínű tömegtájékoztatás feltételeinek? Egyáltalán mit jelent pontosan a sokszínű tömegtájékoztatás az online térben? Nyilvánvaló, hogy lehetetlen elvárás egy online platformmal szemben, hogy patikamérlegben egyensúlyozza ki az egyes felhasználók elé tárt tartalmakat politikai elfogultság mentén, de akkor az előbb említett semlegességen túl mik azok a pozitív kívánalmak, amelyeket elvárhatunk a platformoktól? Mindezek mellett pedig ott van a következő nagy kérdés: a meghozott intézkedések ellenőrizhetősége is. Az online szolgáltatók és hirdetőik ugyanis olyan mértékben integrálták a személyre szabott technológiákat a felhasználói élménybe, hogy elveszítettük a számukra megjelenített információk

⁸³ DSA (47) preambulumbekkezdés.

⁸⁴ DSA 34. cikk.

⁸⁵ Katona Zsolt – Ron Berman: *Curation Algorithms and Filter Bubbles in Social Networks*. NET Institute Working Paper No. 16–08. 2016. 34.

⁸⁶ Podlas (2022): i. m. 2244.

objektív ellenőrzésének lehetőségét.⁸⁷ Míg egy hagyományos médiafolyam esetén mindenki ugyanazt látja – beleértve adott esetben a területet felügyelő hatóságokat is –, a közösségi médiában megjelenő tartalmak összetétele minden felhasználó esetében más, így voltaképpen lehetetlen központi, mindenhol általánosan érvényes tartalomfelügyeletet alkalmazni. Mára beléptünk a „hálózatalapú információs gazdaság” korába, ahol az információt általában decentralizáltan a felhasználók állítják elő, és mivel ez voltaképp ingyenesen megtehető, ezért nagyon nagy számban élnek is ezzel a lehetőséggel, ezáltal szinte ellenőrizhetetlen, hogy mi és hogyan jelenik meg minden egyes felhasználó esetén.⁸⁸

Látható, hogy a kérdés nem pusztán technológiai vagy jogi probléma, hanem mindkét szempontból megoldást igényel. A technológia ellen nem lehet pusztán korlátozásokkal vagy előírásokkal küzdeni, mivel növekedése elkerülhetetlen, a korlátozás pedig hamar irreálissá válhat.⁸⁹ A perszonalizáció, szűrőbuborék és visszhangkamrák kérdése nagyon szorosan érinti az egyéni felelősség kérdését is. Egy lehetséges jogi szabályozás esetében a jogalkotó által megválasztandó értékvalasztás valójában annak a felelősségi kérdésnek a visszhangja, amelyet minden állampolgárnak, a civil társadalom tagjának fel kell tennie magának.⁹⁰ A társadalomnak el kell tudnia dönteni, hogy hol húzható meg a határ az egyéni felelősség és az állami szabályozás által nyújtott védelem között. Sztítás Péter szerint is hiba a közösségi médiát minden rossz eredőjeként kezelni, hiszen ezzel végső soron levesszük a felelősséget az egyén válláról. Azt azonban ő is hozzáteszi, hogy végső soron a szűrőbuborékok jelensége növeli a társadalmi polarizációt, és ez nem marad hatás nélkül a demokráciák működésére sem.⁹¹ Vannak, akik szerint nem is a platformok oldaláról kellene kezelni a kérdést, hanem az újságírók felelősségét kell kihangsúlyozni, hiszen ma már, az algoritmusok korában megváltozott a sajtó szerepe, és egyre ritkább esetben szolgálnak a valódi, elfogulatlan tájékoztatás eszközeként.⁹² Stacy Strong szerint erőteljes interdiszciplináris folyamatra lesz szükség ahhoz, hogy visszafordítsák azokat a „pszichológiai, neurológiai és társadalmi folyamatokat”, amelyek miatt ennyire lecsökkent a médiába vetett bizalom.⁹³ Ehhez kapcsolódóan pedig Sue Robinson úgy érvel, hogy az előbb említett bizalomvesztés ellenére a sajtó megfelelő terepe lehet annak, hogy a több, párhuzamos valóságon

⁸⁷ Thomas Beretich: *How Online Tracking and the Filter Bubble Have Come to Define Who We Are*. 2013. 14.

⁸⁸ Giovanni Pitruzzella – Oreste Pollicino: *Disinformation and Hate Speech. A European Constitutional Perspective*. Milano, Bocconi University Press, 2020. 7.

⁸⁹ Bhandarkar (2021): i. m. 1923.

⁹⁰ Krzysztof Jankowski: *Living in the Filter Bubble. Is What We Lose Something We Need to Preserve?* Ottawa, University of Ottawa, Faculty of Law, 2014. 26.

⁹¹ Sztítás Péter: Filter buborékba zárva? *Barankovics Alapítvány*.

⁹² Carroll (2017): i. m. 73.

⁹³ S. I. Strong: Alternative Facts and the Post-Truth Society: Meeting the Challenge. *University of Pennsylvania Law Review*, 165. (2017), 1. 145.

keresztülnyúlva újra közös pontokat hozzanak létre az újságírók, és közös értékekre építve teremtsenek hidakat a különböző buborékok között.⁹⁴

Összefoglalásként elmondható, hogy bár a buborékok vagy visszhangkamrák léteznek, társadalmi jelentőségük és az általuk okozott lehetséges társadalmi károk valódiak, azonban az a gondolat, amely az online platformokat hibáztatja ezek kialakulásáért, nem igazolható tudományos kutatásokkal. A napjainkban is tapasztalható fokozódó társadalmi polarizálódás a hagyományos és az online média kölcsönös együttthatásaként alakult ki: az internetnek köszönhetően létrejött figyelemalapú médiakörnyezetben a hagyományos média egyre inkább véleményalapúvá vált, ezáltal megnőtt a személyes perszonalizáció lehetősége, amely folyamatot tovább erősített a közösségi média, aminek következtében a sajtó még inkább a kevésbé minőségi, de nagyobb interakciót eredményező, polarizált tartalom-előállítás irányába mozdult el. Az így létrejött ördögi kör nagyon nehezen kezelhető, a legalkalmasabb eszköz talán a minőségi, objektív újságírói tartalmak előállításának támogatása lehet, ami által nehezebbé válik a párhuzamos nyilvánosságok elkülönítésének fenntartása. A minőségi tartalmak előállítása és terjesztése talán az egyén által alkalmazott, explicit perszonalizáció lehetőségét is csökkentheti, hiszen kiegyensúlyozott és hiteles információk közül nehezebb személyre szabottan válogatni. Ezáltal talán a médiába vetett bizalom is növelhető lenne, és esetleg újra lehetségessé válna a kizárólag véleményen és meggyőződésen alapuló társadalmi diskurzusoktól inkább a tényeken alapuló demokratikus viták felé tenni pár lépést.

Felhasznált irodalom

- Ananny, Mike – Kate Crawford: A Liminal Press. Situating News App Designers within a Field of Networked News Production. *Digital Journalism*, 3. (2015), 2. 192–208. Online: <https://doi.org/10.1080/21670811.2014.922322>
- Az Európai Parlament és a Tanács (EU) 2017/541 irányelve (2017. március 15.) a terrorizmus elleni küzdelemről, a 2002/475/IB tanácsi kerethatározat felváltásáról, valamint a 2005/671/IB tanácsi határozat módosításáról. L 88/6. (2017. március 31.)
- Az Európai Parlament és a Tanács (EU) 2019/1150 rendelete (2019. június 20.) az online közvetítő szolgáltatások üzleti felhasználói tekintetében alkalmazandó tisztességes és átlátható feltételek előmozdításáról. L 186/57. (2019. július 11.)
- Az Európai Parlament és a Tanács (EU) 2019/790 irányelve (2019. április 17.) a digitális egységes piacon a szerzői és szomszédos jogokról, valamint a 96/9/EK és a 2001/29/EK irányelv módosításáról. L 130/92. (2019. május 17.)
- Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (2022. október 19.) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (digitális szolgáltatásokról szóló rendelet). L 277/1. (2022. október 27.)

⁹⁴ Sue Robinson: Crisis of Shared Public Discourses: Journalism and How It All Begins and Ends with Trust. *Journalism*, 20. (2018), 1. 58.

- Bajomi-Lázár Péter: Manipulál-e a média? *Médiakutató*, 18. (2017), 4. 61–79.
- Bakshy, Eytan – Solomon Messing – Lada A. Adamic: Exposure to Ideologically Diverse News and Opinion on Facebook. *Science*, 348. (2015), 6239. 1130–1132. Online: www.science.org/doi/10.1126/science.aaa1160
- Barberá, Pablo – John T. Jost – Jonathan Nagler – Joshua A. Tucker – Richard Bonneau: Tweeting From Left to Right: Is Online Political Communication More Than an Echo Chamber? *Psychological Science*, 26. (2015), 10. 1531–1542.
- Benson, Sara J.: @PublicForum: The Argument for a Public Forum Analysis of Government Officials' Social Media Accounts. *Washington University Jurisprudence Review*, 12. (2019), 1. 85–114. Online: https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1207&context=law_jurisprudence
- Beretich, Thomas: *How Online Tracking and the Filter Bubble Have Come to Define Who We Are*. 2013. Online: <https://ssrn.com/abstract=2878750>
- Bernal, Paul: *The Internet, Warts and All*. Cambridge, Cambridge University Press, 2018.
- Bhandarkar, Madhura: Legality of Social Media Algorithms: How They Shape Our Minds and Democracy. *International Journal of Law Management & Humanities*, 4. (2021), 1. 1912–1924. Online: <http://doi.org/10.1732/IJLMH.25952>
- Bruns, Axel: Filter Bubble. *Internet Policy Review*, 8. (2019a), 4. Online: <https://doi.org/10.14763/2019.4.1426>
- Bruns, Axel: *It's Not the Technology, Stupid: How the 'Echo Chamber' and 'Filter Bubble' Metaphors Have Failed Us*. Brisbane, Digital Media Research Centre (QUT), 2019b. Online: <http://snurb.info/files/2019/It's%20Not%20the%20Technology%2C%20Stupid.pdf>
- Carroll, Erin C.: Making News: Balancing Newsworthiness and Privacy in the Age of Algorithms. *Georgetown Law Journal*, 106. (2017), 1. 69–114.
- Casey, Rachel: John Stuart Mill and Social Media: Evaluating the Ethics of De-Platforming. *University of Central Florida Department of Legal Studies Law Journal*, 4. (2021). 15–34.
- Ciampaglia, Giovanni Luca – Filippo Menczer: Misinformation and Biases Infect Social Media, Both Intentionally and Accidentally. *The Conversation*, 2018. június 20. Online: <https://theconversation.com/misinformation-and-biases-infect-social-media-both-intentionally-and-accidentally-97148>
- Dubois, Elizabeth – Grant Blank: The Echo Chamber Is Overstated: The Moderating Effect of Political Interest and Diverse Media. *Information, Communication & Society*, 21. (2018). 5. 729–745. Online: <https://doi.org/10.1080/1369118X.2018.1428656>
- Dutto, William H. – Bianca Reisdorf – Elizabeth Dubois – Grant Blank: *Social Shaping of the Politics of Internet Search and Networking: Moving Beyond Filter Bubbles, Echo Chambers, and Fake News*. Quello Center Working Paper No. 2944191. Online: <http://dx.doi.org/10.2139/ssrn.2944191>
- Európai Bizottság: *A dezinformáció visszaszorítását célzó uniós gyakorlati kódex megerősítése*. Online: https://ec.europa.eu/info/strategy/priorities-2019-2024/new-push-european-democracy/european-democracy-action-plan/strengthened-eu-code-practice-disinformation_hu
- Fitzpatrick, Neill: Media Manipulation 2.0: The Impact of Social Media on News, Competition, and Accuracy. *Athens Journal of Mass Media and Communications*, 4. (2018), 1. 45–62. Online: <https://doi.org/10.30958/ajmmc.4.1.3>
- Fletcher, Richard: The Truth Behind Filter Bubbles: Bursting Some Myths. *Reuters Institute for the Study of Journalism*, 2020. január 24. Online: <https://reutersinstitute.politics.ox.ac.uk/news/truth-behind-filter-bubbles-bursting-some-myths>
- Gálík Mihály: Visszhangkamrák és szűrőbuborékok. A hírfogyasztásról szóló vita a digitális hálózati média-ökoszisztéma világában. *Médiakutató*, 21. (2020), 1. 27–35.

- Gillespie, Tarleton: The Politics of 'Platforms'. *New Media & Society*, 12. (2010), 3. 347–364. Online: <https://doi.org/10.1177/1461444809342738>
- Gillespie, Tarleton: The Relevance of Algorithms. In Tarleton Gillespie – Pablo J. Boczkowski – Kirsten A. Foot (szerk.): *Media Technologies. Essays on Communication, Materiality, and Society*. Cambridge, MA, The MIT Press, 2014. Online: <https://doi.org/10.7551/mitpress/9780262525374.003.0009>
- Grafanaki, Sofia: Platforms, the First Amendment and Online Speech: Regulating the Filters. *Pace Law Review*, 39. (2018), 1. 111–162. Online: <https://doi.org/10.58948/2331-3528.1987>
- Hours of Video Uploaded to YouTube Every Minute. *Statista*, 2022. április 4. Online: www.statista.com/statistics/259477/hours-of-video-uploaded-to-youtube-every-minute/
- Jankowski, Krzysztof: *Living in the Filter Bubble: Is What We Lose Something We Need to Preserve?* Ottawa, University of Ottawa, Faculty of Law, 2014. Online: <http://dx.doi.org/10.2139/ssrn.2982025>
- Katona, Zsolt – Ron Berman: *Curation Algorithms and Filter Bubbles in Social Networks*. NET Institute Working Paper No. 16-08. 2016. Online: <https://ssrn.com/abstract=2848526>
- Lee, Katrina: Your Honor, on Social Media: The Judicial Ethics of Bots and Bubbles. *Nevada Law Journal*, 19. (2019), 3. Online: <https://scholars.law.unlv.edu/nlj/vol19/iss3/4>
- Maggen, Daniel: Law In, Law Out: Legalistic Filter Bubbles and the Algorithmic Prevention of Nonconsensual Pornography. *Cardozo Law Review*, 43. (2022), 5. 1747–1805.
- Moeller, Judith – Natali Helberger: *Beyond the Filter Bubble: Concepts, Myths, Evidence and Issues for Future Debates*. Amsterdam, University of Amsterdam, 2018. Online: https://pure.uva.nl/ws/files/29285427/beyond_the_filter_bubble_concepts_myths_evidence_and_issues_for_future_debates_1_.pdf
- Oranburg, Seth: Social Media and Democracy after the Capitol Riot, or, A Cautionary Tale of the Giant Goldfish. *Mercer Law Review*, 73. (2022), 2. 591–613.
- Papp János Tamás: *A közösségi média szabályozása a demokratikus nyilvánosság védelmében*. Budapest, Wolters Kluwer, 2022.
- Pariser, Eli: *The Filter Bubble. How the New Personalized Web Is Changing What We Read and How We Think*. New York, Penguin Publishing, 2012.
- Pariser, Eli: Did Facebook's Big Study Kill My Filter Bubble Thesis? *Wired*, 2015. május 7. Online: www.wired.com/2015/05/did-facebooks-big-study-kill-my-filter-bubble-thesis
- Pauli, Carol: The "End" of Neutrality: Tumultuous Times Require a Deeper Value. *Cardozo Journal of Conflict Resolution*, 23. (2022), 3. 557–571.
- Pitruzzella, Giovanni – Oreste Pollicino: *Disinformation and Hate Speech. A European Constitutional Perspective*. Milano, Bocconi University Press, 2020.
- Podlas, Kimberlianne: Reconsidering the Nomos in Today's Media Environment. *Touro Law Review*, 37. (2022), 4. 2211–2252.
- Pogorelskiy, Kirill – Matthew Shum: *News We Like to Share: How News Sharing on Social Networks Influences Voting Outcomes*. 2019. Online: <http://dx.doi.org/10.2139/ssrn.2972231>
- Political Bias on Social Media Emerges from Users, Not Platform, IU Study Says. *Indiana University*. Online: <https://research.impact.iu.edu/key-areas/social-sciences/stories/social-media-platform-bias.html>
- Robinson, Sue: Crisis of Shared Public Discourses: Journalism and How It All Begins and Ends with Trust. *Journalism*, 20. (2018), 1. 56–59. Online: <https://doi.org/10.1177/1464884918808958>
- Stark, Birgit – Daniel Stegmann – Melanie Magin – Pascal Jürgens: *Are Algorithms a Threat to Democracy? The Rise of Intermediaries: A Challenge for Public Discourse*. Algorithm Watch, 2020.

- Online: <https://algorithmwatch.org/en/wp-content/uploads/2020/05/Governing-Platforms-communications-study-Stark-May-2020-AlgorithmWatch.pdf>
- Strong, S. I.: Alternative Facts and the Post-Truth Society: Meeting the Challenge. *University of Pennsylvania Law Review*, 165. (2017), 1. 137–146.
- Sunstein, Cass R.: *Republic.com*. Princeton, Princeton University Press, 2001.
- Sunstein, Cass R.: The Law of Group Polarization. *The Journal of Political Philosophy*, 10. (2002), 2. 175–195.
- Sunstein, Cass R.: *Republic.com 2.0*. Ford. Veres Péter. Budapest, Wolters Kluwer, 2013.
- Sunstein, Cass R.: *#Republic: Divided Democracy in the Age of Social Media*. Princeton, Princeton University Press, 2017.
- Sunstein, Cass: Is Social Media Good or Bad for Democracy? *International Journal on Human Rights*, 15. (2018), 27. Online: <https://sur.conectas.org/en/is-social-media-good-or-bad-for-democracy/>
- Szítás Péter: Filter buborékba zárva? *Barankovics Alapítvány*. Online: <https://barankovics.hu/filter-buborekba-zarva/>
- Török Bernát – Rab Árpád – Szikora Tamás: *Internetes attitűdök – Régióink és a világháló*. Budapest, NKE Információs Társadalom Kutatóintézet, 2020. Online: www.ludovika.hu/wp-content/uploads/2020/12/EJJK_ITKI_Kozep-Europa_kutatasi_jelentes_v.pdf
- Veszelszki Ágnes: deepFAKEnews: Az információmanipuláció új módszerei. In Balázs László (szerk.): *Digitális kommunikáció és tudatosság*. Budapest, Hungarovox Kiadó, 2021. 93–105.
- Vikje-Freiberg, Vaira – Herta Däubler-Gmelin – Ben Hammersley – Luís Miguel Poiars Pessoa Maduro: *A Free and Pluralistic Media to Sustain European Democracy*. The Report of the High Level Group on Media Freedom and Pluralism, 2013.
- Vo, Lam Thuy: How the Internet Created Multiple Publics. *Georgetown Law Technology Review*, 4. (2020), 2. 399–412.
- Woolley, Samuel C. – Philip N. Howard (szerk.): *Computational Propaganda. Political Parties, Politicians, and Political Manipulation on Social Media*. New York, Oxford University Press, 2018.
- Zuiderveen Borgesius, Frederik J. – Damian Trilling – Judith Moeller – Balazs Bodo – Claes de Vreese – Natali Helberger: Should We Worry About Filter Bubbles? *Internet Policy Review*, 5. (2016), 1. Online: <https://doi.org/10.14763/2016.1.401>

Vákát

A pluralizmus érvényesülése a tömegtájékoztatás piacán



Az állampolgárok tömegtájékoztatása kizárólag akkor minősíthető kétséget kizáróan sokszínűnek, ha a társadalmi nyilvánosságban szerepet vállaló médiapiaci szereplők mind a külső pluralizmus, mind a belső pluralizmus követelményének teljesülésére tekintettel vannak. A tájékoztatás piacán megjelenő tartalmak sokszínűsége kétségtelenül a demokratikus közvélemény kialakulásához szükséges egyik legfőbb alapfeltétel.

A tájékoztatási piac struktúrája azonban az internet térhódításával és az ott alkalmazott új technológiákkal (például algoritmusok, szűrőbuborék alkalmazása) radikálisan megváltozott, valamint folyamatosan változik. Az online platformszolgáltatók tevékenységére irányadó „tartalomszabályozás” világszerte gyerekcipőben jár, továbbá felmerültek olyan jogsértések és anomáliák, amelyekre az államok szabályozása és felügyeleti tevékenysége nem tudott időben reagálni, az érintett vállalatok pedig időközben saját önálló normarendszerrel magánszabályozási folyamatot indítottak el. Mindezeket figyelembe véve a jogalkotó számára jelenleg egy hatékonyan működő demokratikus médiarendszeri modell kialakítása kihívást jelent, hiszen az eddig már ismert médiapiacot és sajtót illető általános fogalmak jelentéstartalmai sem egyértelműek. A tájékoztatási piacon jelentkező változásokra tekintettel szükséges tehát újfent megvizsgálni, hogy az Alaptörvényben deklarált demokratikus közvélemény kialakulásához szükséges pluralizmus, mint alapfeltétel, milyen mértékben, milyen feltételekkel érvényesülhet a tartalomterjesztés innovációja következtében.

Bevezetés

Magyarországon a médiaszektorra vonatkozóan az utóbbi évtizedben megalkotott kulcsfontosságú jogszabályok rendelkezései, a médiaszolgáltatásokról és a tömegkommunikációról szóló 2010. évi CLXXXV. törvény (médiatörvény), illetve a sajtószabadságról és a médiatartalmak alapvető szabályairól szóló 2010. évi CIV. törvény (médiaközlöny) kialakítottak egy olyan, törekvő demokratikus médiarendszert, amely az Alaptörvénybe foglalt véleménynyilvánítás szabadságára és a kapcsolódó alapjogok tartalmára tekintettel a médiapiac jellegzetességeire reagált. A hagyományos médiatartalom-szolgáltatásokat tekintve hangsúlyosan lépett elő az a kritérium, hogy az állampolgárok milyen mértékben tájékozódhatnak e tekintetben több forrásból, továbbá ezen források és a média által szolgáltatott tartalmak kapcsán a belső, valamint külső pluralizmus is porondra került. Az előzőek érvényesülése újabb közigazgatási jogintézmények bevezetésével részben követhetővé, „mérhetővé”

vált a médiapiacra, ennek ellenére a tömegtájékoztatásban napjainkban domináns szerepet vállaló platformszolgáltatókról a kritériumok teljesülése tekintetében ez nem mondható el. A magánszabályozást alkalmazó platformszolgáltatók normái a felhasználási feltételeiken és további elenyésző mértékben közzétett dokumentumaikon keresztül felületesen ismerhetők meg, teljes mértékben nem kifürkészhetők, a műveleteket végző algoritmusokba rejtett parancsok – főként a szolgáltatók gazdasági érdekei miatt – nem nyilvánosak.

Az Európai Unió Alapjogi Chartájának 11. cikke specifikusan megjelölt, kötelezett alany hozzárendelése nélkül meghatározza, hogy a tömegtájékoztatás szabadságát és sokszínűségét tiszteletben kell tartani. Ennek megfelelően a tájékoztatási piac sokszínűségének vizsgálata a szolgáltatásnyújtás engedélyezése, korlátozhatósága tekintetében az Európai Unió Bírósága (EUB) előtt is vizsgálendő körülménynek, közérdeken alapuló kényszerítő indoknak minősül. Az EUB a kapcsolódó ügyekben azt elemzi, hogy egy tagállam által alkalmazott intézkedés a tömegtájékoztatás sokszínűségéhez kapcsolódó közérdekű cél megvalósításának biztosítására, avagy korlátozására mennyiben alkalmas, ítélkezési gyakorlata szerint a fórum elfogadja, hogy a tömegtájékoztatás sokszínűségének tiszteletben tartására irányuló cél megvalósítása tekintetében mérlegelési mozgásteret kell biztosítani a tagállamok számára.¹ Ahhoz azonban, hogy bármilyen módon és mértékben követelményként lehessen meghatározni a sokszínűséget minden tömegtájékoztatást megvalósító szolgáltatás tekintetében, feltételezni szükséges, hogy létezik tájékoztatáshoz való jog, hiszen a pluralizmus a tájékoztatási tevékenységhez köthetően a jogalkotásban már minőségi feltételként fogalmazódik meg. Kit illet meg ez a jog? Egy tagállam állampolgárait, az uniós polgárokat? A tájékoztatási piaci szereplőket? Mi a „jogosultság” pontos tartalma, mi több, jelentősége, továbbá ha tagadnánk ezen „jog” létezését, az vajon milyen hatással lenne a demokráciára? Ezen kérdésekre keresem a választ a következőkben.

Emberi jogok, alapvető jogok, tájékoztatáshoz való jog

Az alkotmányos emberi jogok tekintetében kijelenthető, jelen társadalmunkat és annak fejlődési irányát alapjaiban változtatta meg, hogy elődeink felismerték azok létjogosultságát, valamint megformálták tartalmuk fő körvonalait, hangsúlyozták jelentőségüket. Mégis fontos megjegyezni, hogy rendeltetésük betöltése szempontjából deklarációjuk, alkotmányos szintre emelésük sajnos nem elegendő. Alapjogi minőségükben főként csak szigorú irányt mutatnak a jogalkotó, jogalkalmazó

¹ Lásd például: A C-250/06. sz. United Pan-Europe Communications Belgium SA és társai kontra belga állam ügyben 2007. december 13-án hozott ítélet; A C-555/19. sz. a Fussl Modestraße Mayr GmbH kontra SevenOne Media GmbH és társai ügyben 2021. február 3-án hozott ítélet.

számára tevékenységük gyakorlása során, az egyén számára pedig viszonyítási pontot jelentenek a társadalmi együttélés alapvetései tekintetében, továbbá egyértelművé teszik számukra, hogy milyen jogosultságok illetik őket meg hivatalos fórumok előtt, és egymás közötti viszonyaikban mire hivatkozhatnak. Az emberi jogoknak azonban a közigazgatásban, annak szabályozásában, mindennapi működésében is jelen kell lenniük ahhoz, hogy tartalmuk, funkciójuk ténylegesen érvényt szerezzen a társadalomban. Ez utóbbi értelmezés gyakorlatorientált megközelítést szorgalmaz; azt mutatja meg, hogy deklarációjuk kevés – a természetjogi szemléletet igazolva a tartalmuk iránti igény egy demokratikus szférában anélkül is fellépne –, a technológia fejlődésével inkább már jogrendszerekben való alkalmazásuk, és érvényesülésük intézkedésekkel történő elősegítése a lényegesebb, vizsgálandó szempont. Az Alkotmánybíróság – bár más tárgykörben, azonfelül az Alaptörvényt megelőző Magyar Köztársaság Alkotmányának értelmezése során hozott határozatában, de a mai napig releváns, alapjogok vonatkozásában tett indokolásában – megállapította: az állam kötelessége az egyéni alapvető jogokkal kapcsolatban nem merülhet ki abban, hogy a megsértésüktől tartózkodik, hanem magában foglalja azt is, hogy gondoskodnia kell az érvényesülésükhöz szükséges feltételekről.² Hazánkban a jogalkotó ezen kötelezettségének tett eleget, amikor az Alaptörvény IX. cikk (2) bekezdésébe foglalta, hogy Magyarország elismeri és védi a sajtó szabadságát, sokszínűségét, valamint biztosítja a demokratikus közvélemény kialakulásához szükséges szabad tájékoztatás feltételeit. Az Alkotmánybíróság szintén egy korábbi ítéletében azt is megállapította, hogy három, egymással szorosan összefüggő, egymást feltételező tényező sorolható a véleménynyilvánítás szabadságának az alkotmányos védelmi körébe; az egyéni véleménynyilvánítás lehetősége, a saját törvényei szerint kialakuló közvélemény, továbbá a minél szélesebb tájékozottságra épülő egyéni véleményalkotás lehetősége.³ Minden olyan tartalom ugyanis, amely a véleménynyilvánítás hatálya alá sorolható, relevanciával rendelkezik a demokratikus közvélemény alakulása szempontjából, és közös halmazt alkot.⁴

Egy képvisleti demokráciában a közvetlen népuralmi hatalomgyakorláshoz közeledés szándékaként, és így az intézmény egyes hiányosságait kiküszöbölve az egyik legfőbb alkalmazott korrekciós eszköz a plurális tömegtájékoztatás.⁵ Utóbbi demokratikus funkciójának a biztosítója, hogy működése a sokszínűség elvén alapul, attól függetlenül, hogy a tájékoztatási jellegű információ előállítására, közzétételére, megosztására a szolgáltató milyen módozatot vagy eszközt választ. Az alkotmányos szintre emelt emberi jogok és a pluralizmus érvényesülése tekintetében azonban

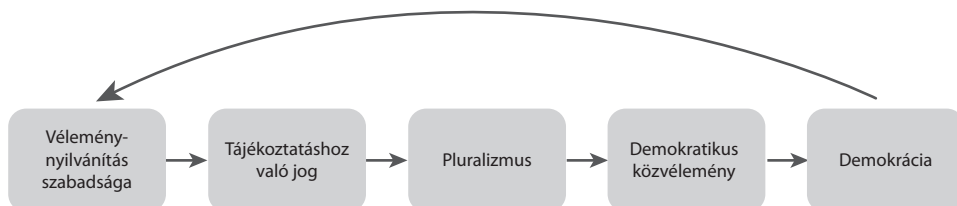
² A Magyar Köztársaság Alkotmánya (1949. évi XX. törvény); 32/1992. (V. 29.) AB határozat.

³ 30/1992. (V. 26.) AB határozat.

⁴ Török Bernát: *Szabaddan szólni, demokráciában. A szólásszabadság magyar doktrínája az amerikai jogirodalom tükrében*. Budapest, HVG-ORAC, 2018. 43–48.

⁵ Bihari Mihály – Pokol Béla: *Politológia*. Budapest, Nemzeti Tankönyvkiadó, 2009.

nemcsak az államnak van felelőssége, hanem az üzleti, vállalati szférának is. Ez az elmélet az emberi jogok felett az üzleti vállalkozások azon képességét veszi figyelembe, hogy vállalati hatalomként az egyének emberi jogainak megvalósulására, avagy visszafejlődésére szintén nagymértékű befolyással rendelkeznek.⁶



1. ábra: A tömegtájékoztatásra irányadó fő jogok és kötelezettségek, valamint a demokratikus hatalomgyakorlás összefüggései

Forrás: a szerző szerkesztése

Az előző okfejtést követve a fenti ábra azt ismerteti, hogy a véleménynyilvánítás szabadsága és említett alkotmányos védelmi köre, továbbá egy olyan, teljes körű, fikciós tájékoztatáshoz való jog, amelynek minden tájékoztatási tevékenységet végző piaci szereplő a kötelezettje és fogyasztó alany a jogosultja, illetve mindezek mellett a sokszínűség kötelezettségének teljesítésére törekvés mint feltételek fennállásának köszönhetően hogyan alakulhat ki a demokratikus közvélemény és a demokrácia. Ezen feltételként megjelenő jogosultsági elemek egyenként minden, az érvényesülési folyamatban részt vevő elemre hatással vannak, ugyanis abban az esetben, ha valamelyik felsorolt elem sérülne, kiesik, avagy nem teljes körű, a folytonosság és az érvényesülés láncolata megszakadhat, ezzel arányosan a demokratikus hatalomgyakorlás legitimitása bizonytalanabb, vitathatóbb lesz. *Ahol azonban demokratikus rezsim uralkodik, ott az emberi jogok tartalma is fejlődik, jobban kirajzolódik, létük pedig általánossá válik.*⁷ Az összefüggés egy legitim demokrácia és a tájékoztatáshoz való jog szükségessége között tagadhatatlan, még ha utóbbi jog egy fikciós tartalmú intézményt is vázol fel.

A médiaalkotmány 10. §-a a tájékoztatáshoz való jogot követelményként deklarálja a médiarendszer egésze tekintetében, tartalma azonban a fentebb felvázolt fikciós jogtól eltérő és önmagában nehezen megragadható. A rendelkezés szerint mindenkinek joga van arra, hogy megfelelően tájékoztassák a helyi, az országos és az európai közélet ügyeiről, emellett a Magyarország polgárai, a magyar nemzet tagjai számára jelentőséggel bíró eseményekről. A jogalkotó az értelmezési

⁶ David Birchall: Corporate Power over Human Rights: An Analytical Framework. *Business and Human Rights Journal*, 6. (2021), 1. 42–66.

⁷ Lásd Samuel P. Huntington: *A civilizációk összecsapása és a világrend átalakulása*. Ford. Gázsity Mila – Gecsényi Györgyi – Pusztai Dóra. Budapest, Európa Könyvkiadó, 2019. 316–319.

rendelkezőkben azt nem határozza meg, hogy mi minősül közéleti ügynek, sem azt, hogy mi minősülhet jelentőséggel bíró eseménynek, a médiarendszer egészére támaszkodva a piaci és közszolgálati szereplőkre, alkalmazott munkatársaik etikai és szakmai megítélésére bízva ezek tartalmi körét. Maga a (tömeg)tájékoztatáshoz való jog tartalmában azért érdekes a magyar jogrendszerben, mert bár jogosultságot sugall, inkább kötelezettséget testesít meg a médiatartalom-szolgáltatók felé. A kötelezettek köre mégsem fedi le a médiarendszer összes tájékoztatási tevékenységet nyújtó médiatartalom-szolgáltatóját.⁸

A tájékoztatáshoz való jog tehát nem általános alkotmányos emberi jog, hanem inkább a magyar médiaszabályozásban meghatározott olyan követelmény, amely az Alaptörvényben foglaltak szerinti demokratikus közvélemény kialakulását segíti elő. Ezt a funkciót közelebbről megvizsgálva főként politikai és szakmai értéket közvetít, ennek megfelelően a választópolgárok döntéshozatalában tölt be fontosabb szerepet. Voltaképpen minél több releváns, hírértékű információt közvetít a szakma, annál megalapozottabb lehet a választói döntés maga, amellyel arányban egy demokrácia legitimitása is erőteljesebb, ezenkívül a kötelezettség természetesen a fogyasztói kör magánérdekeit érintő, magánéletben hozott választásaira is hatványozottan pozitív hatással van. Nélkülözhetetlen kiemelni tehát a szakma felelősségét a Médiaalkotmányba foglalt rendelkezés vonatkozásában a tömegtájékoztatási rendszerben, hiszen a „hírérték” nem elhanyagolható körülmény a deklarált tájékoztatáshoz való jog, így a demokratikus közvélemény kialakulása szempontjából. A megfelelő tájékoztatás műfaji besoroláson és a hiteles forrásfeltárásban is rejlik, amely feladat ellátása, ellenőrzése a médiapiaci szolgáltatók belső strukturális, szakmai etikai kötelezettsége. A vélemények tényként való bemutatása a publicisztikai műfaj nem rendeltetésszerű használatakor félretájékoztatáshoz, álhírek terjesztéséhez is vezethet, nem véletlen, hogy utóbbi azonosításánál elsősorban azt kell megvizsgálni, hogy az adott tartalom tényt vagy véleményt közvetít.⁹ Érdekesség és megfigyelhető tendencia, hogy a hírek, közlemények mint szakmai műfajok alkalmazása a médiatartalom-szolgáltatások nyújtáskor sajnos egyre kevésbé népszerű.

A technológiai innováció következtében azonban előlépett egy, a médiapiacnál bővebb, többszereplős tömegtájékoztatási piac, ahol a médiaspecifikus intézmények már nem alkalmazhatóak. *A médiapiaci szereplők által megvalósított „tájékoztatási monopólium” már nem kizárólagos, az online platformszolgáltatók felületei bár a médiatartalom-szolgáltató kifejezést önmagukra tekintve nem tartják irányadónak, a felhasználóknak fogyasztható információkat közvetítenek, még hozzá legtöbbször személyes adatokat felhasználva, egyénhez rendelve.* Az online platformok saját bevallásuk szerint a tartalmakat nem előállítják, csak közvetítik, ezért nem végeznek olyan tájékoztatási

⁸ A médiaalkotmány 2. § (1a) bekezdése szerint az adott rendelkezés a Magyarország területén letelepedett médiatartalom-szolgáltató által kiadott sajtótermékek tekintetében nem alkalmazandó.

⁹ Lásd Koltay András: A közügyek vitáinak szabadsága és a személyiségi jogok védelme. *Pázmány Law Working Papers*, (2019), 4. 12–16.

típusú tevékenységet, amely a médiapiaci szereplőkéhez hasonló többletkötelezett-ségek vállalását eredményezné számukra. A tájékoztatási piac struktúrája tehát radikálisan megváltozott és folyamatosan változik, azt is problémás meghatározni, pontosan mely szolgáltató végez az online térben valóban ilyen tevékenységet, továbbá utóbbinak ilyen körülmények mellett mi is a pontos tartalma. Mégis, a minőségi tájékoztatás érdekében felállított mércék fenntartása okán is, de szükséges kijelenteni, hogy az a tájékoztatási piaci (nem fogyasztói) szereplő, amely közvetve vagy közvetlenül a szolgáltatásával a közélet eseményeiről informál, és arra befolyásolási képességgel is rendelkezik, nem hivatkozhat arra, hogy ő a szolgáltatását csupán a fogyasztó felé ellenértékért – avagy közvetetten ingyenesen – kínáló gazdasági tevékenységet folytató vállalkozás, ez utóbbi szemlélet a tájékoztatási tevékenységet szinte egyfajta szórakoztatási tevékenységgé degradálja, kifejezetten figyelmen kívül hagyva a tájékoztatás valódi, politikai értéként is fellépő szerepkörét.

Mindezek mellett azt is szükséges kiemelni, hogy a tájékoztató jellegű tartalmakat már nem kizárólag a médiaszektorban alkalmazott szakemberek, hanem az online platformok felhasználói is előállíthatják, akik ilyen módon egyszerre jelennek meg a felületen fogyasztói és tartalom-előállítói szerepben. Ezen személyi körben a műfaji kritériumok tudatos használata nem elvárható. A felhasználó állampolgárok hiába avansáltak a tartalmak előállítása és közzététele révén a társadalmi nyilvánosság olyan aktív szereplőivé, akik a közügyekhez kapcsolódó diszkussziót irányítani tudják, a sokszínűséget hitelt érdemlően támogatni nem tudják, mert nem rendelkeznek olyan erőforrásokkal, se nem kiterjedt közönséggel, mint egy tájékoztatási tevékenységet végző vállalat.¹⁰ Hátrány továbbá ezen tartalmak megítélését illetően, hogy a későbbiekben kifejtett szűrőbuborék típusú tájékoztatás hatására a felhasználók pontos tájékozottsága külön megkérdőjelezhető lett.

A fentiek tekintetében az online platformok szolgáltatásainak szabályozása világszerte alapvető és sarkalatos kérdés mind felelősségi körök, mind a pluralizmus érvényesülésének témakörében, ugyanakkor kifejezetten a tájékoztatási piacra, a demokratikus közvéleményre való hatására is tekintettel, és a felhasználók védelme szempontjából. Az Európai Unióban a platformok szabályozásának harmonizálása folyamatban van, az Európai Bizottság a közelmúltban két kapcsolódó jogalkotási kezdeményezést javasolt: a digitális szolgáltatások egységes piacáról szóló rendelet (DSA), illetve a digitális ágazat vonatkozásában a megtámadható és méltányos piacokról szóló rendelet (DMA) megalkotását. A Bizottság 2020 decemberében tette meg a javaslatát, 2022 márciusában és áprilisában ezzel együtt politikai megállapodás született azok tartalmát illetően. Egyes rendelkezések kivételével a DMA rendelet 2023 májusától, a DSA rendelet 2024 februárjától minősül közvetlenül alkalmazandónak. Ezen normákhoz kapcsolódóan szükséges még megemlíteni, hogy a tömegtájékoztatást érintve az Európai Bizottság új, előremutatóbb

¹⁰ Peter Coe: *Media Freedom in the Age of Citizen Journalism*. Cheltenham, Elgar, 2021. 2.

szabályozást javasolt a médiapluralizmus és a függetlenség védelme céljából is.¹¹ Az EU-tagállamok azonban egymást megelőzve már korábban és különállóan megkezdték az online platformok szabályozásának kialakítását a rendeletek hatálybalépésére tekintet nélkül, ami szintén jelzi, hogy a kapcsolódó problémák megoldása, a jelentkező szabályozási anomáliák kiküszöbölése nem várhat. A dán vagy akár a német állam jogalkotói a közelmúltban az előzőre tettek kísérletet, ahol az online platformokra vonatkozó jogszabályok, rendelkezések megalkotása során az értelmező rendelkezésekben elsősorban megpróbálták definícióval lefedni és megragadni azt a szolgáltatói jogalanyi kört, amely érintettnek minősül, így például „kommunikációs platformnak”, avagy „médiaközvetítőnek” aposztrofálják az online platformszolgáltatókat. Egy kialakított szabályozási rendszer csak akkor lehet megfelelő és hatékony, ha azon tárgykör fogalmával együtt jellege, amelyre irányul, pontosan meghatározott, ezeknek a körülményeknek mind a dán, mind a német jogalkotó ismeretében volt. A dán jogszabály egyértelműen kizárja a hatálya alól azon tömegtájékoztatásra irányadó médiatartalmakat, amelyek szolgáltatóira a médiafelelősségi törvény telepít kötelezettségeket, a német jogalkotó azonban pont fordítva gondolkodott: a médiáról szóló államszerződésbe, ezzel pedig a médiajogi rendszerbe helyezte bele az online platformszolgáltatókat, avagy azok egy meghatározott csoportját.¹² A szabályozási kísérletekkel egy az üzenet: a tartalmak közvetítése a felhasználók felé a fogyasztóvédelemhez kapcsolódó felelősség mértékét tekintve többletkötelezettségek vállalása nélkül nem lehet megengedett.

A DSA rendeletben foglaltak alapján a jogellenes online tartalmak bejelentése esetén a szolgáltató tartalommoderálást végezhet, amelynek megfelelően majd azok elérhetőségét, láthatóságát, hozzáférhetőségét érintő intézkedéseket hozhat. Dario La Nasa, a Twitter mint közösségi platform alkalmazottjának nyilatkozata szerint a rendelet hatálybalépése esetén a jogsértő tartalmakat a közösségi oldal felületén automatizált művelettel tudják majd a felhasználók jelenteni a szolgáltató felé, mégis azokat kizárólag a Twitter munkatársai, és nem algoritmusokban foglalt parancsoknak megfelelően fogják vizsgálni. A rendelet azonban a kivizsgálás időtartamára tekintettel egzakt határidőt nem szab meg, La Nasa sem tudott nyilatkozni arról, hogy egy-egy ügy áttekintését és a döntés meghozatalát milyen időintervallumban hajthatják majd végre.¹³

¹¹ European Media Freedom Act.

¹² 2022/126/DK számú notifikációs bejelentés: Social Media Regulation Act. 2022/126/DK (Denmark), (2022. szeptember 12.) 1. fejezet, 2. pont; Medienstaatsvertrag (MStV) in der Fassung des zweiten Staatsvertrags zur Änderung medienrechtlicher Staatsverträge (Zweiter Medienänderungsstaatsvertrag), 91. § Medienintermediäre.

¹³ A European Gaming and Betting Association (EGBA) által rendezett webinar-panelbeszélgetés: „Online consumer protection: How to promote a safer internet” in the EU címmel. 2022. október 20. European Safer Gambling Week. 2022. október 17–23.

Személyes adatok – a nudge-elmélet megjelenése az algoritmusokban

A tömegtájékoztatás online piacon való térnyerése, valamint emellett az internetes online platformok által kínált, szolgáltatási körben nyújtott információ hatalmas mennyisége a demokratikus közvélemény kialakulását egyszerre erősítik fel, azonkívül egyszerre gyengítik, továbbá a szolgáltatók által alkalmazott, új technológia által lehetővé tett eszközök (például szűrőbuborék, algoritmusok) alkalmazásával további anomáliák jelennek meg a tömegtájékoztatás rendszerében. Elengedhetetlen tehát a hagyományos médiatartalom-szolgáltatásokat kiegészítően az online térben kialakult hírpia „beszámításával”, gyakorlati példákkal szemlélve újragondolni a vonatkozó emberi jogok és a pluralizmus érvényesülését.

Az online platformszolgáltatók tömegtájékoztatási piacát „figyelempiac” elnevezéssel illeti Tóth András, a Versenytanács elnöke, amely az emberi figyelem és adatok felhasználásával felületet kínál az online térben hirdetőknak, valamint adatokat a felhasználók szokásait is megérteni kívánó harmadik feleknek, függetlenül attól, hogy az emberek figyelmét nem közvetlen díjazással kínált szolgáltatás-nyújtással szerzik.¹⁴ A figyelempiaci szolgáltatókban a felületek biztosítása, továbbá a zéróáras üzleti modell alkalmazása a közös jellemző, piacuk viszont úgynevezett nem tranzakciós piacként pontosan olyan elven működik, mint a hirdetésekből profitáló médiatartalom-szolgáltatók piaca. Mindkét esetben a szolgáltatás tárgya a tartalom, amellyel a felhasználóknak szórakoztatást, tájékoztatást ígérnek, a hirdetőket önmaguk finanszírozására szervezik, felületeik és felhasználóik kiárusításával egyszerre jutnak tehát adathoz, amely értéket képvisel, és emellett szintén fizetett reklámokhoz is. A platformok profitorientált tájékoztatási modellje tehát a médiapiaci modell továbbfejlesztett verziója, mindebben ezen alkalommal is a fogyasztó az, aki sérül, és akinek közvetítéssel teljesített tájékoztatása a szolgáltató által nem a demokratikus közvélemény kialakulását tekinti fő, elérendő céljának. Az egyébként a médiapiacon is megjelenő utóbbi problémakört tovább mélyíti jelen esetben a személyes adatok védelmének biztosítása is, a fogyasztó már több fronton szenvedhet sérelmet.

A közösségi média jeles képviselője, a Meta Platforms a felhasználási feltételeiben tájékoztat arról, hogy szolgáltatása bár díjmentes, azonban a vállalkozások, szervezetek, egyéb személyek fizetnek részére azért, hogy termékeiket, szolgáltatásaikat felületén reklámozza.¹⁵ A szolgáltató a személyes adatok alapján felhasználóit „célcsoportokba” sorolja, és ennek megfelelően számukra olyan információkat tesz személyre szabott hirdetésekben közzé, amelyek „relevánsak lehetnek a felhasználó és érdeklődési köre szempontjából”. A feltételek 2. pontjának rendelkezései azt is megfogalmazzák, hogy „a személyes adatokat a szolgáltató arra is használja,

¹⁴ Ilyen típusú online platformszolgáltató felület például: a Twitter, a Facebook, a YouTube, a Google stb.

¹⁵ Felhasználási feltételek. *Facebook*.

hogyan meghatározza, egyénre szabottan mely hirdetéseket jelenítse meg”. A figyelemre méltóan az a vállalkozás rendelkezik nagyobb értékkel, amely minél pontosabban behatárolt, személyes adatokkal előállított „fogyasztásicélközönség-csomagot” tud összeállítani hirdetői számára. Hatványozottan jelentkeznek továbbá a médiapiacra megfigyelt hirdetésszervezési gyakorlatok is, ugyanis a platformok a közzétett reklámok esetében sokszor nem olyan tartalmakat biztosítanak, amelyeket a felhasználó szeretne – hanem inkább olyan tartalmakat, amelyeknek fizetési hajlandóságon mért értéke nagyobb, mint amennyibe kerülnek.¹⁶ A felállított üzleti modell tehát gátat szab annak, hogy a felhasználó igazi fogyasztói és tájékoztatási igényei maradéktalanul teljesítve legyenek.

Ehhez kapcsolódóan, a gondolatmenetet folytatva szükséges a nudge-elméletet bemutatni, amelyet először Cass R. Sunstein és Richard H. Thaler vázoltak fel közösen a 2008-as évben kiadott könyvükben, az akkoriban bekövetkező gazdasági válságra is reagálva.¹⁷ A mű fejezeteiben a szerzők azt fejtegetik, hogyan lehet apróbb változtatásokkal jól hatni a társadalomra, annak és a benne élőknek a jóléte érdekében. Utóbbi állítás alátámasztására több esetet tanulmányoznak, ismertetnek, ilyen az a példa is, hogy a köznevelési intézmények büféiben érdemes a gyümölcsöket, zöldségeket a tanulók szemmagasságába helyezni a mindennapi, egészségesebb táplálkozás okán. Az elmélet szerint az állampolgárok választási szabadsága finoman terelhető lehet úgy, hogy saját életükre jó hatást gyakorló döntéseket hozzanak, emellett pedig a döntési szabadságuk is megmaradjon. A szerzők szerint téves feltevés az, hogy minden ember minden alkalommal olyan döntéseket hoz, amelyek önnön érdekeit szolgálják, vagy legalábbis jobban, mint azok a döntések, amelyeket valaki más hozott volna meg helyettük. A választási helyzeteket megkomponáló alanyokat „választási mérnököknek” nevezik a mű során, akiknek mind a fennálló életszituációról, mind azok alanyairól elegendő információval, adattal kell rendelkezniük ahhoz, hogy megfelelő döntést hozzanak, és pozitív hatást gyakorolhassanak. A platformok által használt algoritmusok tartalmáról meglehetősen keveset tudunk, ennek ellenére a nudge-elmélet szemüvegén keresztül megállapítható: minden szükséges adat és információ rendelkezésre áll az online platformszolgáltatóknak ahhoz, hogy ezen elmélet eszközét, az „enyhe ösztökélést” azok parancsaiba foglalja a hirdetőinek szánt termékcsomag tökéletesítése szempontjából. Az algoritmusok jellemzője, hogy nagy adatmennyiséget kezelnek automatizált döntéshozatal és profilalkotás céljából, utóbbi tevékenységek pedig jelentős kockázattal járhatnak az érintett személyek emberi jogaira. Az online platformok, köztük például a Meta Platforms is, a nudge-elméletet üzleti modelljük kiépítésekor ugyan felhasználhatták, azonban a felhasználókat termékként kezelve a fogyasztó, valamint az adatvédelem tekintetében az életükre tett jó hatást

¹⁶ Lásd Edwin C. Baker: *Media, Markets and Democracy*. Cambridge, Cambridge University Press, 2002. 1. fejezet, 4. rész: The market as a measure of preferences.

¹⁷ Richard H. Thaler – Cass R. Sunstein: *Nudge*. London, Penguin Books, 2009.

garantálni nem tudják, hiszen azok nem a szolgáltató jóléti érdekeit képviselik. A *Társadalmi dilemma* című dokumentumfilmben javaslatként azt fogalmazza meg az online platformok káros hatásainak megelőzésével kapcsolatban a témakörben érintett gazdasági társaságok foglalkoztatottjai és a nyilatkoztatott szakértők, hogy segíthet, ha a felhasználók semmilyen körülmények között nem kattintanak a felugró, hirdetésben javasolt tartalmakra.¹⁸ A platformok ugyanis a kattintás – tehát döntéshozatal – vonatkozásában új, vélelmezhető személyes adatcsomagot gyűjtenek a felhasználóról, amelyet eladnak a hirdetőiknek.

Az említett körülményeket mérlegelve, komplex képet vázol fel a figyelempiaci szolgáltatók tevékenysége tekintetében Yuval Noah Harari, aki korunk egyik legolvasottabb filozófusa, történésze. *21 lecke a 21. századra* című művében azt fejtegeti, hogy az adatóriások az információhalmazból kinyerhető tudással már nemcsak döntéseket hoznak helyettünk, és manipulálni próbálnak minket, de a mesterséges intelligencia fejlesztésében is segítheti őket a felhasználóktól szerzett, felhalmozott személyesadat-halmaz.¹⁹ Véleménye szerint, még ha most az adatok értékesítése nehezebbnek tűnik is, érdemes azokat birtokolni, hiszen kulccsal szolgálhatnak a jövő és az élet formálásához, ezt pedig a piac szem előtt tartja. Mindazonáltal a szerző kijelenti, hogy az adatok birtoklásának szabályozásához nehéz hozzáfogni, mert bár az ember például az ingatlanhoz kapcsolódó tulajdonjogi viszonyok rendezését nagyjából már kialakította, az adat nehezebb tárgykörnek bizonyul ilyen szempontból, mert az ingatlantól eltérően természetéből fakadóan egyszerre van jelen mindenhol és sehol, rendkívül gyorsan továbbítható, valamint másolni is korlátlanul lehetséges. A fent említett koncepciók és tények fényében egyre kevésbé érthetők a Fővárosi Törvényszék mint elsőfokú bíróság, majd a Kúria mint felülvizsgálati bíróság által a Gazdasági Versenyhivatal Facebook Ireland Ltd.-vel szemben meghozott, 1,2 milliárd forint bírság kiszabását elrendelő, a fogyasztók megtevesztését megállapító határozatát megsemmisítő ítéletekben foglalt megállapítások.²⁰ A Kúria szerint a Facebook nem követett el jogsértést akkor, amikor ingyenesként tüntette fel nyújtott szolgáltatását, a magyar igazságszolgáltatás fórumain tehát következképpen nem ismerték el azt a mások által már tényként kezelt körülményt, hogy a személyes adatok vagyoni értékkel bírnak, így a magyar joggyakorlat ellenkező, a köznapi felismeréssel és gyakorlattal ellentétes irányba forduló, nehezen megfogható értelmezési pályára terelődött.

Az Európai Unióban az általános adatvédelmi rendelet szolgál némi iránymutatással, mégis egyelőre csekély védelmet nyújt az online platformok által kezelt személyes adatok tekintetében, az egyéni ügyek esetében sokszor van szükség azok

¹⁸ *The Social Dilemma*. Rend. Jeff Orlowski. Exposure Labs – Argent Pictures – The Space Program, 2020.

¹⁹ Yuval Noah Harari: *21 lessons for the 21 century*. London, Penguin Books, 2019. 95.

²⁰ A Kúria Kfv.II.37.243/2021/11. számú ítélete.

külön értelmezésére.²¹ Az előbbi megállapítást támasztja alá az EUB előtt jelenleg is folyamatban lévő ügy, amelyben az előzetes döntéshozatal iránti kérelemben foglaltak szerint a Bundeskartellamt (német szövetségi versenyhatóság) eljárást indított a Meta Platforms (korábban Facebook Inc.) ellen, és a vitatott határozatában megtiltotta számára a felhasználási feltételeinek megfelelő adatkezelést, valamint e feltételek végrehajtását, továbbá intézkedéseket írt elő a szolgáltató számára a tevékenységek megszüntetésére irányulóan.²² A német versenyhatóság a meghozott döntését különösen azzal indokolta, hogy a szóban forgó adatkezeléssel a gazdasági társaság a hatályos német versenytörvény 19. §-a értelmében visszaélészerűen kihasználta a németországi magánfelhasználóknak szánt közösségi hálózatok piacán fennálló erőfölényét.²³ A Meta Platforms a német versenyhatósággal szemben keresetet nyújtott be a düsseldorfi regionális felsőbírósághoz, azonkívül megfogalmazta kétségeit afelől, hogy egyrészt a nemzeti versenyhatóságok ellenőrizhetik-e azt, hogy az adatkezelés megfelel-e az általános adatvédelmi rendeletben megfogalmazott követelményeknek, illetve versenyhatósági minőségükben megállapíthatják és szankcionálhatják-e a rendelet rendelkezéseinek megsértését. A regionális felsőbíróság az eljárást felfüggesztette, és az Európai Unió Bíróságához fordult értelmezési kérdésekben. Mindez alátámasztja, hogy az általános adatvédelmi rendeletben meghatározottak jelentéstartalma a jogalkalmazók számára sem egyértelmű, azok vizsgálata miatt gyakorta fordulnak a tagállami fórumok az EUB felé. Az online magánélet hatékony védelmét nem lehet csupán fogalmakban körülírni, a jogi kereteknek való megfelelést a gyakorlatban is biztosítani kell technológiai eszközökkel, így például annak védelmét javító technológiákkal, beépített adatvédelemmel.²⁴

Szűrőbuborék alkalmazása és a tájékoztatás sokszínűségének érvényesülése

A Meta Platforms felhasználási feltételeinek rendelkezései, továbbá a *Társadalmi dilemma* című dokumentumfilm által és a személyes használat során mind többen meggyőződnek arról, hogy hirdetésekén keresztül, a személyes adataik felhasználásával tájékoztatják őket az online platformok, kérdés azonban a mai napig, hogy pontosan milyen módon és milyen értékválasztás mentén. Feltehető az a kérdés is,

²¹ Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet). L 119/1 (2016. május 4.).

²² C-252/21. sz. Facebook Inc. és társai kontra Bundeskartellamt ügyben 2021. április 22-én benyújtott előzetes döntéshozatal iránti kérelem.

²³ Gesetz gegen Wettbewerbsbeschränkungen (GWB).

²⁴ Adamantia Rachovitsa: Engineering and Lawyering Privacy by Design: Understanding Online Privacy Both as a Technical and an International Human Rights Issue. *International Journal of Law and Information Technology*, 24. (2016), 4. 374–399.

hogy a profilozás következtében alkalmazott személyre szabott információválasztás mennyiben minősülhet szerkesztői tevékenységnek, hiszen az algoritmusok a felhasználókra nézve ilyen módon teremtenek információs szűrőbuborékokat az online platformszolgáltatók felületein. Példaként említve szűrőbuborékkal – más néven információs „visszhangkamrákkal” – működik a Facebook idővonala, továbbá hirdetési metódusa, valamint a Google is személyekre, illetve földrajzi elhelyezkedésre vonatkozó jellemzők szerint jeleníti meg a találatait. Az egyes felhasználók nem ugyanazon tartalmakkal szembesülnek, hanem a róluk kialakított digitális profiltérkép alapján válogathatnak a számukra megjelenő információk között – így egyénenként alternatív valóságokat létrehozva. A szűrőbuborék tehát olyan egyénre szabott, mesterséges virtuális információs térnek minősül, amelynek hatására a felhasználók valóságérzékelése eltorzulhat.²⁵ A Meta Platforms felhasználási feltételeit, de akár más platform feltételeit is újfent felidézhetném, ott, ahol már értékválasztás történik – hiszen a felhasználó által preferált, relevánsnak ítélt tartalmakat jelenítenek meg –, véleményem szerint egyfajta automatizált szerkesztési tevékenység is megvalósul. Megfigyelhető továbbá a szűrőbuborékok alkalmazása és a félretájékoztatás között egyfajta párhuzam, hiszen a buborékban közzétett szűrt tartalommal a szolgáltató a felhasználó előítéleteit nagy eséllyel megerősíti, aki így elfogultsága következtében kifordítva értékelheti és tárhatja a nyilvánosság elé véleményét, rosszabb esetben nem pontosan a tényeket. Amennyiben egy adott előítéletet egy esemény konfirmál, akkor az alany azt nagyobb eséllyel általánosan reprezentatívnak tűntetheti fel, ha viszont annak valami ellentmond, akkor azt nagyobb valószínűséggel izolált eseménynek minősítheti. A sokszínű tömegtájékoztatásra tehát a „visszhangkamra” kifejezetten veszélyes, hiszen a szolgáltató az általa preferált kényelmi és hirdetésszervezési szempontok figyelembevételével hozza létre az egyéni információs tereket, és nem széles körű tájékozódásra neveli felhasználóit. Ezen okból nemcsak hogy csökkenhet a társadalmi viták száma, de kritikus gondolkodásra sincs a célközönség kényszerítve, a felhasználók érdeklődési köreik mentén egyre jobban szeparálódnak, a társadalom polarizáltsága pedig nő, ami az együttélés során tartósan több feszültséget generálhat.

Összegzés

Ismereteink függvényében nem vonható le más következtetés, mint hogy az állampolgárok csak a megfelelő, plurális tájékoztatásuk esetén tudnak a közéletben teljes értékű véleménynyilvánítással, döntésekkel részt venni, jelen lenni, de a szűrőbuborékok alkalmazása egyértelműen káros befolyással van a sokszínűség érvényesülésére,

²⁵ Klein Tamás: A web 2.0 egyes szabályozási kérdései – különös tekintettel az alkotmányjogi vonatkozásokra. In Klein Tamás (szerk.): *Tanulmányok a technológia- és cyberjog néhány aktuális kérdéséről*. Budapest, Médiatudományi Intézet, 2018. 46.

továbbá fikciós tájékoztatási joguk is sérül, mert a tartalmak közvetítésekor nem a fogyasztói jólétüket tartja a szolgáltató szem előtt. Ennek megfelelően azonban a tagállamokban a demokratikus közvélemény biztosítása és a regnáló demokratikus rezsimek is kihívás elé kerülnek. A szolgáltatók által alkalmazott üzleti modell, a technológia gyors ütemben történő fejlődése és a tömegtájékoztatási piac sajátosságai okán kizárólag egy jogág vonatkozó rendelkezései nem tudnak a sokszínű tájékoztatás, a demokratikus közvélemény kialakulásának megvalósításában segíteni, ahhoz több jogág alkalmazása, kapcsolódó szabályozási rendszere, továbbá a tudományterületek között híd megteremtésével lehet megoldásokat keresni. Egyre jobban kirajzolódik, hogy a tömegtájékoztatás megfelelő minősége mellett a személyes adatok védelmért folyó küzdelem ugyanolyan, ha nem erőteljesebb figyelmet igényel a tárgykör szempontjából, hiszen jelenleg az általános adatvédelmi rendelet egyértelműen nem tud teljes körű védelmet nyújtani az online platformszolgáltatók felhasználói számára. Vannak kétségek afelől is, hogy a teljes körű védelem abszolválható-e, avagy elfogadjuk, hogy lesznek szolgáltatások, amelyekért pénz helyett nagyobb rizikót vállalva a személyes adatainkkal fizetünk, és beletörődünk azok feldolgozásának körülményeibe. Mivel a médiapiac tekintetében is felmerült az igény a profitorientáltság lehető legnagyobb fokú mellőzésére a minőségi tömegtájékoztatás javára, kétlem, hogy személyes adataink kezelése tekintetében nem törekednénk arra, hogy az érintetti jólétet, biztonságot megteremtsük. Harari megállapításait vizsgálva azonban utóbbi óriási kihívást fog jelenteni, ennek érdekében többet kell megtudnunk a technológia szabályozási eszközeiről, az algoritmusokról, valamint azok tervezéséről és működéséről is.

Az Európai Unió által harmonizálási célból megalkotott jogszabálysomagban szereplő digitális szolgáltatások egységes piacáról szóló rendelet (DSA) és a digitális ágazat vonatkozásában a megtámadható és méltányos piacokról szóló rendelet (DMA) tartalmi egy rendkívül határozott, de egyelőre kis lépés megtételét jelentik afelé, hogy a közvetített tartalmakkal kivitelezett tömegtájékoztatás minőségét és sokszínűségét védeni lehessen. Amíg nincs teljes meggyőződés arról, hogy az online platformszolgáltatók szerkesztői felelősséggel rendelkeznek a maguk felületére vetítve annak sajátosságaival együtt, addig félő, hogy igazán eredményes szabályozási fejlesztés nem fog megvalósulni az ágazatban. A demokrácia legitimitása ellenben nem válogat, bármilyen eszközön keresztül is érnek el az információk a fogyasztók felé, valójában a tájékoztatási tárgykörben releváns érvényesülési feltételek ugyanazok maradnak; a mindenkit megillető véleménynyilvánítás szabadsága, valamint a tájékozódáshoz való joggal együtt a sokszínű tájékoztatás és a demokratikus közvélemény jelenléte a társadalomban. A magyar szabályozás tekintetében ezen közlemény szerzője még reménykedik abban, hogy valamikor a médiaalkotmányban deklarált tájékoztatáshoz való jog minden szolgáltató vonatkozásában egy objektív szempontrendszer szerint felállított, az állampolgárok által követhetően számon kérhető intézménnyé válik. Utóbbi megoldási eszköze a jogalkotáson kívül azonban inkább a fogyasztók és a szakma képviselői tudatosságának növelésében gyökerezhet.

Felhasznált irodalom

- Baker, Edwin C.: *Media, Markets and Democracy*. Cambridge, Cambridge University Press, 2002.
- Bihari Mihály – Pokol Béla: *Politológia*. Budapest, Nemzeti Tankönyvkiadó, 2009.
- Birchall, David: Corporate Power over Human Rights: An Analytical Framework. *Business and Human Rights Journal*, 6. (2021), 1. 42–66.
- Coe, Peter: *Media Freedom in the Age of Citizen Journalism*. Cheltenham, Elgar, 2021.
- Harari, Yuval Noah: *21 lessons for the 21 century*. London, Penguin Books, 2019.
- Huntington, Samuel P.: *A civilizációk összecsapása és a világrend átalakulása*. Ford. Gázsity Mila – Gecsényi Györgyi – Pusztai Dóra. Budapest, Európa Könyvkiadó, 2019.
- Klein Tamás: A web 2.0 egyes szabályozási kérdései – különös tekintettel az alkotmányjogi vonatkozásokra. In Klein Tamás (szerk.): *Tanulmányok a technológia- és cyberjog néhány aktuális kérdéséről*. Budapest, Médiatudományi Intézet, 2018. 41–49. Online: <http://mek.oszk.hu/18100/18192/18192.pdf>
- Koltay András: A közügyek vitáinak szabadsága és a személyiségi jogok védelme. *Pázmány Law Working Papers*, (2019), 4. 1–23.
- Rachovitsa, Adamantia: Engineering and Lawyering Privacy by Design: Understanding Online Privacy Both as a Technical and an International Human Rights Issue. *International Journal of Law and Information Technology*, 24. (2016), 4. 374–399.
- Thaler, Richard H. – Cass R. Sunstein: *Nudge*. London, Penguin Books, 2009.
- The Social Dilemma*. Rend. Jeff Orlowski. Exposure Labs – Argent Pictures – The Space Program, 2020.
- Török Bernát: *Szabadon szólni, demokráciában. A szólásszabadság magyar doktrínája az amerikai jogirodalom tükrében*. Budapest, HVG-ORAC, 2018.

Jogszabályok

2010. évi CIV. törvény a sajtószabadságról és a médiatartalmak alapvető szabályairól
2010. évi CLXXXV. törvény a médiaszolgáltatásokról és a tömegkommunikációról
- Social Media Regulation Act. 2022/126/DK (Denmark) (2022. szeptember 12.). Online: <https://ec.europa.eu/growth/tools-databases/tris/hu/search/?trisaction=search.detail&year=2022&num=126>
- Medienstaatsvertrag (MStV) in der Fassung des zweiten Staatsvertrags zur Änderung medienrechtlicher Staatsverträge (Zweiter Medienänderungsstaatsvertrag). Online: www.die-medienanstalten.de/fileadmin/user_upload/Rechtsgrundlagen/Gesetze_Staatsvertraege/Medienstaatsvertrag_MStV.pdf
- Gesetz gegen Wettbewerbsbeschränkungen (GWB). Online: www.gesetze-im-internet.de/gwb/
- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet). L 119/1 (2016. május 4.)

Kéringer Szabolcs

NetzDG, avagy gyakorlati példa a platformszabályozás megvalósítására



Amíg az Európai Unió az egységes online piac szabályozási kereteinek megalkotásán dolgozik, addig a tagállamok is szolgáltatnak példákat a platformszabályozás megvalósítására, és szabályozásaik iránya és tartalma jelentősen különbözhetnek is egymástól. A jelen írás a NetzDG elmúlt öt éve alapján vizsgálja meg, hogy ugyanarra a problémára Németország és közvetlen szomszédai mennyire eltérő módon reagálnak.

Előszó

Az elmúlt hónapokban többször is említette interjúi során a Nemzeti Média- és Hírközlési Hatóság (NMHH) elnöke a platformszabályozás kérdését, ezen interjúkból önkényesen kiragadott egy-egy gondolattal lehet talán legjobban megalapozni a jelen cikk tárgyának. Koltay András a közösségi médiáról először akként nyilatkozott, hogy rengeteg pozitívumot hoztak ezek a szolgáltatások, „hiszen kiterjesztették a véleményformálás és az információhoz jutás lehetőségét, de vannak komoly veszélyei is: ezek a platformok saját maguk döntenek arról, hogy mit engednek a saját felületeiken megjelentetni és mit nem. Ez látszólag tiszta jogi helyzet, hiszen magántulajdonú platformokról van szó, ők határozzák meg a szabályokat”, de mára a közösségi média „olyan nyilvánosság-befolyásoló erőt jelent, amit súlyos hiba lenne érintetlenül hagyni [többek között azért, mert] ezek a platformok szerkesztői szerepben vannak. Hogy mit lát ugyanis a felhasználó, azt nagy mértékben a platform dönti el.”¹ Megállapította továbbá azt is, hogy veszélyesek a szólás szabadságára azok a jelenségek, hogy a platformok sok olyan tartalmat törölnek, amely egyébként nem jogellenes, illetve ha a politikai-közéleti vitákba avatkoznak moderálás útján.²

A jelenlegi uniós szabályozási keretek között a platformszolgáltatók mint közvetítő szolgáltatók immunitást élveznek a harmadik fél, tehát a felhasználó által közzétett tartalom területén, ameddig – leegyszerűsítve – a tartalom a szolgáltató

¹ Az idézés nem teljes, a cikk témájához igazodóan rövidítettünk rajta, nem feltétlen tükrözi az elnök úr gondolatait; elérhető: Baranya Róbert: Nem az államtól kell félni a sajtószabadságot – Koltay András NMHH-elnök a Mandinernek. *Mandiner*, 2022. március 4.

² Vizvári Soma: A techcégek cenzúrája veszélyes a szólás szabadságára. *Magyar Nemzet*, 2022. július 20.

nem hajt végre tartalomszerkesztési jellegű beavatkozást. Ez a szabályozás az e-kereskedelmi irányelvből³ ered, amely az „irányelv megalkotásakor egy, a 2000-es évek elején még reálisnak mondható, de pillanatszerű technológiai kereteket vett alapul, ám az azóta eltelt mintegy két évtized során jelentős változáson és fejlődésen ment át a szabályozás háttéréül szolgáló technológia”.⁴ A német jogalkotó szerint a 2010-es évek második felére érkezett el az ideje annak, hogy a közösségi média-szolgáltatók igenis szigorúbb felelősséget viseljenek az általuk kínált platformokon akár bűncselekményt is megvalósító tartalmak közzétételéért, tehát időszerűnek tartotta az immunitás határait visszanyírbálni kissé.

A NetzDG megalkotásának háttere

A jelen cikk tárgyát képező úgynevezett NetzDG megértéséhez elengedhetetlen, hogy a technológiai változások mellett a kétezertizedes évek felhasználói szokásainak folyamatait, valamint a közbeszéd fő témáját szolgáltató társadalmi jelenségeket is figyelembe vegyük. A törvényt a Bundestag a 2017. évben fogadta el és 2018. év elejétől kellett ténylegesen is alkalmazni. Hazánkban éppen ebben az időben készített az NMHH egy kutatást,⁵ amelynek eredménye azt igazolta, hogy a hazai internetezők már előnyben részesítették az internetet a televízióhoz és más hagyományos platformhoz képest, ráadásul szinte minden internetező megtekintett valamilyen audiovizuális tartalmat online, és egyes vizsgált korcsoportok tagjainak 96%-a heti rendszerességgel használt valamilyen közösségi szolgáltatást is. Időközben az NMHH elkészítette ezen felmérés frissítését is, amely megállapításai szerint a leggyakoribb internetes tevékenység a közösségi oldalak használata, ráadásul a 2018-as felméréshez képest is tovább nőtt, immáron az internetezők 98%-a használja a közösségimédia-felületeket.⁶ Mindamellet, hogy töretlenül növekszik a közösségi platformok látogatottsága és felhasználóinak száma – függetlenül attól, hogy melyik szolgáltatás aktuálisan a trendi, vagy veszít éppen valamelyest népszerűségéből –, egy másik jelenség is szorosan összekapcsolódik ezen folyamattal: fokozatosan a tájékozódás első számú terepévé fejlődött a közösségi média. Ennek megfelelően a közösségimédia-platformok funkciója már régen meghaladta a kezdetben jellemző kapcsolattartást, és egyre nagyobb szerepet töltenek be immár nemcsak a szűken vett szociális kapcsolatok ápolásában, de a közvetlen

³ Az Európai Parlament és a Tanács 2000/31/EK irányelve (2000. június 8.) a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem, egyes jogi vonatkozásairól (Elektronikus kereskedelemről szóló irányelv). L 178/1 (2000. július 17.).

⁴ Tatár Attila: A tárhelyszolgáltatók körében felmerülő felelősségi kérdésekről. *Infokommunikáció és Jog*, 72. (2019), 1. 8–13.

⁵ NMHH: *Lakossági internethasználat 2018*. 2019. március 19.

⁶ NMHH: *Az elektronikus hírközlési piac fogyasztóinak vizsgálata*. Internetes felmérés 2020.

tartalom- és hírfogyasztásban is, tehát a tömegtájékoztatásban, működésük ezért egyre inkább hasonlít egy analóg médiaszolgáltatóhoz, és egyre kevésbé tekinthetők csak semleges, technológiai feladatokat ellátó háttérszolgáltatóknak.⁷ Az amerikai közvélemény-kutató, a Pew Research már 2015-ben azt mutatta ki, hogy a felhasználók jelentős része politikai álláspontját a közösségi média alapján alakítja ki.⁸ A platformok igazi hatalmát a közügyek vitáinak befolyásolására a platformok azon tevékenysége jelenti, hogy az algoritmusaik segítségével az egyes felhasználókról gyűjtött adatok alapján személyre szabhatják az egyes felhasználók által érzékelt és elérhető tartalmakat. A leginkább eklatáns példa erre a Facebook hírfolyama vagy a Twitter. Emögött természetesen praktikus okok is húzódnak, hiszen elméletileg a felhasználók számára kedvező, ha a platform igyekszik számukra valamelyest rendet vágni a tartalmak tömegében, és a feltehetően őket leginkább érdeklőket megmutatni nekik. Ezt a szolgáltatói tevékenységet nagymértékű információs aszimmetria jellemzi, hiszen nem lehet tudni, hogy a platform mi alapján válogat, milyen módon viszonyul a közügyek vitájára vonatkozó tartalmak és a nyaralási élménybeszámolók megfelelő arányának kérdéséhez, és milyen gazdasági érdekei húzódnak meg egyik-másik tartalom előtérbe helyezése mögött.

A német médiaszabályozás vonatkozásában gyakran találkozhatunk a nézettel, hogy óvatosabb a nyugati demokráciákban megszokottakhoz képest a II. világháború eseményei miatt, hiszen a nemzetiszocialisták megerősödésében és hatalomátvételében jelentős szerepe volt a propagandának, beleértve a külső hatalmak félrevezetését is.⁹ Amíg például Németország élen jár a holokauszttagadás kriminalizálásában, addig például az Egyesült Államokban az is a szólásszabadság részét képezi, és így védelmét élvezi. 2020-ban a Facebook¹⁰ és a Twitter¹¹ is bejelentette, hogy törölni fogják az ilyen tartalmakat, igaz, a Twitter később ezt akként finomította, hogy nem holokauszttagadó tartalommal szemben lépnek fel, hanem az egyben dezinformációnak minősülő tartalmakkal szemben, ugyanis a politikai véleményeknek helye van a közbeszédben.¹² Mindenesetre az elmúlt években a téma egyértelmű „népszerűségnek” örvend, és a közösségi média ezen nézetek széles körű

⁷ Bartóki-Gönczy Balázs: *Az online közvetítő szolgáltatók mint az információhoz való hozzáférés új kapuőrei*. Budapest, Pázmány Press, 2018.

⁸ Amy Mitchell – Jeffrey Gottfried – Katerina Eva Matsa: Millennials and Political News. Social Media – the Local TV for the Next Generation? *Pew Research Center*, 2015. június 1.

⁹ Charlotte Hsu: How media ‘fluff’ helped Hitler rise to power. *University at Buffalo*, 2015. augusztus 28.

¹⁰ Mark Zuckerberg [@Mark Zuckerberg]: Today We’re Updating Our Hate Speech Policy to Ban Holocaust Denial. [Idővonal-bejegyzés]. *Facebook*, 2020. október 12.

¹¹ Sam Shear: Twitter Follows Facebook on Removing Posts That Deny the Holocaust. *CBNC*, 2020. október 15.

¹² Ramsey Touchberry: Twitter CEO Says Holocaust Misinformation Does Not Violate Its Policy. *Newsweek*, 2020. október 28.

terjesztésének elsődleges platformja.¹³ Az elmúlt évtized második felében ráadásul az idegengyűlölet újból erősödni látszik az afrikai és ázsiai menekültválság miatt, Angela Merkel kancellár Németországa megnyitotta kapuit a menekültek előtt (ügynevezett Willkommenskultur¹⁴). Ezzel párhuzamosan viszont egyre nagyobb sajtóvisszhangot váltanak ki a bevándorlók által elkövetett erőszakos bűncselekmények, ezek közül több is terrorista cselekménynek minősült, ráadásul az Iszlám Államhoz is sokan csatlakoztak Németország területéről.¹⁵ Párhuzamosan a német bevándorláspolitikát a társadalom egy részének ellenszenvét is kiváltotta, ami egyben a menekült- és iszlámellenes politika megerősödését is jelentette,¹⁶ és a bevándorlásellenes közbeszéd elsődleges színtere a közösségi média lett.¹⁷ Az idegengyűlölet nem áll meg az idegeneknél, és a közösségi médiában egyre gyakrabban válnak a gyűlölködések tárgyává a menekültpárti hazai politikusok is. A NetzDG alkalmazásának kezdete, 2018 óta ráadásul a jóléti Európa nyakába szakadt egy koronavírus-járvány, a lezárások és karanténhelyzetek, a szociális és szórakozási korlátozások, majd az orosz–ukrán ellentét kiéleződése, illetve mindvégig e kettő okozta ellátási problémák és várható gazdasági recesszió, amelyek újabb és újabb táptalajt biztosítanak az online anonimitás mögött megbújó fröcsögőknek és trolloknak.

A szövetségi igazságügy-minisztérium ebben a milióben hozott létre még 2015-ben egy internetszolgáltatókból, civil szervezetekből és médiaszabályozással foglalkozó intézetekből álló bizottságot, hogy találjanak önkéntes alapú megoldást a közösségimédia-felületeken terjedő gyűlölködés és dezinformáció problémájára, azonban a kormány nem volt elégedett a bizottság jelentésével.¹⁸ Egy 2017-es kutatás eredménye ráadásul arra világított rá, hogy a közösségimédia-platformok nem igazán jeleskednek a jogsértő tartalmak eltávolításában.¹⁹ A társadalom, a közélet és az online kommunikáció ezen folyamatai vezettek a NetzDG 2017-es tervezetéhez, majd a törvény elfogadásához: leegyszerűsítve azt mondhatjuk, hogy a német jogalkotó kevésnek találta a szolgáltatók aktivitását és erőfeszítéseit, így kiemelte a tárgyat az önszabályozás keretéből, és törvényalkotás mellett döntött.

¹³ Adam G. Klein: How to Fight Holocaust Denial in Social Media – With the Evidence of What Really Happened. *The Conversation*, 2020. december 3.

¹⁴ Willkommenskultur. *Wikipédia*.

¹⁵ Matthias von Hein: 20 Years After 9/11, Germany Targets Militant Islamists. *Deutsche Welle*, 2021. szeptember 11.

¹⁶ Isabelle Hertner: Germany: a Country of immigration – Or Integration? Merkel's Uncomfortable Legacy. *The Loop*, 2021. április 21.

¹⁷ Lisa-Maria N. Neudert: Germany: A Cautionary Tale. In Samuel C. Woolley – Philip N. Howard (szerk.): *Computational Propaganda. Political Parties, Politicians, and Political Manipulation on Social Media*. Oxford, Oxford University Press, 2018. 153–184.

¹⁸ Gemeinsam gegen Hassbotschaften. 2015. december 15.

¹⁹ *Löschung rechtswidriger Hassbeiträge bei Facebook, YouTube und Twitter. Ergebnisse des Monitorings von Beschwerdemechanismen jugendaffiner Dienste.*

A német szövetségi országgyűlés, a Bundestag végül 2017 júniusában fogadta el a NetzDG-t, teljes nevén *Netzwerkdurchsetzungsgesetz* (Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken; azaz a közösségi médiára vonatkozó hálózat-végrehajtási törvény), amelyet néha szokás Facebook-Gesetz, azaz Facebook-törvény gúnynévvel is illetni. A törvény rövid felkészülési időt követően 2018. január 1. napjától alkalmazandó ténylegesen is, azóta pedig már kiegészítéseket is elfogadott hozzá a jogalkotó. A törvény értelemszerűen az uniós e-kereskedelmi irányelv által felállított kereteken belül igyekezett kitágítani a „tudomásszerzésen alapuló szolgáltatói felelősség” határait, ily módon nem teremtett új „jogintézményt”, csak nagyobb aktivitásra kötelezi a platformszolgáltatókat, pénzügyileg érzékelhető bírság kilátásba helyezésével.

A törvény főbb rendelkezései

A NetzDG főbb rendelkezéseinek bemutatása során nem törekszünk teljességre, csak a „jogintézmény” és céljának megértéséhez szükséges szabályokra szorítkozunk, a konkrét részletszabályok nélkül.

A törvény személyi hatálya alá azok a platformszolgáltatók tartoznak, amelyek a Német Szövetségi Köztársaságban legalább kétmillió regisztrált felhasználóval rendelkeznek.²⁰ Nem tartozik ugyanakkor a törvény hatálya alá a szerkesztői/újságírói tartalom, amely felett egy beazonosítható és ily módon felelősségre vonható (szerkesztői) felelősséget visel.²¹ Ez a kivétel teljességgel érthető, hiszen a platformszolgáltatók immunitásának korlátozása vagy helyesebben feltételhez kötése éppen egy olyan másodlagos, kiegészítő jellegű felelősséget hoz létre, amelynek szükségét az elsődleges és közvetlenül érvényesülő szerkesztői felelősség hiánya teremti meg. Fontos kritérium még a szolgáltatással szemben, hogy a zárt kommunikációs csoportoknak felületet biztosító szolgáltatások (e-mail- vagy chatszolgáltatások) nem, tehát csak a nyilvánosan hozzáférhető felületek tartoznak ide.²²

A NetzDG-ben „tiltott” tartalmak közvetlenül a büntetőjogra épülnek, hiszen a törvény a német Büntető Törvénykönyvben (*Strafgesetzbuch – StGB*)

²⁰ A különböző felmérések alapján a teljes lakosság 90-94%-a használ internetet, míg social médiát 66 millió ember, tehát a teljes lakosság körülbelül 80%-a, míg az internetezők 85%-a használ. Ezekhez a számokhoz viszonyítva a kétmillió regisztrált felhasználó kevesebb, mint a teljes lakosság 3%-a; lásd Digital 2021: Germany; Share of internet users in Germany from 2001 to 2021.

²¹ NetzDG 1. cikk 1. szakasz (1) és (2) bekezdés.

²² A social media igen tág fogalom, lényegesen tágabb és sokrétűbb szolgáltatást foglal magában, mint a mindennapi szóhasználatban a Facebook-szerű szolgáltatásokra való utalás; erre vonatkozóan lásd Papp János Tamás: *A közösségi médiaplatformok szabályozása a demokratikus nyilvánosság védelmében*. Doktori értekezés. Budapest, Pázmány Péter Katolikus Egyetem, 2021. 14–20; míg a közösségi platformok szabályozási szempontú azonosításának és definíciójának nehézségeiről lásd Zódi Zsolt: Az európai platformszabályozás jellegzetességei. *In Medias Res*, 11. (2022), 1. 70–75.

meghatározott egyes bűncselekményeket megvalósító, azaz büntetőjogi szakki-fejezéssel élve tényállásszerű magatartásokat (tartalmakat) helyez a tárgyi hatálya alá oly módon, hogy közvetlenül hivatkozik (kiutal) a StGB egyes tényállásaira. A NetzDG-be importált egyes tényállások szelekciója természetesen nem véletlenszerű, hanem a törvény megalkotását megelőző bő évtized társadalmi jelenségeire igyekezett reflektálni a jogalkotó, amit az is jelez, hogy a jogszabály időközbeni kiegészítésével újabb tényállásokat is behúzott a hatálya alá, ami a törvény alkalmazása első időszakának megfigyelésein alapul, mintegy folyamatos hatáskövetés eredményeként. A bűncselekmények kiválasztása során a jogalkotó a közbeszédben ténylegesen és gyakran előforduló és így társadalmi szinten, tehát nem csak vagy nem feltétlenül az online térben problémásként értelmezhető magatartásokra igyekezett reflektálni. A NetzDG tehát tulajdonképpen egy válogatás aszerint, hogy mely bűncselekményeket megvalósító tartalom esetében vár el reakciót a jogalkotó a szolgáltatótól, ezek között megtalálhatók a becsületsértés és rágalmozás, az uszítás és gyűlöletkeltés, a magánélethez való jog megsértése, gyerekpornográfia, politikailag szélsőséges tartalmak, alkotmányellenes szervezetek propagandaanyagai/-tartalmi felbujtás és erőszak, valamint államellenes vagy a közösség nyugalmanak megzavarására alkalmas tartalmak.²³

A törvény alapján véve nem vár el proaktivitást a szolgáltatóktól, nem nevezi ki őket csendőrré, és a szolgáltatók nem kötelesek nyomozni vagy előzetes tartalomkontrollt végezni a felületükön megjelenő felhasználói tartalmakra vonatkozóan. A gyűjtőzsinór vége ily módon a felhasználók kezében van, ugyanazon felhasználók kezében tehát, akik a törvényellenes tartalom közzétételét is cselekszik. A szolgáltató ugyanis elsősorban arra köteles, hogy a NetzDG hatálya alá tartozó valamely bűncselekményt megvalósító felhasználói „feljelentést” kivizsgálja. Ezen cél érvényesüléséhez természetesen elengedhetetlen, hogy a felhasználók tisztában legyenek ezen lehetőségükkel, a bejelentés feltételei oly módon legyenek adottak, hogy azok kifejezetten elősegítsék a felhasználói részvételt, tehát könnyen elérhető, közérthető és könnyen használható felületeket kell erre kialakítaniuk a szolgáltatóknak.²⁴ Az egész törvény rendszerének kulcsa tehát a panaszbejelentési garanciák felállítása, és a sor legelején a fogyasztói részvétel: mintha azt mondaná a jogalkotó, hogy amire a felhasználók mint a társadalom tagjai nem élnek panaszbejelentéssel, az vagy nem éri el az össznépi ingerküszöböt, vagy ha igen, akkor sem botránkoztatja meg az embereket annyira, hogy vegyék a fáradságot egy panaszbejelentés megtételére (feltételezve persze, hogy egyáltalán tudatában vannak ezen lehetőségnek). Álláspontunk szerint ez kissé szokatlan megközelítés egy jogalkotótól, ámde megfontolásra érdemes: a Bundestagban ülő képviselők nem akarják a padok közül megmondani, hogy mi az a mérce, amit az aktuális közbeszéd nem bír el, inkább a társadalom tagjaira bízzák, hogy maguk vessék ki a szólásszabadság

²³ NetzDG 1. cikk 1. szakasz (3) bekezdés.

²⁴ NetzDG 1. cikk 3. szakasz (1), (2) és (4) bekezdés.

védelmére nem érdemes tartalmakat. Természetesen mindez akkor érvényesülhet megnyugtató módon, ha az adott társadalom vagy közösség tagjai kellő fogyasztói öntudattal rendelkeznek, tehát érzékenyek a számukra káros tartalmakra, ismerik a rendelkezésre álló „jogorvoslati eszközöket”, és nem restek élni is ezen jogaikkal, tehát van egyfajta felhasználói aktivitás és önkéntes részvétel, egyfajta online polgár-ország. A törvény egyébként kiemeli, hogy a szolgáltató különös figyelemmel köteles eljárni, ha egy panaszbejelentés valamely jogvédelmi szervezettől, tipikusan civil szervezettől érkezik, és nem csak ráérő haragos szomszédok bosszantják egymást a másik feljelentgetésével.

A szolgáltató köteles a formailag megfelelő módon beadott bejelentéseket kivizsgálni, rövid határidővel, majd eljárása eredményéről az érintetteket, így elsősorban a bejelentőt és amennyiben elérhető, a bepanaszoltat értesíteni és a rendelkezésükre álló jogorvoslati lehetőségekről tájékoztatni. Amennyiben a szolgáltató a kivizsgálás során arra a megállapításra jut, hogy a panasszal érintett tartalommal bizony megvalósul a NetzDG alá is behúzott valamely büntető tényállás, úgy köteles az érintett tartalmat törölni, vagy legalábbis annak a Német Szövetségi Köztársaság területén történő hozzáférését blokkolni. A szolgáltató szigorú eljárási határidőhöz kötött, ugyanis a jogsértő tartalmakat hét nap alatt kell eltávolítani, de a „nyilvánvalóan jogsértő tartalmakat” mindössze 24 óra alatt. Amennyire törekedett a jogalkotó az egész hálózat-végrehajtás intézménye során a törvényi-eljárási szabályok és garanciák megalkotására, különösen a szolgáltatói eljárások lefolytatását és a felhasználási jogok érvényesülését tekintve, annyira rezeg a léc a „nyilvánvalóan jogsértő tartalom” fogalmának megalkotásával. A Bundestaghoz benyújtott előterjesztés értelmezésében nyilvánvalóan jogsértőnek tekintendő az a tartalom, amely jogsértő jellegének megállapításához nem szükséges mély elemzés.²⁵ Amint látni fogjuk, a francia testvértörvény 24 órás reakciót ír elő alapesetként, és egyes nyilvánvalóan jogsértő tartalmak eltávolítására egy egész órát enged(ett volna) a szolgáltatók részére.

Ha összevetjük ezen a ponton a NetzDG-t és az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvényt (Ektv.), azt látjuk, hogy ez utóbbi alapján a szolgáltató az immunitás köpenye alatt főszabályként nem felel a más (például a felhasználó) által rendelkezésre bocsátott, de a közvetítő szolgáltató által nyújtott információs társadalommal összefüggő szolgáltatással (leegyszerűsítve a felületen) továbbított, tárolt vagy hozzáférhetővé tett információért, és szintén nincs proaktív nyomozati kötelezettsége²⁶ – másfelől azonban a hazai szabályozás nem is ír elő olyasféle felhasználói jogokat és eljárási garanciákat, amelyek biztosítják a sérelmes(nek vélt) tartalmak kivizsgálását a szolgáltató oldalán. Az összehasonlításba bevehetjük az e-kereskedelmi irányelvet is, amely a preambulumának rendelkezései

²⁵ Gesetzentwurf der Fraktionen der CDU/CSU und SPD. Deutscher Bundestag: Drucksachen[BT]18/12356, 2017. május 16. 22–23.

²⁶ Ektv. 7. § (2) és (3) bekezdés.

között azt mondja ki, hogy az adattárolásból álló szolgáltatás nyújtójának felelőssége korlátozott, de a szolgáltató köteles haladéktalanul intézkedni az adat eltávolítása, illetve az ahhoz való hozzáférés megszüntetése iránt, ha valamely jogellenes tevékenységről ténylegesen tudomást szerez.²⁷ Ugyanakkor az irányelv lehetőséget ad a tagállami jogalkotók számára, hogy ennek részletszabályait megalkossák, amikor is kimondja, hogy az eltávolítást, illetve a hozzáférés megszüntetését a véleménynyilvánítás szabadsága elvének és az e célból nemzeti szinten megállapított eljárásoknak a figyelembevételével kell elvégezni; ezért az irányelv nem érinti a tagállamok lehetőségét arra, hogy olyan különös követelményeket állapítsanak meg, amelyeknek az adat eltávolítását, illetve az ahhoz való hozzáférés megszüntetését megelőzően haladéktalanul meg kell felelni.

Ha ebből az irányból vizsgáljuk a NetzDG-t, úgy felmerül a kérdés, hogy a német jogalkotó nem csupán annak eljárási, ily módon garanciális szabályait fektette-e le, hogy az e-kereskedelmi irányelvből eredő kötelezettségét a platformszolgáltató mikor (milyen feltételek esetén) és hogyan (milyen módon) köteles teljesíteni. Valójában nem csupán eljárási szabályokat, amolyan felhasználó és szolgáltató közötti „perrendtartást” vezetett-e be az új törvény anélkül, hogy ténylegesen egy újfajta felelősségi formulával kínálta volna meg a szolgáltatókat? A perrendtartás szóhasználat mindenképpen túlzó és szakmailag pontatlan, viszont kifejező és éppen ezért szándékos is. Merthogy az uniós vagy a magyar szabályozás hivatkozik a szolgáltató eltávolítási kötelezettsége keretében arra, hogy azt bíróság vagy egyéb kompetens hatóság rendeli el, míg ezen felül nyitva hagyja a tudomásszerzés mint előfeltétel részleteit. Egy találó kifejezéssel ezt nevezhetjük a tudomásszerzésen alapuló felelősségmegállapítás elvének („knowledge based liability principle”).²⁸ Ehhez képest a NetzDG megadja a tudomásszerzés definícióját azáltal, hogy a szolgáltató immunitása feltételelessé homályosul abban a pillanatban, hogy panaszbejelentést regisztrál, mindaddig, amíg elvégzi annak kivizsgálását, és dönt a tartalom eltávolításáról vagy a panasz visszautasításáról. Itt tehát a tudomásszerzés egyik formájának jogszabályi konkretizálásáról van szó, ami az e-kereskedelmi irányelv keretein belül nem jelent teljes és kizárólagos tudomásszerzési lehetőséget vagy forrást, tehát nem zárja be a lehetséges kört, csak egy egyértelmű módját jelöli ki.

A perrendtartás szóhasználat ugyanakkor nemcsak emiatt kínálkozik, hanem mert a szolgáltatóra olyan kötelezettséget és felelősséget ró, amely bizony nem sajátja, és alighanem az e-kereskedelmi irányelv legtágabb értelmezésében sem lehet beleérteni abba: tudniillik a NetzDG azt várja el egy piaci alapon működő és szerveződő gazdasági társaságtól, másképpen fogalmazva magánjogi jogalanytól, hogy lefolytasson egy büntetőeljárást, méghozzá gyorsított eljárásban anélkül, hogy

²⁷ E-kereskedelmi irányelv (46) preambulumbekkezdés, valamint 14. cikk (1) bekezdés a) és b) pontjai.

²⁸ Folkert Wilman: The EU's System of Knowledge-based Liability for Hosting Service Providers in Respect of Illegal User Content – Between the e-Commerce Directive and the Digital Services Act. *Jipitec*, 12. (2021), 3. 317–341.

az ehhez szükséges nyomozati hatáskörökkel és kényszerítőeszközökkel rendelkezne. Némi gúnnyal azt is mondhatnánk, hogy a jogalkotó maga nem találta meg a megfelelő eszközt és megoldást a probléma kezelésére, ezért az általános megoldás helyett áthárította a konkrét esetek tüneti kezelését a szolgáltatókra. Önmagában nem tűnik ördögötől valónak, hogy a platformok, főleg a NetzDG alá tartozó globális techóriások szerepet és nagyobb felelősséget vállaljanak a kulturált diszkurzus feltételei fenntartásában, hiszen egyértelműen feljük billen a serpenyő azáltal, hogy egyre több bevételre és egyre nagyobb információs hatalomra tesznek szert, miközben a szabályozók az információs aszimmetria miatt nem képesek hatékonyan érvényesíteni az érdekeiket.²⁹ Leegyszerűsítve úgy is fogalmazhatunk, hogy akinél a bevétel és a gazdasági előny lecsapódik, az aktívan vegyen részt a kockázatok enyhítésében is, képletes párhuzammal élve az autógyártókra is mind újabb és több biztonsági előírás vonatkozik, amelyeknek egyre újabb fejlesztésekkel tudnak csak megfelelni. Mindazonáltal még akkor is túlméretezett lépésnek tűnik a bűnüldözési szerepkör szolgáltatókra történő kiszignálása, ha valamennyire érthető is bevonásuk a folyamatba: a szolgáltató rendelkezik a legtöbb, ráadásul közvetlen, első kézből származó információval mind a tartalmat, mind a közzétevő felhasználót, a tartalom terjedését, elérését és utóéletét illetően. A szolgáltató közvetlen részvétele tehát indokolt, de nem mindegy, hogy „perbeli szerepe” fél, tanú, vádlott vagy esetleg bíró. Óhatatlanul felmerül a kérdés tehát: nem azt látjuk-e, hogy amit az állam nem képes maga megoldani, azt inkább a szolgáltatóra hárítja?³⁰

A törvényt, helyesebben már magát a jogalkotási koncepciót számos helyről érte kritika, kérdéses mindamellett, hogy ezek mennyire bizonyultak valósak a lassan ötéves jogalkalmazás tapasztalatai alapján. A leginkább megalapozott ellenérvnek talán éppen ez a kiszélesített szerepkényszer tűnik, mert olyan kompetenciák meglétét várja el a magáncégektől, amelyek megnyugtatóan többéves szakmai tapasztalatszerzés után halmozódnak fel szakembereknél. Az állami bíraskodás és ítélezés társadalmi legitimáción, alkotmányos alapokon nyugszik, és törvénybe foglalt eljárásrendek szabályozzák – ehhez képest a jogalkotó hirtelenjében azt várja el a szolgáltatótól, hogy 24 órás időpérésben döntse el, hogy egy tartalom nyilvánvalóan jogsértő-e, vagy sem. Egy felmérés szerint a vizsgált uniós tagállamok (Németország, Ausztria, Franciaország, Dánia és az akkor még uniós tag Egyesült Királyság) bíróságai átlagosan 778 nap alatt hoznak döntést a gyűlöletbeszéddel kapcsolatos ügyekben.³¹ Nem véletlen, hogy mint az az időszakos szolgáltatói

²⁹ Egyes techóriások kapitalizációja már meghaladja a legtöbb tagállam GDP-jét; lásd Clothilde Goujard – Samuel Stolton: Europe reins in Big Tech: What you need to know. *Politico*, 2021. november 25.

³⁰ Jacob Mchangama – Natalie Alkiviadou – Raghav Mendiratta: *Rushing To Judgment: Are Short Mandatory Takedown Limits for Online Hate Speech Compatible with The Freedom of Expression?* Kopenhága, The Future of Free Speech Project – Justitia, 2021.

³¹ Mchangama–Alkiviadou–Mendiratta (2021): i. m.

jelentésekből kiderül, a legtöbb szolgáltató tipikusan két szakmai gárdával végzi a panaszok kivizsgálását, és az inhouse szűrő (rendszerint szintén két lépcsőben) mellett külső jogi tanácsadókat is igénybe vesznek, sőt, maga a törvény is propagálja a szakmai (civil) szervezetekkel való együttműködést. Mindezek azonban csak kozmetikáznak azon a tényen és körülményen, hogy a platformszolgáltató igenis egyfajta jogérvényesítési szerepkörben találta magát, négy hónapos felkészülési határidővel. Amennyire törekszik a NetzDG az egész folyamat jogi garanciáinak lefektetésére, annyira nem tűnik megalapozottnak ez a transzformáció, legalábbis elméletben semmiképpen. Amint látni fogjuk, a francia testvértörvény többek között ezen is csúszott el az alkotmányossági vizsgálatán.

A szolgáltatói szerepvállalás mögött talán az a felismerés is rejlik tehát, hogy az állami jogérvényesítési lehetőségek igénybevétele lényegesen lassabb, az általános munkateher mellett az egyes szolgáltatók esetében akár az évi milliós számot is elérő ügyteher nem kezelhető, márpedig az online tér dinamikájában egy éveket késő bírósági ítéletnek nincs érdemi haszna. Erre azonban megoldást kínálhatna egy hibrid módszer, amely a jogalkalmazás egységességét is elősegíthetné: a szolgáltató mint gazdaságilag érdekelt fél vegyen részt az eljárásban, de ne mint ügyszó, hanem amolyan kiszignált titkár vagy előadó bíró, aki a döntéshez szükséges információkat begyűjti (amennyire az hatósági jogkörök nélkül lehetőségében áll), majd az adatokat feldolgozza, és egy erre hivatott szakmai grémium (bírószék, hírközlési hatóság, külön e célra felállított szerv) döntést hoz. Maradva a pénzügyi érdekek és szerepvállalás kérdésénél, a szolgáltatók ennek finanszírozásában is jelentős kötelezettségeket kaphatnának, tehát az államot nem terhelné a rendkívüli eljárás humán és tárgyi erőforrásigénye.

NetzDG a gyakorlatban – ami a szolgáltatói jelentésekből (nem) derül ki

Az Európai Unió magas szintű szervezetei régóta vívnak szópárbajt a techóriásokkal, elsődlegesen az adózás és az adatkezelés, adatvédelem és adatvagyon felhasználása, monetizálása területén. Az uniónak több, olykor egymásnak talán ellentmondó gazdasági, politikai és egyéb szempontot is figyelembe kell vennie. A két fél nem egyenlő információs bázissal vesz részt a vitában, egyfajta információs aszimmetria jellemzi a két felet, habár ez a kifejezés elsődlegesen arra utal, hogy a szolgáltató csak általa ismert módszerekkel (algoritmusokkal) és csak általa ismert adatokat gyűjt, tárol és dolgoz fel a felhasználókról és szokásaikról (elég csak a Cambridge Analytica-féle botrányra hivatkozni). Éppen ezért az uniós jogalkotási törekvések középpontjában rendszerint a transzparencia, a szolgáltatói működés minél mélyebb megértése áll, így a digitális szolgáltatások egységes piacáról és a digitális

szolgáltatásokról szóló új jogszabályok esetében is.³² A NetzDG egyik vívmánya, hogy maga is törekszik a szolgáltatói eljárások átláthatóvá, egyúttal számonkérhetővé tételére: a törvény időszakos (féléves), igen részletes jelentéstételi kötelezettséget ró a platformokra, amely jelentések teljesen nyilvánosak és online hozzáférhetőek.³³ (Ugyanígy visszaköszön az uniós tervezetekben és a német törvényben a szolgáltatói kapcsolattartó/képviselő kijelölésének kötelezettsége is.)³⁴

A törvény alkalmazásának kezdetétől eltelt időszak féléves szolgáltatói jelentéseinek vizsgálata, összevetése egyfelől érdekes, esetenként meglepő eredményeket hoz, mégis egyúttal hiányérzetet is hagy maga után, mert álláspontunk szerint különösebb következtetések levonására kevésbé alkalmasak. Mindenféleképpen a meglepő kategóriába sorolható, hogy a Facebookhoz az első hat félévben beérkező panaszbejelentések száma egyszer sem érte el a 14 ezret,³⁵ miközben azonos időszakban a YouTube (Google) 214-388 ezer,³⁶ míg a Twitter akár közel 850 ezer panaszt is kénytelen volt elbírálni.³⁷ Ennek oka azonban, hogy a kezdeti időszakban a Facebook nem tett eleget a felhasználók tájékoztatására vonatkozó kötelezettségének, így ismereteink szerint mindmáig az egyetlen, a törvény alapján kiszabott bírságot éppen ez a cég kapta, a nem kielégítő eljárásrendszere miatt (ennek megfelelően a vizsgálatot követő változtatások következményeként több mint hússzorosára ugrott a Facebookhoz érkező bejelentések száma 2021 első félévében). Habár a panaszbejelentések mennyisége összességében növekszik valamennyi szolgáltató esetében, ez nem egy konstans emelkedő vonalat jelent, észlelhetők visszaesések, olykor jelentősen, akár százezres nagyságrendben. A leggyakoribb, tipikusnak mondható területek (tehát hivatkozott bűncselekmények) az egyes szolgáltatások esetében mutatnak némi eltérést, ami érthető, ha figyelembe vesszük a platformok sajátosságait. Amíg például a képek és videók, tehát a vizuális tartalmak megosztására használatos Instagram³⁸ vagy TikTok³⁹ kiemelkedő számot jelent a fényképek közzétételével megvalósuló magánszféra megsértésében, addig a rövid szöveges üzenetekre specializálódott Twitteren a gyűlölködő tartalmak és a becsületsértés,

³² Digital Market Act: Az Európai Parlament és a Tanács (EU) 2022/1925 rendelete (2022. szeptember 14.) a digitális ágazat vonatkozásában a versengő és tisztességes piacokról, valamint az (EU) 2019/1937 és az (EU) 2020/1828 irányelv módosításáról. (digitális piacokról szóló jogszabály). L 265/1 (2022. október 12.) és Digital Services Act: Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (2022. október 19.) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (digitális szolgáltatásokról szóló rendelet). L 277/1 (2022. október 27.).

³³ NetzDG 1. cikk 2. szakasz (1) és (2) bekezdés.

³⁴ NetzDG 1. cikk 5. szakasz (1) és (2) bekezdés.

³⁵ Törvény a közösségi hálózatokon történő jogérvényesítés javításáról („NetzDG”). *Facebook*.

³⁶ Eltávolítások a Hálózati Végrehajtási Törvény alapján. *Google*.

³⁷ Germany – Twitter Transparency Center. *Twitter*.

³⁸ Törvény a közösségi hálózatokon történő jogérvényesítés javításáról („NetzDG”). *Instagram*.

³⁹ NetzDG Transparenzbericht. *TikTok*.

rágalmazás a leggyakoribb esetek. A YouTube-os videómegosztások között szintén kiemelkedő mennyiségben jelenik meg a gyűlöletkeltés, mellette pedig az erőszakos tartalmak (tehát az indokolatlanul, meghökkentő módon erőszakos, vagy az erőszakot magasztaló videók) és a szexuális tartalmak – ez utóbbi nyilvánvalóan nem jellemző a Twitterre. Az egyes szolgáltatásokat nem lehet tehát közvetlenül összehasonlítani, hiszen a platformok sajátosságai, a jellemző felhasználók köre és korcsoportja, ezáltal az érdeklődési körök is eltér(het). A törlések aránya is vegyes képet mutat, nem észlelhető semminemű tendencia vagy törvényszerűség, a szolgáltatók rendszerint a bejelentések 10–30%-a alapján távolítanak el tartalmakat – ugyanakkor az nem derül ki a jelentésekből, hogy a bejelentés alapján már az első szűrőn, tehát a szolgáltató által alkalmazott community guideline-on sem megy át az inkriminált tartalom, vagy azon még átengednék a moderátorok, és ténylegesen a NetzDG szabályai miatt távolítanak el egy tartalmat. A törvény bevezetésének egyik indoka abban a praktikus megközelítésben rejlett, hogy önmagában az a körülmény, hogy a közösségimédia-platformok saját irányelveket írnak elő, és az alapján moderálási tevékenységet végeznek, még nem oldja meg azokat a helyzeteket és problémákat, amelyeket a szolgáltatók nem kezelnek.⁴⁰ A megismert jelentések viszont nem adnak igazolást arra, hogy a szolgáltatói szabályokon átengedett, ámde valójában súlyos kockázatot hordozó tartalmak szűrkezónája mekkora is. Álláspontunk szerint éppen az egyik legnagyobb hiányossága a jelentéseknek/adatszolgáltatásnak, hogy a részletesen vizsgált szolgáltatók közül csak a Google adta meg a már első körben, tehát a community guideline alapján törölt és a csak második körben, azaz a NetzDG alapján blokkolt tartalmak számát, ez utóbbi rendre 10% alatti arányt képviselt, tehát a YouTube-ról a bepanaszolt tartalmak már rendszerint a szolgáltató saját szabályai szerint is problémásnak minősültek.

Ami egyértelműen megállapítható tehát, hogy mindegyik szolgáltató esetében nő az egy időszakban megtett bejelentések száma, még ha egy-egy félévben tapasztalható is visszaesés, viszont a panaszbejelentések számának növekedése nem jár feltétlenül az eltávolítások arányának növekedésével. E ponton érdemes megjegyezni, hogy a NetzDG életbelépését követően készült felmérés szerint a megkérdezett németek mintegy 67%-a kifejezetten, míg 20%-a csak egyszerűen értett egyet a törvénnyel, míg elutasító csak 5% volt. Megjegyzendő, hogy a felmérést készítő szervezet szerint hasonló, még ha némileg alacsonyabb fogadtatásban részesülne egy hasonló szabályozás Franciaországban vagy az Egyesült Államokban is.⁴¹

⁴⁰ Patrick Zurth: The German NetzDG as Role Model or Cautionary Tale? Implications for the Debate on Social Media Liability. *Fordham Intellectual Property, Media & Entertainment Law Journal*, 31. (2021), 4. 1084–1153.

⁴¹ Anisa Holmes: *87% of Germans Approve of Social Media Regulation Law*.

A szolgáltatói jelentések statisztikai adatai, tehát a bejelentések számának emelkedése ennyiből alátámasztja a társadalmi egyetértést, tehát valószínűsíthetően élnek is a lehetőséggel a felhasználók.

A törvény egyébként igen súlyos(nak tűnő) bírságok kiszabásának lehetőségéről is rendelkezik, akár ötmillió euró összegig terjedően,⁴² bár az eddigi gyakorlatban a bírságolás nem igazán jelent meg, a Facebook esete kivételével, ami azonban a jelentéseik elégtelenségének a következménye volt, nem pedig az eltávolítási kötelezettség elmulasztásán alapult.⁴³ A törvény kritikusai szerint a bírság lehetősége jelentős chilling effecttel bírhat. Meg kell jegyezzük ugyanakkor, hogy ezek a vélemények inkább a jogalkotás időszakát jellemezték, és mostanában már kevésbé jelentkeznék, talán azért is, mert nem bizonyosodott be, hogy a hatóság szórná a milliós büntetéseket, illetve a szolgáltatók is szemmel láthatóan beálltak a sorba. A chilling effect tágabb értelemben hatással lehet a globálisan értelmezett szolgáltatásra is. Ameddig a közösségi médiaszolgáltatások közvetítő szolgáltatásnak minősülnek, és immunitással bírnak a felületükön közzétett felhasználói tartalomért való felelősség tekintetében, addig a tartalmi jellegű ellenőrzés és szolgáltatói moderálás alapja az önszabályozás, amelyben kiemelkedő szerepe van a szolgáltatók által alkalmazott alapelveknek, felhasználási feltételeknek (community guidelines). Márpedig a techóriások törekednek arra, hogy egységes guideline-okat használnak, lehetőség szerint az összes országban, ahol szolgáltatásuk elérhető, ahelyett, hogy minden országban a helyi jogszabályok szerint váltakoznának ezek a szabályok (ez egyébként valamelyest egybevág az EU egységes online piac megalkotására irányuló törekvéseivel, persze ott nem a globalitás, csak az európai egység a cél). Azonban ha a NetzDG-féle nemzeti szabályozások megszorodnak, úgy fennáll a kockázata, hogy a szolgáltatók megszigorítják a felhasználási feltételeiket az egyszerűbb megfelelés érdekében, amivel viszont más szabályozás alatt egyébként védett tartalmak indokolatlanul kerülnének törlésre.⁴⁴ Persze a NetzDG globálissá hízásától egyelőre semmiképp nem kell tartanunk, mint ahogy a szolgáltatói túlkapásoktól, a túlmoderálástól sem, az eddigi tapasztalatok szerint nem tűnik megalapozottnak a chilling effecttel riogatás Németországban sem, amit alátámaszt az imént hivatkozott statisztika is – igaz, csak a Google-tól –, hogy alig plusz 10%-ban törölnek tartalmakat a NetzDG alapján.

⁴² NetzDG 1. cikk 4. szakasz (1) és (2) bekezdés.

⁴³ Thomas Escritt: Germany Fines Facebook for Under-reporting Complaints. *Reuters*, 2019. július 2.

⁴⁴ Amelie Heldt: Germany Is Amending Its Online Speech Act NetzDG... But Not Only That. *Internet Policy Review*, 2020. április 6.

Nemzetközi kitekintés – platformszabályozás a német határok mentén

A korábbiakban többször is utaltunk már a NetzDG „testvértörvényeire”, ugyanis több országban fogadtak már el hasonló tartalmú törvényt 2018 óta.⁴⁵ A lista hosszú, még az Egyesült Államokban is felmerült – habár egyáltalán nem tűnik valószínűnek – a Communications Decency Act vonatkozó 230. szakaszának felülvizsgálata és módosítása, miközben az Európai Unióban szinte a NetzDG teljes életpályáját párhuzamosan lekövette a DSA és a DMA előkészítése, lényegesen visszafogottabb megközelítéssel.⁴⁶ Ehhez képest alighanem pusztán véletlen, hogy Németország közvetlen határszomszédságában jelent meg három olyan érdekes példa, amelyet indokolt röviden bemutatnunk a megértés szélesítése érdekében: egy NetzDG kópia (Ausztria), egy elbukott adaptálási kísérlet (Franciaország) és egy totális ellenút (Lengyelország).

Ausztriában a szövetségi parlament az úgynevezett kommunikációsplatform-törvényt (Kommunikationsplattformen-Gesetz – KoPl-G)⁴⁷ fogadta el 2020-ban. A törvény a helyi adottságok mellett egyértelmű hasonlóságokat mutat a német verzióval, gyakorlatilag annak honosított másolata. Érdekesség, hogy a magyar népességszámhoz megközelítőleg azonos (nagyjából 10%-os az eltérés) osztrákok a százezer felhasználóval rendelkező szolgáltatókat tették a jogszabály alanyává, tehát körülbelül 1%-os a küszöb a teljes népességhez viszonyítva. Itt tehát egy „szerzői jogi jogsértést” is felvető másolásról beszélhetünk.

Sokkal izgalmasabb a platformszabályozás története Franciaországban. A francia Nemzetgyűlés szintén 2020-ban fogadta el az úgynevezett Avia-törvényt, amely tárgyat tekintve „gyűlöletbeszéd-törvényként” jelent meg, de lényegében a NetzDG nem is különösebben titkolt adaptálása volt a célja.⁴⁸ A francia törvényalkotási szokásoknak megfelelően annak rapportöréről, Laetitia Avia alsóházi képviselőről kapta nevét, a törvénytervezetről kialakult viták során a képviselő asszony maga komoly támadásokkal nézett szembe, német kollégájához hasonlóan őt is megvádolták azzal, hogy korábbi személyes sérelmei miatt igyekszik bosszút állni a törvénnyel.⁴⁹

⁴⁵ A nemzetközi platformszabályozási törekvésekre lásd Christoph Schmon – Haley Pedersen: Platform Liability Trends Around the Globe: Recent Noteworthy Developments. *Electronic Frontier Foundation*, 2022. június 1.

⁴⁶ A hivatkozott két uniós szabályt még nem fogadták el, az azonban látszik, hogy lényegesen visszafogottabb eszközökkel közelítik a tárgyat, és inkább az átláthatóság és a szolgáltatói együttműködési hajlandóság növelése, a „nevelés” a DSA és a DMA célja az immunitás felrúgása és a törlési kötelezettség előírása helyett, ugyanakkor ennek részletes elemzése önmagában kitesz egy önálló publikációt.

⁴⁷ Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Kommunikationsplattformen-Gesetz, Fassung vom 24.10.2022.

⁴⁸ Loi n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet.

⁴⁹ David Perrotin: Laetitia Avia, la députée LREM qui horripile ses assistants. *Mediapart*, 2020. május 12.; illetve Laetitia Avia [@LaetitiaAvia]: En 2 mois, David Perrotin a publié 3 articles sur moi. [Thread]. *Twitter*, 2020. május 12.

Maga a törvény egyébként nem önálló norma volt, hanem az elektronikus kommunikációt és szolgáltatásokat szabályozó más törvények kiegészítésével akarta szigorítani a szolgáltatók eljárási kötelezettségeit és felelősségét. A francia törvényverzió leginkább szembetűnő eltérése a némethez képest a lényegesen lerövidített határidő: itt egy, illetve 24 óra állt (volna) a szolgáltatók rendelkezésére ahhoz, hogy a bejelentéseket kivizsgálják, és döntsenek a tartalom eltávolításáról; az egyórás halmazba a terrorizmussal kapcsolatba hozható és a gyermekpornográf tartalmak tartoztak, mint a törvény szerint nyilvánvalóan jogellenes tartalmak.

A feltételes mód oka, hogy a törvény valójában sosem lépett alkalmazásba, mert az Alkotmánytanács⁵⁰ hatályon kívül helyezte,⁵¹ annak ellenére, hogy az Avia-törvény valójában nem értelmezhető teljesen új szabályozási megközelítésnek a francia jogban, hiszen elsődlegesen egy hatályos és alkalmazott törvényt⁵² módosított, amely már egyébként is rendelkezett a terrorista cselekményekre uszító vagy illet népszerűsítő, illetve a gyermekpornográfiához kapcsolódó tartalmak eltávolításának lehetőségéről. Ennek ellenére már a törvény megszületése is igen gyötrelmesre sikeredett, ugyanis az alsóház és a Szenátus nem jutott egyezsére, az ellenzéki oldal folyamatosan támadta a tervezetet,⁵³ így végül a francia alkotmányos szabályoknak megfelelően a végső szót az alsóház mondhatta ki,⁵⁴ és a Nemzetgyűlés meg is szavazta azt,⁵⁵ amellyel szemben a Szenátus hatvan tagja előzetes normakontrollt kért az Alkotmánytanácstól – amely tulajdonképpen meg is semmisítette azt. A tanács indokolásában kitér arra, hogy Franciaországban a szólásszabadság alkotmányos alapja történelmileg egészen az 1789-ben elfogadott Emberi és polgári jogok nyilatkozatáig⁵⁶ nyúlik vissza, amely alapján a gondolatok és vélemények kifejezése az egyik legértékesebb emberi jog, aminek az online térben azonosan kell érvényesülnie. A francia alkotmány⁵⁷ alapvető szinten biztosítja polgárai részére a szabadságjogok gyakorlását (34. cikk), ennek megfelelően írja elő a szólásszabadságról szóló törvény I. cikkének első mondatában az elektronikus eszközökön keresztül megvalósuló nyilvános kommunikáció szabadságát, majd annak garanciális keretei között rögzíti, hogy a szólásszabadság gyakorlásának korlátozására csak a szükséges mértékig és meghatározott okból vagy célból, így többek között a gyermekek és fiatalok védelme, a közrend fenntartása vagy

⁵⁰ Conseil constitutionnel.

⁵¹ Décision n° 2020-801 DC du 18 juin 2020.

⁵² Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

⁵³ Avis relatif à la proposition de loi visant à lutter contre la haine sur internet. Commission nationale consultative des droits de l'homme. 2019. július 9.

⁵⁴ Soós Petronella Eszter: Párizs törvénnyel lépne fel az online gyűlölet ellen. *A Tett és Védelem Alapítvány honlapja*, 2020. június 2.

⁵⁵ A szavazás eredménye elérhető itt: Première séance du mercredi 13 mai 2020.

⁵⁶ Déclaration des droits de l'homme et du citoyen.

⁵⁷ Constitution française du 4 octobre 1958.

a nemzetvédelem céljából kerülhet sor. Persze maga az Avia-törvény is éppen ezen érdekek védelmét szolgálta volna ugyebár.

Az Alkotmánytanács természetesen maga is lefekteti, hogy a kiskorúakat érintő pornográf, illetve a terrorizmust népszerűsítő tartalmak súlyosan sértik mások jogait, és alkalmasak a közrend megingatására, ezért érthető, hogy a jogalkotó igyekszik fellépni ezekkel szemben, és egyébként ilyen esetben helye is lehet a szabadságjogok törvényi korlátozásának. A korlátozásnak azonban meg kell felelnie a szükségesség, arányosság és hatékonyság mércéjének, ráadásul erre megfelelő eljárási garanciák mellett kerülhet csak sor. Az indokolás alighanem legfontosabb része, hogy egy tartalom jogellenes természetének megállapítása az arra felhatalmazott hatóság kizárólagos hatásköre, így módon nem értelmezhető a tartalom nyilvánvaló jogellenességének feltételezése. Emellett az egyórás törlési határidő a sérelmezett tartalom közzétevőjének eljárási garanciális jogait is sérti, ugyanis a törlést elrendelő döntéssel szembeni fellebbezésnek nincs felfüggesztő hatálya, ezért az egy órán belül megvalósuló törlés esetén kizárt, hogy bíróság felülvizsgálhassa a törlő határozatot. Az Alkotmánytanács álláspontja szerint jelentős kockázatként kell értékelni a törvény esetében várható chilling effectet, a szabályok tényleges alkalmazása nagy valószínűség szerint indokolatlan cenzúrázáshoz vezetne, részben a kilátásba helyezett bírság miatt is, hiszen ekkor a szolgáltató (illetve az egyes ügyekben eljáró moderátor) a jobb félni, mint megijedni elv alapján valószínűsíthetően inkább törli a határvonalon mozgó tartalmakat, mintsem euró százezres-millió bírságokat kockáztasson.

A törvény(tervezet) kálváriája azonban aligha ért véget az Alkotmánytanács határozatával. 2020 őszén, alig pár hónappal a törvény elfogadása és az előzetes normakontroll lefolytatása után egy igen súlyos eset rázta meg a francia közvéleményt: egy francia tanár lefejezése,⁵⁸ amely mögött sokan a közösségimédia-platformok szerepét és felelősségét is felvetették,⁵⁹ újból felszínre hozva egy sosem feloldott feszültséget, és egy 2021-es törvény is részben érinti a szabályozási területet, azonban a NetzDG-féle szabályozási koncepciótól lényegesen eltérő, visszafogottabb módon.⁶⁰

A német, osztrák és francia platformszabályozásnak/törekvésnek szöges ellentéte a lengyel irány, ahol a kormányt évek óta foglalkoztatja a gyűlöletbeszéd és más kiemelten jogsértő felhasználói tartalmak szabályozásának kérdése. Ők azonban a Facebookkal való együttműködésre törekedtek, és 2018-ban megállapodásban⁶¹ rögzítették, hogy a felhasználók jogorvoslattal fordulhatnak a szolgáltatóhoz egy

⁵⁸ Samuel Paty: French Teacher's Beheading Directly Linked to Social Media Campaign, Say Prosecutors. *Euronews*, 2020. október 21.

⁵⁹ Laura Kayali – Elisa Braun: France Pushes Tougher EU Rules for Social Media in Wake of Terror Attack. *Politico*, 2020. október 26.

⁶⁰ Loi n° 2021-1109 du 24 août 2021 confortant le respect des principes de la République.

⁶¹ Agreement on the creation of a Contact Point.

meghatározott listán szereplő esetek miatt törölt posztjuk, profiljuk vagy felhasználói fiókjuk visszaállítása érdekében.⁶² A lengyel helyzetértékelés szerint a felhasználókat nem elsősorban egymástól kell megvédeni, hanem az indokolatlan szolgáltatói cenzúrától, ugyanis reális veszélyként értékelik, hogy a felhasználók gyakran „ideológiai cenzúra áldozatai” lesznek a tartalomtörlést megalapozó valós jogszabályi felhatalmazás hiányában,⁶³ amitől meg kell védeni a felhasználókat.⁶⁴ A jogalkotási koncepciók között olyan is megjelent, miszerint a szólásszabadság érvényesülésének biztosítására a szolgáltatók saját felhasználási feltételeik alapján nem,⁶⁵ csak a lengyel törvények megsértése esetén és alapján törölhetnének tartalmakat.⁶⁶ Az uniós egységesítési törekvéseknek így igen nehéz lesz érvényt szerezni, ha – bár ez nyilván csak vizuálisan bír jelentőséggel – két szomszédos, ráadásul nagy lélekszámú piac ennyire eltérő módon nyúl a probléma szabályozásához.

Összegzés

Amíg tehát az Európai Unió az egységes online piac szabályozási kereteinek megalkotásán dolgozik, addig a valóságban éppen a tagállami fragmentációt látjuk megvalósulni abban, hogy ugyanarra a problémára Németország és közvetlen szomszédai mennyire eltérő módon reagálnak. Ami közös az EU és a négy hivatkozott tagállam megközelítésében, hogy „a kialakult helyzetben az államok a klasszikus eszközt, a szabályozást sürgetik, mert a jogban látják a problémák megoldásának kulcsát”,⁶⁷ de még a Facebook vezérigazgatója is felvetette a szabályozás szükségességét a közelmúltban, persze Mark Zuckerberg egészen más érdektől vezérelve tette ezt.⁶⁸ A szabályozás iránya és tartalma ugyanakkor igencsak eltérő is lehet, és a NetzDG eddigi öt éve alapján aligha várható, hogy hirtelen gombamód bukkannának fel újabb és újabb testvértörvényei, bár időről időre olvasni ilyen törekvésekről híreket.

⁶² Pierwsze tego typu porozumienie. Ministerstwo Cyfryzacji i Facebook. *Portal Gov.pl*, 2018. november 28.

⁶³ Fóris György: Lengyelországban törvény tiltaná a közösségi médiáról való törlést. *Infostart*, 2021. január 13.

⁶⁴ Poland Works on Law Limiting Powers of Facebook, Twitter and Other Social Platforms. *WION*, 2021. január 16.

⁶⁵ Dobozi Gergely: Pénzbüntetéssel sújtaná a facebookos cenzúrát Lengyelország. *Mandiner*, 2020. december 31.

⁶⁶ Paweł Mering: Ministerstwo Sprawiedliwości chce walczyć z fake newsami i hejtem. Nowe przepisy dotyczyćłyby m.in. wpisów w serwisach społecznościowych. *Bezprawnik*, 2020. december 17.

⁶⁷ Sorbán Kinga: A videómegosztóplatform-paradoxon, avagy az új európai szabályok alkalmazhatósága a globalizáció és az eltérő tagállami implementáció keresztmetszetében. *In Medias Res*, 8. (2019), 2. 212.

⁶⁸ Mark Zuckerberg: The Internet Needs New Rules. Let's Start in These Four Areas. *The Washington Post*, 2019. március 30.

Ha elfogadjuk, hogy a törvényalkotás egyben értékválasztás a jogalkotó részéről, hiszen a normaalkotással kijelöl bizonyos, a jog eszközei által is védett értékeket, akkor a NetzDG – és a hasonló testvértörvények – esetében a képviselők a közbeszéd tisztaságát privilegizálták a jogszolgáltatás bizonyos eljárási garanciái vagy a szólásszabadság minél szélesebb érvényesülésével szemben.⁶⁹ Azonban a NetzDG csak egy lehetséges eszközt kínál az online platformok immunitásából eredő szűrkezónával szembeni küzdelemben, de egyelőre nem tűnik mindent elsöprő erejű megoldásnak, semmiképpen sem oldja fel a problémát magát. Persze ez teljes mértékben nem is várható el, hiszen a platformok(on közzétételre kerülő tartalmak) szervesen kapcsolódnak a közösséghez és annak érdeklődéséhez, párhuzamosan pedig a közösség tagjainak cselekedeteihez, problémáihoz, magatartásához, tehát az aktuális társadalmi jelenségekhez és folyamatokhoz. A közösségi média nem az oka, hanem a felülete és „lehetősége” a problémásnak tekintett tartalmak egyre szélesebb terjedésének – az ok azonban a társadalomban magában található, így nem is a tartalomszabályozás fogja megoldani, az legjobb esetben is csak a felszín, a tünetek kezelésére kínálhat részbeni, tehát önmagában nem elégséges eszközt.

Ha párhuzamot keresünk a német és magyar politikai közbeszédben, úgy a bevándorlás és bevándorlásellenesség természetesen itthon is a közvita, sőt a választási kampányok egyik kiemelt témáját szolgáltatja évek óta, és a globális aktuálpolitikai eseményeket ismerve ebben nem várható változás a közeljövőben. Emellett a magyar politikusokat is óriási mennyiségben találják meg a felhasználók a közösségi felületeken, személyeskedő, bántó és megalázó hozzászólásokban nincs hiány, azonban itthon ezekből jellemzően „nem lesznek ügyek”, a nyilvános diskurzusba ezek ritkán kerülnek át. Mindazonáltal bármennyire is izgalmas szabályozási lehetőségnek mutatkozik a NetzDG, egyelőre nem tűnik úgy, hogy a közbeszéd és különösen a közösségi média minőségének javítására a szolgáltatók csendőrszerepe kényszerítése lenne az egyértelmű megoldás.

Felhasznált irodalom

2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről
- Agreement on the Creation of a Contact Point. Online: www.gov.pl/attachment/2b90547d-5b3b-45e9-9dbc-46973aa0b342
- Avia, Laetitia [@LaetitiaAvia]: En 2 mois, David Perrotin a publié 3 articles sur moi. [Thread]. *Twitter*, 2020. május 12. Online: <https://twitter.com/LaetitiaAvia/status/1260308424883134464?s=20>

⁶⁹ A digitális platformok felelősségmegosztásáról lásd Amélie Heldt: Let's Meet Halfway. Sharing New Responsibilities in a Digital Age. *Journal of Information Policy*, 9. (2019); vagy Megregulázni a Facebookot. A közösségimédia-szabályozás dilemmái és lehetséges irányai. A Political Capital kutatása. Budapest, Political Capital – Prága, Heinrich-Böll-Stiftung e.V., 2021.

- Avis relatif à la proposition de loi visant à lutter contre la haine sur internet.* Commission nationale consultative des droits de l'homme. 2019. július 9. Online: <https://perma.cc/HR2L-GH9Q>
- Az Európai Parlament és a Tanács (EU) 2022/1925 rendelete (2022. szeptember 14.) a digitális ágazat vonatkozásában a versengő és tisztességes piacokról, valamint az (EU) 2019/1937 és az (EU) 2020/1828 irányelv módosításáról (digitális piacokról szóló jogszabály). L 265/1 (2022. október 12.)
- Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (2022. október 19.) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (digitális szolgáltatásokról szóló rendelet). L 277/1 (2022. október 27.)
- Az Európai Parlament és a Tanács 2000/31/EK irányelve (2000. június 8.) a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem, egyes jogi vonatkozásairól (Elektronikus kereskedelemről szóló irányelv). L 178/1 (2000. július 17.)
- Baranya Róbert: Nem az államtól kell félni a sajtószabadságot – Koltay András NMHH-elnök a Mandinernek. *Mandiner*, 2022. március 4. Online: https://mandiner.hu/cikk/20220301_media_fuggetlensege_sajtoszabadsag_kozossegi_platformok_koltay_andras_nmhh
- Bartóki-Gönczy Balázs: *Az online közvetítő szolgáltatók mint az információhoz való hozzáférés új kapui*. Budapest, Pázmány Press, 2018.
- Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Kommunikationsplattformen-Gesetz, Fassung vom 24.10.2022. Online: www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20011415
- Décision n° 2020-801 DC du 18 juin 2020.
- Digital 2021: Germany.* Online: <https://datareportal.com/reports/digital-2021-germany>
- Dobozi Gergely: Pénzbüntetéssel sújtaná a facebookos cenzúrát Lengyelország. *Mandiner*, 2020. december 31. Online: https://precedens.mandiner.hu/cikk/20201231_lengyelorszag_kozossegi_media_szigoru_szabalyozas
- Eltávolítások a Hálózati Végrehajtási Törvény alapján. *Google*. Online: https://transparencyreport.google.com/netzdg/youtube?hl=hu&items_by_submitter=period:Y2018H1&lu=items_by_submitter
- Escritt, Thomas: Germany Fines Facebook for Under-reporting Complaints. *Reuters*, 2019. július 2. Online: www.reuters.com/article/us-facebook-germany-fine-idUSKCN1TX1IC
- Fóris György: Lengyelországban törvény tiltaná a közösségi médiáról való törlést. *Infostart*, 2021. január 13. Online: <https://infostart.hu/kulfold/2021/01/13/lengyelorszagban-torveny-tiltana-a-kozossegi-mediaraol-valo-torlest>
- Gemeinsam gegen Hassbotschaften.* 2015. december 15. Online: www.bmjv.de/SharedDocs/Downloads/DE/News/Artikel/12152015_TaskForceErgebnispapier.pdf?jsessionid=65EA1D7E6B-56775F9BB48B4F716E9329.2_cid297?__blob=publicationFile&v=2
- Germany – Twitter Transparency Center. *Twitter*. Online: <https://transparency.twitter.com/en/reports/countries/de.html>
- Gesetzentwurf der Fraktionen der CDU/CSU und SPD.* Deutscher Bundestag: Drucksachen [BT]18/12356, 2017. május 16. Online: <https://dserver.bundestag.de/btd/18/123/1812356.pdf>
- Goujard, Clothilde – Samuel Stolton: Europe Reins in Big Tech: What You Need to Know. *Politico*, 2021. november 25. Online: www.politico.eu/article/europe-digital-markets-act-dma-digital-services-act-dsa-regulation-platforms-google-amazon-facebook-apple-microsoft/
- Heldt, Amélie: Let's Meet Halfway. Sharing New Responsibilities in a Digital Age. *Journal of Information Policy*, 9. (2019), 336–369. Online: www.jstor.org/stable/10.5325/jinfopoli.9.2019.0336#metadata_info_tab_contents

- Heldt, Amélie: Germany is Amending its Online Speech Act NetzDG... But Not Only That. *Internet Policy Review*, 2020. április 6. Online: <https://policyreview.info/articles/news/germany-amending-its-online-speech-act-netzdg-not-only/1464>
- Hertner, Isabelle: Germany: a Country of Immigration – Or Integration? Merkel’s Uncomfortable Legacy. *The Loop*, 2021. április 21. Online: <https://theloop.ecpr.eu/germany-a-country-of-immigration-or-integration-merkels-uncomfortable-legacy/>
- Holmes, Anisa: 87% of Germans Approve of Social Media Regulation Law. Online: <https://medium.com/daliaresearch/87-of-germans-approve-of-social-media-regulation-law-61fb805c1301>
- Hsu, Charlotte: How Media ‘Fluff’ Helped Hitler Rise To Power. *University at Buffalo*, 2015. augusztus 28. Online: www.buffalo.edu/news/releases/2015/08/034.html
- Kayali, Laura – Elisa Braun: France Pushes Tougher EU Rules for Social Media in Wake of Terror Attack. *Politico*, 2020. október 26. Online: www.politico.eu/article/france-renews-social-media-regulation-push-at-eu-level-in-wake-of-terror-attack/
- Klein, Adam G.: How To Fight Holocaust Denial in Social Media – With the Evidence of What Really Happened. *The Conversation*, 2020. december 3. Online: <https://theconversation.com/how-to-fight-holocaust-denial-in-social-media-with-the-evidence-of-what-really-happened-150719>
- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l’économie numérique
- Loi n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet
- Loi n° 2021-1109 du 24 août 2021 confortant le respect des principes de la République
- Löschung rechtswidriger Hassbeiträge bei Facebook, YouTube und Twitter. Ergebnisse des Monitorings von Beschwerdemechanismen jugendaffiner Dienste.* Online: <https://perma.cc/WTX2-XTVF>
- Mchangama, Jacob – Natalie Alkiviadou – Raghav Mendiratta: *Rushing To Judgment: Are Short Mandatory Takedown Limits for Online Hate Speech Compatible with The Freedom of Expression?* Kopenhága, The Future of Free Speech Project – Justitia, 2021. Online: <https://futurefreespeech.com/rushing-to-judgment-are-short-mandatory-takedown-limits-for-online-hate-speech-compatible-with-the-freedom-of-expression>
- Megregulázni a Facebookot. A közösségimédia-szabályozás dilemmái és lehetséges irányai. A Political Capital kutatása.* Budapest, Political Capital – Prága, Heinrich-Böll-Stiftung e.V., 2021. Online: www.politicalcapital.hu/pc-admin/source/documents/pc_boll_megregulazni_a_facebookot_tanulmany_2021.pdf
- Mering, Pawel: Ministerstwo Sprawiedliwości chce walczyć z fake newsami i hejtem. Nowe przepisy dotycząłyby m.in. wpisów w serwisach społecznościowych. *Bezprawnik*, 2020. december 17. Online: https://bezprawnik.pl/ustawa-o-ochronie-wolnosci-slowa/?utm_source=mandiner&utm_medium=link&utm_campaign=mandiner_202111
- Mitchell, Amy – Jeffrey Gottfried – Katerina Eva Matsa: Millennials and Political News. Social Media – the Local TV for the Next Generation? *Pew Research Center*, 2015. június 1. Online: www.journalism.org/2015/06/01/millennials-political-news
- NetzDG Transparenzbericht. *TikTok*. Online: www.tiktok.com/safety/resources/netzdg-jul-dec-2020?lang=de-DE&appLaunch=web
- Neudert, Lisa-Maria N.: Germany: A Cautionary Tale. In Samuel C. Woolley – Philip N. Howard (szerk.): *Computational Propaganda. Political Parties, Politicians, and Political Manipulation on Social Media*. Oxford, Oxford University Press, 2018. 153–184. Online: <https://doi.org/10.1093/oso/9780190931407.003.0008>
- NMHH: *Az elektronikus hírközlési piac fogyasztóinak vizsgálata. Internetes felmérés 2020.* Online: https://nmhh.hu/dokumentum/218531/internetes_felmeres_2020.pdf

- NMHH: *Lakossági internethasználat 2018*. 2019. március 19. Online: http://nmhh.hu/cikk/202179/Lakossagi_internethasznalat_2018
- Papp János Tamás: *A közösségi médiaplatformok szabályozása a demokratikus nyilvánosság védelmében*. Doktori értekezés. Budapest, Pázmány Péter Katolikus Egyetem, 2021.
- Perrotin, David: Laetitia Avia, la députée LREM qui horripile ses assistants. *Mediapart*, 2020. május 12. Online: www.mediapart.fr/journal/france/120520/laetitia-avia-la-deputee-lrem-qui-horripile-ses-assistants?page_article=1
- Pierwsze tego typu porozumienie. Ministerstwo Cyfryzacji i Facebook. *Portal Gov.pl*, 2018. november 28. Online: www.gov.pl/web/cyfryzacja/pierwsze-tego-typu-porozumienie-ministerstwo-cyfryzacji-i-facebook
- Poland Works on Law Limiting Powers of Facebook, Twitter and Other Social Platforms. *WION*, 2021. január 16. Online: www.wionews.com/world/poland-works-on-law-limiting-powers-of-facebook-twitter-and-other-social-platforms-357029
- Première séance du mercredi 13 mai 2020. Online: www2.assemblee-nationale.fr/static/15/scrutins/scrutin_ppl_haine_internet_ld_130520.pdf
- Samuel Paty: French Teacher's Beheading Directly Linked to Social Media Campaign, Say Prosecutors. *Euronews*, 2020. október 21. Online: www.euronews.com/2020/10/21/samuel-paty-french-teacher-s-beheading-directly-linked-to-social-media-campaign-say-prosec
- Schmon, Christoph – Haley Pedersen: Platform Liability Trends Around the Globe: Recent Noteworthy Developments. *Electronic Frontier Foundation*, 2022. június 1. Online: www.eff.org/deeplinks/2022/05/platform-liability-trends-around-globe-recent-noteworthy-developments
- Share of internet users in Germany from 2001 to 2021. Online: www.statista.com/statistics/380514/internet-usage-rate-germany/
- Shed, Sam: Twitter Follows Facebook on Removing Posts That Deny the Holocaust. *CBNC*, 2020. október 15. Online: www.cnn.com/2020/10/15/twitter-follows-facebook-on-removing-posts-that-deny-the-holocaust.html
- Soós Petronella Eszter: Párizs törvénnyel lépne fel az online gyűlölet ellen. *A Tett és Védelem Alapítvány honlapja*, 2020. június 2. Online: <https://tev.hu/parizs-torvennyel-lepne-fel-az-online-gyulolet-ellen/>
- Sorbán Kinga: A videómegosztóplatform-paradoxon, avagy az új európai szabályok alkalmazhatósága a globalizáció és az eltérő tagállami implementáció keresztmetszetében. *In Medias Res*, 8. (2019), 2. 210–229.
- Tatár Attila: A tárhelyszolgáltatók körében felmerülő felelősségi kérdésekről. *Infokommunikáció és Jog*, 72. (2019), 1. 8–13.
- Touchberry, Ramsey: Twitter CEO Says Holocaust Misinformation Does Not Violate Its Policy. *Newsweek*, 2020. október 28. Online: www.newsweek.com/twitter-ceo-says-holocaust-misinformation-does-not-violate-its-policy-1542904
- Törvény a közösségi hálózatokon történő jogérvényesítés javításáról („NetzDG”). *Facebook*. Online: www.facebook.com/help/285230728652028
- Törvény a közösségi hálózatokon történő jogérvényesítés javításáról („NetzDG”). *Instagram*. Online: <https://help.instagram.com/130785144276082>
- Vizvári Soma: A techcégek cenzúrája veszélyes a szólás szabadságára. *Magyar Nemzet*, 2022. július 20. Online: <https://magyarnemzet.hu/belfold/2022/07/a-techcegek-cenzuraja-veszelyes-a-szolas-szabadsagara>

- Von Hein, Matthias: 20 Years After 9/11, Germany Targets Militant Islamists. *Deutsche Welle*, 2021. szeptember 11. Online: www.dw.com/en/9-11-20-years-on-germany-still-grapples-with-militant-islamists/a-59077260
- Willkommenskultur. *Wikipédia*. Online: <https://hu.wikipedia.org/wiki/Willkommenskultur>
- Wilman, Folkert: The EU's System of Knowledge-based Liability for Hosting Service Providers in Respect of Illegal User Content – Between the e-Commerce Directive and the Digital Services Act. *Jipitec*, 12. (2021), 3. 317–341. Online: www.jipitec.eu/issues/jipitec-12-3-2021/5343
- Zódi Zsolt: Az európai platformszabályozás jellegzetességei. In *Medias Res*, 11. (2022), 1. 66–82. Online: <https://media-tudomany.hu/wp-content/uploads/2022/07/mediatudomany-prod.nmhh.hu-az-europai-platformszabalyozas-jellegzetessegei-zodi-zsolt-az-europai-platformszabalyozas-jellegzetessegei.pdf>
- Zuckerberg, Mark [@Mark Zuckerberg]: Today We're Updating Our Hate Speech Policy to Ban Holocaust Denial. [Idővonal-bejegyzés]. *Facebook*, 2020. október 12. Online: www.facebook.com/zuck/posts/10112455086578451
- Zuckerberg, Mark: The Internet Needs New Rules. Let's Start in These Four Areas. *The Washington Post*, 2019. március 30. Online: www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html
- Zurth, Patrick: The German NetzDG as Role Model or Cautionary Tale? Implications for the Debate on Social Media Liability. *Fordham Intellectual Property, Media & Entertainment Law Journal*, 31. (2021), 4. 1084–1153. Online: <https://ir.lawnet.fordham.edu/iplj/vol31/iss4/4>

III. rész

Adatok és normák



Vákát

Menyhárd Attila

Az egészségügyi adatok jogi természete



A jelen tanulmány az adatok jogi természetét a jog belső szerkezete szempontjából vizsgálja. Amellett érvel, hogy az egészségügyi ágazatban keletkező adatok forgalomképessége újszerű gondolkodást igényel, és a szektor számára is számos további következménnyel jár, ideértve a beleegyezés újra-gondolását a szükségességét, illetőleg a készülő európai uniós adatforgalmazási (adatmegosztási) rendeletnek való megfelelés kérdését is.

Személy és tulajdon

A jog belső struktúrájának az alapvető jogi sajátossága, hogy a tárgyi és a társadalmi valóság elemeit két kategóriába sorolja: jogalanyokat és jogtárgyakat feltételez. Bármilyen tárgyi vagy társadalmi valóságban, akár absztrakcióként tételezünk,¹ valamelyik kategóriába besorolható, és ez a besorolás egyúttal szükséges is. A kategorizálás egyúttal kizárólagos: nincs olyan létező (vagy létezőnek tételezett), amely egyikbe sem sorolható be, és olyan sincs, amely mind a kettőbe tartozik. Ez még akkor is igaz, ha a döntés, hogy melyik kategóriába tartozik az adott létező, lehet nehéz,² mert vannak átmeneti állapotok és „szürkezónás” jogi helyzetek is.³

Ez a szerkezeti axióma a polgári jog területén is érvényesül, és számos további, a magánjogi gondolkodásban törvényszerűségnek tekintett tézissel összefügg. Az egyik legalapvetőbb összefüggés az, hogy a jog felépítésében a magánjogi jogviszonyok a jogalanyok között jönnek létre, és a jogtárgyakra vonatkozó jogosultságokat és kötelezettségeket tekintjük a jogviszony tartalmának, az ezekből fakadó és ezekhez mért magatartásokat pedig a jogviszony tárgyának. A jelen tanulmányban bemutatott gondolatmenet szempontjából a tárgyi és a társadalmi valóságnak ez a felosztása elsősorban abból a szempontból releváns, hogy a jogalanyok nem minősülhetnek vagyontárgynak, ezért a jogalanyok személyiségbéli minőségéhez fűződő érdekeket a jog máshogy védi, mint a vagyontárgyakhoz kapcsolódó jogosultságok és kötelezettségek által hordozott érdekeket. A személyiség fogalmának a meghatározására e helyütt nem törekszünk. A jogirodalomban erre

¹ Mint például a jogi személyeket.

² Margaret Jane Radin: Property and Personhood. *Stanford Law Review*, 34. (1982), 5. 957–1015.

³ Ilyen szürkezónás helyzet például az emberi fogantatás és születés közötti életszakasz, ilyen az emberi holttest jogi megítélése vagy a szervek és szövetek jogi minősége is.

számos kísérlet született, amelyek közös jellemzője, hogy képesek megragadni a személyiség valamely jellegzetes vonását, teljes, definitív leírást azonban nem tudnak adni.⁴ Erre a mi gondolatmenetünk szempontjából sincsen szükség. Elegendő számunkra annak a rögzítése, ahogy ez valamennyi, a személy vagy a személyiség meghatározására született definíciókísérletnek is közös eleme, hogy a személy(iség) nem jogtárgy, hanem jogalany. Ez egyúttal azt is jelenti, hogy a személyre és a személyiség részét képező attribútumokra a személyiségvédelem szabályai irányadók, továbbá az a tétel érvényesül, hogy a személyiség és a személyiség részének tekintett attribútumok forgalomképtelenek. Ennek következtében a személyiség és a személyiségjegyek, a személyiség részének tekintett attribútumok nem ruházhatók át, így azok felett másnak rendelkezési jog nem engedhető. Ellenkező esetben a személyiség vagyontárgy lenne, ez viszont ellenétes az uralkodó társadalmi konvencióval. Ezért, ha az adatot forgalomképesnek kell tekinteni, akkor az *per definitionem* nem lehet a személyiség része, és ez fordítva is igaz.

A tulajdonjog *genus proximuma* a tulajdonjogviszony *abszolút szerkezete*. A tulajdonjogot mint abszolút szerkezetű jogviszonyt ezért – annak érdekében, hogy *differentia specificáját* is meg tudjuk határozni – *el kell határolnunk a személyiségi jogoktól mint a magánjogi szabályozás másik abszolút szerkezetű jogviszonyától*. A személyiségi jogoktól való elhatárolás alapja a jogviszony közvetett tárgya közötti különbségtétel, azaz „személy” és „nem személy” (tulajdon) elhatárolása.

A jelen tanulmány középpontjában az egészségügyi adatok átruházhatóságának a vizsgálata áll, az adatok jogi természetének a kontextusában. Az adatok jogi természete a személy és a vagyon („privacy” versus „property”) kettősségére feszül fel. Az adat egyik jellemzője a heterogenitás, és elsősorban ez az akadály annak, hogy az adat jogi minőségére jó válasz legyen adható. Az egészségügyi adatok átruházhatóságának az elfogadását a jelen tanulmány szükségszerűnek tekinti. Strukturális problémaként azonosítja, hogy az átruházhatóság határait az adatok kapcsán nem lehet a személy és a tulajdon (tulajdonjog) szembeállítására mentén meghatározni, és annyiban kell ezt lehetővé tenni, amennyiben azt közérdek támasztja alá. Az adatok értékének allokálásáról jogpolitikai alapon kell dönteni, aminek során az egyéni érdek és a közérdek között kell egyensúlyt találni, ezért az adatok tulajdonjoga nem jó kérdésfeltevés. Újragondolást igényel az egészségügyi adatok feldolgozására vonatkozó tájékozott beleegyezés fogalma, a (feldolgozott) adatokért való felelősség. Kulcsszerepe van az etikai normáknak a helyes (megengedett vagy akár elvárt) és a helytelen (tiltott) magatartások megkülönböztetésében.

⁴ Tattay Levente: *A közszereplők személyiségi jogai*. Budapest–Pécs, Dialóg Campus Kiadó, 2007. 14–15.

Az adatok jogi természete

Az adatok és az információ jogi természetével kapcsolatos kérdésfeltevés a mai formájában a modern gazdaság és a modern társadalom terméke. Az adatok felhasználása kapcsán a jogi kérdésfeltevéseket jelentősen megnehezíti, hogy a fejlődés két fő sávon halad, és ezek a sávok nem ugyanabba az irányba vezetnek. Az egyik, történetileg az iparosodás korai időszakára visszavezethető vonal a gazdasági tevékenység végzése során hasznosítható információ védelméhez és átruházhatóságához kötődik. Ennek mentén merült fel az a gondolat, hogy az üzleti titok, annak egyik megjelenési formájaként pedig a hasznos műszaki-gazdasági ismeret (know-how) a tulajdonhoz (property) hasonló védelmet kapjon, és így annak hasznosítására a jogosult számára a jog monopóliumot biztosítson. Lényegében ez az alapgondolata a szellemi alkotások jogának és a szellemi tulajdon elismerésének is.

A fejlődés másik útja a személyes adatokat és az emberrel kapcsolatos információt vont a magánélethez való jog (privacy) fogalmi ernyője alá. Ennek a célja – szemben a know-how és a szellemi alkotások védelmével – nem az volt, hogy a társadalom és a gazdaság számára értékes ismeretek előállítására ösztönözzön a hasznosítási monopólium biztosításával, hanem azt a szemléletváltást tükrözte, amely üzleti értéktől függetlenül is az egyén privilégiumává tette annak eldöntését, hogy a közösség tagjai számára milyen személyes információt enged át, és annak felhasználását mely feltételek mellett engedi meg. A „privacy” nemcsak egy alkotmányos (emberi) jog, de általános és különös tartalommal bíró jogok gyűjtőfogalma is, amelyet egyébként az Európai emberi jogi egyezmény 8. cikke is példálózó jelleggel felsorol. Ez fordítva is igaz: a magánélethez való jog konkretizált tartalmát nevesített személyiségi jogok adják. Ilyen, a magánélethez való jog általános koncepciója alá vont jog például az egyénre vonatkozó információk, a családi élet, a magánlakás vagy a kommunikáció védelme is. Az egyezmény 8. cikkelye közvetlenül nem az emberi méltóságot védi, hanem a személyiség szabad kibontakozásának lehetőségét biztosítja. A védelem nemcsak természetes személyeket illet meg, hanem megilleti a jogi személyeket is, amennyiben a magánélethez való jog rájuk is értelmezhető.⁵

Az Európai Emberi Jogi Bíróság a magánélet védelmének széles értelmezéséből indul ki, amely a magánkommunikációt, a képmáshoz való jogot, az adatvédelmet és a családi viszonyokat, voltaképpen a magánélethez való jog valamennyi lehetséges aspektusát felöleli.⁶ A Bíróság a döntéseiben nem határozza meg pontosan és nem írja körül kimerítően a magánélet fogalmát, azt nem korlátozza az egyén lakására vagy azokra a helyekre és helyzetekre, amelyek a külvilágtól való visszavonulást szolgálják, hanem kiterjeszti az egyénnek azokra a személyes kapcsolataira is, amelyeket ő a személyiségének kiteljesedése és fejlődése érdekében létesít, ideértve

⁵ EJEB 29197/95 Bernard és mások v. Luxemburg. 1999. június 26.

⁶ Attila Harmathy: On certain Aspects of Privacy. *Annales Universitatis Scientiarum Budapestinensis de Rolando Eötvös Nominatae. Sectio Iuridica*, 46. (2005), 5–27.

azokat a magántermészetű vagy üzleti tevékenységeket is, amelyek a külvilággal való kapcsolatok építését szolgálják.⁷ A magánélethez való jog az egyéni szabadság és a személyiség szabad kibontakozásának a konkretizálása. Az önmeghatározás jogát jelenti. Azt, hogy az egyén önmagát azáltal határozza meg, hogy eldönti, mi az, amit a világ elé tár, és mi az, amit magának megőriz. A jog ebben a tekintetben a folyamatos változás állapotában van, követve a társadalmi igényeket. Számos kérdés jelent majd a jövőben újszerű kihívást, így például az informált beleegyezés megvalósulása, az adatok személyes jellegének kérdései (például az IP-címek személyes adatként való tételezésének kérdése).⁸

Ez a két, teljesen különböző, egyfelől az innovációs ösztönzőként biztosított tulajdoni alapú, másfelől az egyéni önrendelkezést biztosító morális alapú fejlődési vonulat sajátos módon konvergál a jog modern fejlődésében. Ez a sajátosság akként fogalmazható meg, hogy a konvergencia disszonáns. A konvergencia abban jelentkezik, hogy míg az üzleti titok és a know-how kapcsán eredendően természetesnek tekintettük ezeknek az átruházhatóságát, addig a „privacy”-alapú jogvédelem esetén ez korántsem magától értetődő. A személyiségnek is vannak piacképes megnyilvánulásai. Ezek a piacképes megnyilvánulások nem esnek a szellemi alkotásokra vonatkozó szabályozás hatálya alá, és nem minősülnek know-how-nak sem, bár azokhoz hasonlóan maguk is piacképes jószággá válnak. Ennek alapvetően az a feltétele, hogy a jog a felhasználás engedélyezését monopolizálja azzal, hogy csak a jogosult hozzájárulásával tekinti azt jogszerűnek. Márpedig a jogvédelem biztosításából ez is szükségszerűen következik. Az Amerikai Egyesült Államokban a személyiség attribútumainak a felhasználására és annak engedélyezésére a személy számára a magánélet védelmével biztosított jog, a *right of publicity* az elmúlt száz év jogfejlődése során a szellemi tulajdonhoz hasonló forgalomképes jogosultsággá vált. A magánélet védelme tulajdonképpen tulajdonba csúszott át, amennyiben a *right of publicity* alapján az egyén megakadályozhatja a személyiségének a hozzájárulása nélkül kereskedelmi célra való használatát, és lehetővé teszi számára azt, hogy személyiségének megjelenési formáira vonatkozó kizárólagos hasznosítási jogot biztosítson más személyek számára, akik ezt harmadik személyekkel szemben is kikényszeríthetik.⁹ Nagyon hasonló folyamat játszódott le azonban a know-how kapcsán is, amennyiben személyhez fűződő jogként védett műszaki ismeret kizárólagos, harmadik személyekkel szemben is védett átruházását a joggyakorlat és a jogtudomány a forgalomképességet biztosító alanyi jog hiányában is elfogadta. Nem kizárt, hogy a személyek képmásával, hangfelvételével és személyiségük egyéb

⁷ A bíróság a más emberi lényekkel való kapcsolatteremtést a magánélet védelme körébe vonja, kutya tartását azonban nem. EJEB 6825/74 [1976] X v Izland. 1976. május 18.

⁸ Franziska Paefgen: *Der von Art. 8 EMRK gewährleistete Schutz von staatlichen Eingriffen in die Persönlichkeitsrechte im Internet*. Berlin–Heidelberg, Springer, 2016. 233.

⁹ Huw Beverley-Smith – Ansgar Ohly – Agnès Lucas-Schloetter: *Privacy, Property and Personality*. Cambridge, Cambridge University Press, 2005. 65.

megjelenési formáival (például aláírás, név) kapcsolatos felhasználási jogokat a magyar jog a know-how-hoz hasonlóan forgalomképes *in rem* jogosultságnak tekintse, túllépve a magánjog dogmatikai keretein. Ugyanazok az érdekek, amelyek a személyiség megjelenési formáinak a kereskedelmi célú felhasználásához kötődnek, valószínűleg a magyar jogban is indokoltta és szükségessé teszik ezt.

A konvergencia tehát abban mutatkozik meg, hogy a know-how és a privacy (annak keretében pedig az adatok forgalma) egyaránt forgalomképes vagyoni elemmé válhat. A disszonancia ugyanakkor abban van, hogy az adatok kapcsán a jogban erőteljes hangsúly helyeződik a személyes adatok védelmére, miközben a jogosult hozzájárulásával a személyes adatok is forgalomképes vagyoni elemmé válnak. Az adatok forgalomképessége nyilvánvalóan elfogadottnak minősülhet azzal, hogy a digitális tartalmakra és digitális szolgáltatásokra kötött szerződések egyes aspektusairól szóló irányelv¹⁰ 3. cikkelyének (1) bekezdése azokra a szerződésekre is kiterjeszti a hatályát, amelyekben a fogyasztó által vállalt ellenszolgáltatás személyes adatoknak a kereskedő részére való átadásából áll. Az irányelv preambuluma is hosszan igyekszik összhangba hozni az adatok forgalomképességét az adatvédelmi rendelet (GDPR) által biztosított jogvédelem elvi alapjaival. Az adatvédelemnek így más a közjogi és más a magánjogi aspektusa, amit a GDPR-ra épülő európai jogi gondolkodás féloldalasán kezel. Az adatok védelmének a túlhangsúlyozása gyakran vezet olyan gondolatokra, hogy az adatok felett az egyénnek tulajdoni védelmet kellene biztosítani. Ez azonban egyrészt nem lehetséges, másrészt pedig kontraproduktív is. Az adatok felett azért nem lehetséges tulajdoni védelmet biztosítani, mert az adatok nem képeznek homogén halmazt. Nincs olyan közös tulajdonságuk, amely *genus proximum*ként vagy *differentia specific*aként jellemző lenne valamennyi adatra, és így azokból egy egységes halmazt lehetne képezni, vagy más vagyoni elemekről egyértelműen le lehetne őket választani.

A beleegyezés mint paradigma

A forgalomképes és a nem forgalomképes adatok közötti különbségtétel jogpolitikai alapú, mert valójában nem az adat az, aminek az átadására jogi értelemben sor kerül, hanem az adatok felhasználásához adja meg a jogosult a hozzájárulását.

A beleegyezés voltaképpen a jogvédelemről való lemondást jelenti, és egyúttal a forgalomképesség előszobája is. A személyiség (és a személyiségvédelem) részét képező attribútumok kapcsán a jogosult ellenszolgáltatás fejében is lemondhat a jogvédelemről, áruvá téve ezáltal a személyiségjegyeit, szélesebb értelemben

¹⁰ Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on Certain Aspects Concerning Contracts for the Supply of Digital Content and Digital Services. L 136/1 (2019. május 22.).

a személyiségét. A „privacy”-alapú jogvédelem és a know-how- (vagy tulajdoni) alapú jogvédelem így a jogosult beleegyezésén keresztül átjárhatóvá válnak.

A beleegyezés a társadalmi kapcsolatoknak és a jognak is komplex és elmosódó kontúrokkal leírható jelensége, az adatok felhasználása szempontjából pedig az teszi kulcsfontosságúvá, hogy a „privacy” alapú adatvédelmi megközelítés az adatokat a személyiség részének tekinti. A személyiségi jogokba való beavatkozást pedig a jogosult hozzájárulása teszi jogszerűvé. Az már önmagában is kérdés, hogy a jog milyen keretek között engedi meg a jogosult számára azt, hogy a beleegyezésével jogszerűvé tegye a személyiségi jogaiba való beavatkozást. Vannak olyan személyiségi jogok (például az élethez való jog), amelyek esetében a jog nem, vagy csak rendkívül szűk, szabályozott körben teszi lehetővé (orvosi kezeléstről való lemondás) azt, hogy a jogosult a beleegyezésével jogszerűvé tegye a beavatkozást. Vannak olyan személyiségi jogok is, amelyek esetében a jog lehetővé teszi azt, hogy az azokba való beavatkozást a jogosult a beleegyezésével jogszerűvé tegye, azonban nem engedi a jog, hogy ez ellenérték fejében történjen. Ebben a körben is lehetséges, hogy csak hozzátartozók körében jogszerű az ilyen beleegyezéssel való beavatkozás (szervek és szövetek átengedése, béranyaság). Vannak olyan személyiségi jogok is, amelyek kapcsán a beleegyezés csak bizonyos, jellemzően időbeli korlátok között megengedett (például rabszolgaság tilalma). Vannak továbbá olyan személyiségi jogok, amelyek tekintetében a jogosult teljesen szabadon dönt arról, hogy ingyenesen vagy visszatérően, és milyen megszorításokkal (vagy azok nélkül) egyezik bele a személyiségi jogba való beavatkozásba (például képmáshoz, hangfelvételhez való jog).

Abban a téren, amelyben a beleegyezés jogszerűvé teheti a személyiségi jogba való beavatkozást, további kérdések vizsgálata szükséges annak megállapításához, hogy a jogosult nyilatkozata valóban érvényes beleegyezésnek minősülhet-e. Ez számos tekintetben nem jogi, hanem társadalmi kérdés. A beleegyezés – explicit vagy implicit módon kommunikált – feltételei, a jogosult feltevései, a beleegyezés visszavonása, annak önkéntessége és informáltsága mind olyan kérdések, amelyek az adott helyzetben figyelembe veendőek annak megállapításához, hogy a hozzájárulás ténylegesen megadottnak tekinthető-e. A társadalmi konszenzus ebben változhat is. Az internetes kommunikáció struktúrája éppúgy formálja ezt a képet, ahogy a „Metoo” mozgalom is, és egyúttal fel is veti a beleegyezés elmosódó határaiból adódó bizonytalanságok kockázatának a telepítését is. A határok többnyire azért mosódnak el, mert a felek kommunikációja nem feltétlenül egyértelmű, mögöttes feltevéseken alapulhat, és sokszor az sem világos, hogy pontosan mi a beleegyezés terjedelme. Ennek fényében teljes mértékben megalapozottnak tűnik az a felvetés, hogy a beleegyezés egy mozgó skála, amelyen az elvárások az eset konkrét körülményeinek, az érintett személyiségi jogi jogosultság súlyának, az autonómia veszélyeztetettségének a mentén formálódnak.¹¹ Az tehát, hogy a jogosult

¹¹ Nancy S. Kim: *Consentability. Consent and Its Limits*. Cambridge, Cambridge University Press, 2019. 81.

nyilatkozata beleegyezésként jogszerűvé tette-e a személyiségi jogosultságba való beavatkozást, kontextustól függ, ami ugyanakkor túl sok bizonytalanságot is eredményez.

Bármely döntés akkor tekinthető autonóm döntésnek, ha önkéntes és informált, azaz ha nem kényszer hatására született. Ezért paradigmaticus tétele az orvosi jogviszonyoknak is a tájékozott beleegyezés. A tájékozott beleegyezés a beteg önrendelkezési jogának a lenyomata, és azt feltételezi, hogy a döntés meghozatala során a jogosult minden, számára lényeges körülményt figyelembe vehetett. Ehhez természetesen meg kell hogy ismerje ezeket a körülményeket. A tájékozott beleegyezés elve az orvos-beteg jogviszony kapcsán fogalmazódott meg hangsúlyosan, valójában azonban olyan általános követelmény, amelynek érvényesülése nem korlátozódik a társadalmi viszonyoknak (jogviszonyoknak) meghatározott körére. A személyiségi jogokat érintő – így többek között az adatok kezelésébe, felhasználásába és átruházásába való – beleegyezésnek is feltétele a beleegyezés önkéntessége és informáltsága. Az más kérdés, hogy az információhiány kockázatát a jog akkor telepíti a másik félre, ha az tudott volna tenni a jogosult információhiányának a megelőzésére vagy kiküszöbölésére. Ezt az elvárást közvetíti a tájékoztatási kötelezettség.

Az egészségügyi adatok felhasználásával kapcsolatos tájékozott beleegyezés anynyiban mindenképpen újragondolást igényel, hogy az adatok további felhasználása a hozzájárulás megadásának időpontjában a hozzájárulás jogosultja számára sem ismert.¹² A feldolgozással az adatok elveszíthetik a személyes jellegüket, és olyan információvá is válhatnak, amelynek a jogosultja az, aki az adatok feldolgozásával azt előállította. Pillanatnyilag nem világos, hogy ezeknek az adatoknak a jogosulti pozícióit hogyan lenne helyes allokálni. Ettől függetlenül azonban még igaz, hogy ha az eredeti jogosult a hozzájárulását visszavonja, vagy a hozzájáruló nyilatkozatát például tévedésre vagy megtévesztésre hivatkozva megtámadja, akkor az adat feldolgozása jogellenessé válik, és így azzá válik az ezzel előállított új adat vagy információ is.

Az egészségügyi adatok felhasználásával szerzett haszon allokálása; az egészségügyi adatok „monetizálása”

Az egészségügyi adatok kapcsán szinte természetesen adódik a közvélekedés számára az, hogy azok – éppen az érzékenységük miatt – feltétlen védelmet kell hogy kapjanak. Az egészségügyi adatok sajátossága azonban az is, hogy a felhasználásukkal mások életének vagy egészségének a védelmét lehet hatékonyabbá tenni. A felhasználás azonban olyan piaci szereplők (gyógyszergyárok, egészségügyi szolgáltatók) közvetítésével valósul meg, akiknek a számára ez haszonszerzéssel

¹² Anne S. Y. Cheung: Moving Beyond Consent for Citizen Science in Big Data Health and Medical Research. *Northwestern Journal of Technology and Intellectual Property*, 16. (2018), 1. 39.

járó üzleti tevékenység. Emellett ugyanakkor a felhasználás közérdek is. Ezért már önmagában annak a kérdésnek a megválaszolása is jogpolitikai döntést igényel, hogy az adatjogosult megtagadhatja-e az adatainak továbbításához és feldolgozásához való hozzájárulást akkor, ha ezzel másokat, vagy esetleg a társadalom szélesebb körét segíti a gyógyulásban vagy abban, hogy csökkentsék a megbetegedés kockázatát. Ebben az esetben ugyanis az ehhez fűződő közérdek felülírja az adatok védelmét megalapozó magánérdeket.

Az adatok felhasználása ebben a szektorban is rendszerint haszonszerzéssel jár, még akkor is, ha nem közvetlenül irányul erre az adatok felhasználásával járó, jellemzően kutatási tevékenység. Ennek kapcsán több kérdés is felmerül. Az egyik kérdés az, hogy a tájékoztatás ki kell-e hogy terjedjen arra, hogy a kutatás potenciálisan haszonszerzéssel jár. Mivel a jogosult számára lényeges kérdés lehet, hogy az adatainak a felhasználásával milyen cél vagy eredmény megvalósulását támogatja, erre a kérdésre azt a választ kell adnunk, hogy a felhasználásra vonatkozó tájékoztatást, ideértve az azzal járó üzleti lehetőséget is, a jogosult számára meg kell adni. Ennek az elmulasztása a nyilatkozatot megtámadhatóvá teszi, amelyre a szerződés érvénytelenségének a következményeit kell alkalmazni, azzal, hogy ebben a helyzetben az eredeti állapot jellemzően nem állítható helyre.

Ennek logikus következménye lehet, hogy a jogosult jogalap nélküli gazdagodási igényt érvényesíthet azzal az intézménnyel vagy vállalkozással szemben, amely az adatainak a felhasználásával haszonra tett szert.¹³ Bár ez logikus következmény, a hatása társadalmi szinten negatív, mert visszafogja az innovációt.

Érdemes ennek kapcsán átgondolni annak a jogpolitikai megfontolásnak az adatok felhasználásra való adaptálását, amelyet egy amerikai felsőbbbíróság a Moore-ügyben¹⁴ megfogalmazott. Ez az eset az embernek a teste feletti rendelkezési jogát helyezte sajátos módon vagyoni jogi kontextusba, ezért kézenfekvő lehet az analógia az adatok feletti rendelkezési joggal. Az eset a tényállásánál fogva bármilyen jogi környezetben előfordulhat, és a válasz sem függ jogrendszerbeli sajátosságoktól. Ezért általános tézisként is megfontolandó az amerikai bíróság érvelése. Az eset tényállása szerint a leukémiában szenvedő felperes lépét a gyógyulása érdekében az UCLA Medical Centerben eltávolították. A beavatkozás sikeres volt, eredményeként a felperes meggyógyult. A műtét előtt a felperes beleegyezett abba, hogy eltávolított lépét tudományos célokra felhasználják, és abba is, hogy a műtétet követő kontrollvizsgálatok során további sejtmintákat vegyenek tőle. Ez meg is történt. A felperes sejtjei – ahogy ezt az orvosok a felhasználásba való beleegyezés előtt már gyanították – olyan egyedi tulajdonsággal rendelkeztek, amely a tudományos

¹³ A magyar jogi környezetben ez következik a Ptk. 2:51. § (1) bekezdés f) pontja szerinti rendelkezésből is, amely szerint az, akinek a személyiségi jogába jogellenesen beavatkoztak, kérheti azt, hogy a jogsértő vagy jogutódja a jogsértéssel elért vagyoni előnyt engedje át a javára a jogalap nélküli gazdagodás szabályai szerint.

¹⁴ John Moore v. Regents of University of California et al. 739 P. 2d 479 (Cal 1990).

vizsgálatokat és mintavételeket követő továbbtenyésztés eredményeként lehetővé tette, hogy abból annak szabadalmaztatása után a gyógyászatban hasznosítható anyagot állítsanak elő. Az orvosok az előállított anyag felhasználási jogát nagyon komoly haszon ellenében adták el egy gyógyszergyárnak. A felperes a keresetét az egyébként a tulajdoni igények megsértése esetén alkalmazható *tort of conversion*ra alapította, amit a bíróság elutasított.

A kereset elutasításának az indokolása során a bíróság megállapította, hogy „[...] a felelősség, amelynek megállapítását Moore szorgalmazza, azzal fenyeget, hogy megsemmisíti a fontos orvosi kutatások végzésének gazdasági ösztönzését”. Ha a sejtek kutatásban való felhasználása tulajdonjogi jogsértés, ahogy azt a felperes állítja, akkor az olyan, mintha a felhasználással a kutató „peres lottót” vásárolna. A bíróság megállapítása szerint „valószínűtlen, hogy vállalatok nagy összegeket fektetnének egy termék fejlesztésébe, gyártásába vagy forgalmazásába, ha bizonytalan felette a rendelkezési joguk”. Véleményünk szerint „[i]lyen körülmények között nem észszerűtlen azt a következtetést levonni, hogy a szigorú felelősség nem szolgálná az e fontos termékek fejlesztéséhez és hozzáférhetőségéhez fűződő közérdeket”.¹⁵

A bíróság megállapította ugyanakkor azt is, hogy az orvosok jogsértő módon jártak el, amikor a felperest a beleegyezés előtt nem tájékoztatták arról, hogy a tudományos szempontokon túlmenően saját érdekükben, kereskedelmi hasznosításra alkalmas anyag előállítása érdekében is történnek a vizsgálatok. Ebből ugyanakkor nem vont le olyan következtetést, hogy a felperest akár tulajdoni igényként (*tort of conversion*), akár jogalap nélküli gazdagodási igényként (*unjust enrichment*) megilletné bármilyen kompenzáció, részesedés vagy megtérítési igény. A döntés jogpolitikai indoka világos: a haszonból való részesítés jobb esetben jelentős mértékben megdrágítaná a kutatásokat, rosszabb esetben azonban meg is gátolná azokat, mert a kutatásban részt vevő intézmények és orvosok számára kiszámíthatatlan kötelezettséget és ezzel kiszámíthatatlan kockázatot teremtené. A bíróság számára döntő szempontnak a közérdeket szolgáló orvosi kutatások ösztönzése bizonyult.

Ezzel együtt ellentmond egymásnak egyfelől az a konklúzió, hogy tájékoztatási kötelezettségüknek a kutatást végző orvosok nem tettek eleget, másfelől pedig az a döntés, hogy a felperesnek nem jár kompenzáció, és ezért a keresetet el kell utasítani. Logikus csak akkor lehet a döntés, ha azt feltételezzük, hogy a felperest hozzájárulási kötelezettség terheli olyan esetben, amelyben az adatainak felhasználása közérdeket szolgál, függetlenül attól, hogy a felhasználó azon profitot szerez-e, vagy sem. Lényegében hasonló volt a társadalmi reakció a Covid-19 által előidézett vírushelyzetben is. A vértesztekből nyerhető genetikai és egyéb adatok az oltások fejlesztését szolgálták, ezért közérdek támasztotta alá azoknak a felhasználását.

Ami a tájékoztatást illeti, ennek már azzal is eleget tud tenni a kutatási célú adatfelhasználáshoz hozzájárulást kérő orvos, hogy feltárja a kutatás mögött álló iparági szereplőt. Az, hogy a piaci szereplő (gyógyszergyár, orvosi műszereket

¹⁵ John Moore v. Regents of University of California et al. 739 P. 2d 479 (Cal 1990). 146. bekezdés.

és segédeszközöket gyártó cég, egészségügyi szolgáltató) profitra törekszik, olyan köztudomású tény, amelyről a tájékoztatás észszerűen nem lehet szükséges.

Az egészségügyi adatok forgalomképessége

A digitális vagyontárgyak jogi minősége kapcsán az elméleti megközelítések elsősorban azzal foglalkoznak, hogy azok a tulajdonjog tárgyainak a körébe sorolhatók-e. Ez a rendszertani szemlélet azt a kérdést teszi fel, hogy a magánjogi dogmatika meglévő fogalmi rendszerébe és struktúrájába miként illeszthetők azok az immateriális javak, amelyek anyagi értékkel bírnak. A kérdésfeltevés lényegében párhuzamos azzal, hogy a személyiség forgalomképes attribútumai miként illeszkednek ebbe a rendszerbe. Ez a megközelítés több szempontból sem tud eredményes lenni. Egyfelől ragaszkodik ahhoz, hogy megfelelően címkézett jogi dobozokba rakja a gazdasági és társadalmi jelenségeket, miközben a központi kérdés az, hogy ezek a javak átruházhatók és ekként jogi értékkel bírnak-e. Erre a választ az élet és a jog már megadta.

Ha a jog elfogadja, hogy a jogosult a személyiségjegyeinek – köztük a személyes adatainak – a felhasználásához akár ellenérték fejében, haszonszerzési céllal hozzájáruljon, és így azt jogszerűvé tegye, nincs ok arra, hogy azt ne kezelje forgalomképes vagyoni elemként.¹⁶ Ez igaz az egészségügyi adatokra is. Ezzel együtt merül fel az a kérdés is, hogy ha valaki meghal, akkor ki kapja meg a személyiségjegyeinek (és adatainak) a felhasználásával kapcsolatos jogosultságokat. A polgári jog logikus és őszinte válasza erre az, hogy a jogosult örökösei, akik egyébként nem feltétlenül azonosak a kegyeleti jog jogosultjaival.

Rendelkezés az elhunyt személy személyiségi attribútumaival

A magyar jog kapcsán abból biztosan ki lehet indulni, hogy a Polgári Törvénykönyvről szóló 2013. évi V. törvény (Ptk.) 2:42. § (3) bekezdésében foglalt rendelkezés alapján – összhangban a korábbi polgári jogi szabályokkal és a nemzetközi trendekkel – az érintett hozzájárulása jogszerűvé teszi a személyiségi jogába való beavatkozást. A Ptk. rendelkezései és a bírói gyakorlat alapján olyan személyiségi jogok esetében, amelyek az egyént a társadalom számára jelenítik meg (különösen a képmáshoz, aláírásképhez, hangfelvételhez, névhez, valamint egyéb külső személyiségjegyekhez fűződő jogok), elfogadott az is, hogy az érintett ellenszolgáltatás fejében engedjen másoknak olyan jogot, amely ezeknek a személyiségjegyeknek a hasznosításához fűződik. Ugyanez vonatkozik a magántitok és a személyre

¹⁶ Menyhárd Attila: Forgalomképes személyiség? In Menyhárd Attila – Gárdos-Orosz Fruzsina (szerk.): *Személy és személyiség a jogban*. Budapest, Wolters Kluwer, 2016. 82.

vonatkozó adatok felfedéséhez és hasznosításához való jogra is. Ezeknek a személyiségjegyeknek a feltárására, illetőleg hasznosítására biztosított jogosultság a személyiségi jog jogosultja javára fennálló vagyoni értékű joggá is, tehát kettős természetű joggá válik. A jog gyakorlása útján vagyoni értékű jog keletkezik annak a személynek a vagyonában, akinek javára a hasznosítást az érintett engedélyezte.

Az örökös az örökhagyó egyetemes jogutódja (Ptk. 7:1. §). A hagyaték részét képezik mindazok a vagyoni elemek, amelyek átszállását a jog nem zárja ki, függetlenül attól, hogy azok dolgok, követelések, jogok vagy szerződési pozíciók. Ezek közé tartoznak azok a vagyoni elemek is, amelyeket a jog által hasznosíthatónak tekintett személyiségi jogok képeznek. Az örökhagyó személyiségi jogai a jogi természetüknél fogva megszűnnek az örökhagyó halálával, az örökhagyónak a személyiségjegyei azonban továbbra is hasznosítható javak (vagyontárgyak) maradnak. E személyiségjegyek hasznosításának a joga a hagyatékkal együtt, annak részeként az örökhagyó halálával az örökös(ök)re száll át.

Az örökhagyó halála nem szünteti meg azokat a szerződéseket, amelyeket az örökhagyó még életében ezeknek a személyiségjegyeknek a hasznosítására kötött (kivéve azt az esetet, ha a felek a személyiségi jog jogosultja halálát szerződésmegszüntető okként határozták meg). Ezekben a szerződésekben az örökhagyó szerződési pozíciója képezi a hagyaték részét, és az örökösökre az örökléssel az örökhagyó szerződési pozíciója száll át. Annak sincsen akadálya, hogy az örökhagyó a hasznosítható személyiségjegyeknek a hasznosítási jogáról a végintézkedésekre vonatkozó általános szabályok szerint a végintézkedésében rendelkezzen. Ennek keretében kijelölheti azokat a személyeket, akik ezeknek a személyiségjegyeknek a hasznosítására jogosultak, illetőleg azokat, akiknek a hozzájárulása a személyiségjegyek jogszerű hasznosításának a feltétele.

Eltérő rendelkezés hiányában az örökösöket ezek a jogosultságok és e jogosultságok gyakorlásának a hasznai jogközösségként illetik meg. A jogosultaknak a hasznosítás kapcsán meghozandó döntésére, a döntés megtámadhatóságára és a döntés hiányában alkalmazandó eljárásra a Ptk. 5:78–79. §-aiban a közös tulajdon tárgyának a hasznosítására vonatkozó rendelkezéseket kell megfelelően alkalmazni.

Ezek a rendelkezési jogok nem érintik a Ptk. 2:50. §-ában foglalt kegyeleti jog tartalmát és a kegyeleti jog megsértése kapcsán a kegyeleti jog alapján jogosított személyek fellépését és igényérvényesítését. A kegyeleti jog megsértése esetén a Ptk. 2:50. §-a alapján a hasznosítási jogot engedő örökössel és a hasznosítási jog jogosultjával szemben is fel lehet lépni, amennyiben a hasznosítás az elhunyt személy emlékét sérti.

A 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.) 25. §-a is próbál erre a helyzetre szabályozást adni, azonban ezt más síkon teszi, és nem is konzekvensen, mert csak az elhunyt személyt életében megillető jogok gyakorlásáról rendelkezik, anélkül, hogy a jogosult személyét azonosítaná.

Vállalatfelvásárlás

Az adatok forgalomképessége kapcsán nemcsak a szerződéses és az öröklési viszonyok relevánsak, hanem a vállalatfelvásárlási helyzetek is. A vállalatok szerkezeti átalakulásai jogutódlással eredményeznek alanyváltozást a jogosulti és kötelezeti pozíciókban. Ezekben a helyzetekben a jogutódlás *ipso iure* történik. Amennyiben az átalakulásban részt vevő jogelőd vállalat adatok felhasználásával kapcsolatos jogosultságokat szerzett – például az általa kötött szerződések alapján –, akkor ezekben is bekövetkezik a jogutódlás. Az adat eredeti jogosultja számára ugyanakkor ez jelentős változás, mert kihatással lehet az adatok felhasználásával keletkező haszonallokálására és arra, hogy azt mire fordítják.

Amennyiben a vállalatnak az M&A tranzakció során való megszerzése azzal járhat, hogy a vállalat megszerzője az adatok eredeti jogosultjainak a döntése vagy a jogi környezet sajátosságai folytán elveszítheti az adatok felhasználásához való jogosultságot, akkor ez negatív ösztönzőként akadályozhat olyan piaci mozgásokat, amelyek egyébként növelnék az adott ágazat működésének a hatékonyságát. Általában véve is viszonylag kevés szó esik az adatok felhasználásával kapcsolatos jogosultságoknak és az erre irányuló szerződéses kötelezettségeknek a viszonyáról. Még kevesebb szó esik ugyanakkor arról, hogy az adatok védelme és átruházhatósága hogyan jelenik meg a vállalkozások szerkezeti átalakulásainak az összefüggéseiben, és hogy ebből a szempontból milyen lenne az optimális jogi környezet.

A készülő adatforgalmi rendelet lehetséges hatásai

Az elfogadás előtt álló, úgynevezett Data Act¹⁷ az európai uniós adatjogi szabályozás újabb pilléréként a nem személyes adatok feletti hasznosítási jogok allokálásáról szól. Az érintettek közötti jogviszonyt a tervezet nem érinti. A jogosultság allokálása a felek közötti szerződéssel elsősorban a szerződések jogszerűségének a tartalmi korlátai között lehet kikényszeríthető, mindenekelőtt a tisztességtelen szerződési kikötések kontrollja alapján.

A készülő rendelet középpontjában a nem személyes ipari adatok és a dolgok internetéhez kapcsolódó termékek terjedésével keletkező adatok felhasználási jogosultságainak az allokálása áll. A szabályozás nem fogyasztóvédelmi szempontú, hanem a piaci és a kormányzati szereplőkre fókuszál, az adatáramlás, az adathozzáférés és az adatfelhasználás megkönnyítése a célja. Elő kívánja továbbá segíteni a felhő- és peremszolgáltatások közötti váltást, valamint elvárja az ágazatok között újrafelhasználható adatok interoperabilitási szabványainak a kidolgozását.

¹⁷ European Commission: *Proposal for a Regulation of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data. (Data Act)*. COM(2022)68 végleges (2022. február 23.).

Az európai jogalkotó várakozásai szerint így jóval több adat válik majd hozzáférhetővé. A Bizottság várakozása szerint az új szabályok 2028-ig várhatóan 270 milliárd euró többlet-GDP-t eredményeznek. Becslések szerint ugyanis a rögzített adatoknak csak 20%-át használják fel, a többi elveszik a piac számára. Azzal, hogy a rendelet korlátozza a monopolhelyzetek kihasználhatóságát, hozzáférhetővé teszi az eddig monopolizált és nem hozzáférhető adatokat is. A rendelet a tárgyi hatálya folytán valamennyi szektort, így az egészségügyi ágazatot is érinteni fogja. Kiterjed a termékek vagy kapcsolódó szolgáltatások használata révén generált adatok rendelkezésre bocsátására az adott termék vagy szolgáltatás felhasználója számára, az adatok adattulajdonosok általi rendelkezésre bocsátására az adatátvevők számára, valamint az adatok adattulajdonosok általi, rendkívüli szükséglet alapján való rendelkezésre bocsátására a közsférabeli szervezetek vagy uniós intézmények, ügynökségek vagy szervek számára, közérdekű feladataik ellátása érdekében.

A mesterséges intelligencia által vezérelt eszközök a gyártó számára jellemzően kizárólagos hozzáférést biztosítanak az eszköz által generált adatokhoz (adatmonopólium), ami lehetővé teszi exkluzív adatvezérelt szolgáltatások értékesítését a felhasználók számára. A vállalkozás a tevékenysége során keletkező ipari és kereskedelmi adatokhoz nem fér hozzá (a természetes személy sem a tevékenysége szempontjából releváns, nem személyes adatokhoz), és nem használhatja azokat más célokra, illetve nem juthat konkurens adatalapú szolgáltatásokhoz. Ez torzíja a versenyt az adatalapú szolgáltatások piacain, és ez az a jellegzetes helyzet, amelyre a rendelet megoldást kínál.

A javaslat a hatályát a fizikai eszközök által generált adatokra korlátozza. Ebben a körben nem teljesen világos a „termék” és a „nem termék” által generált adatok közötti különbségtétel alapja. A rendelet alkalmazásában termék az, ami a környezetre vonatkozó adatokat szerez, generál vagy gyűjt, és amely képes ezeket az adatokat nyilvánosan elérhető elektronikus kommunikációs szolgáltatáson keresztül továbbítani (IoT). Egyes termékek, amelyeket elsősorban tartalom megjelenítésére vagy lejátszására, illetve tartalom rögzítésére és továbbítására terveztek, nem tartoznak a rendelet hatálya alá, így nem tartoznak ide a személyi számítógépek, szerverek, táblagépek és okostelefonok, kamerák, webkamerák, hangrögzítő rendszerek és szövegolvasók. A „gépek” és a számítástechnikai eszközök közötti különbségtételnek az a következménye, hogy a mobileszközös vagy számítógépes eszközök alkalmazásai nem tartoznak a rendelet alkalmazási körébe.

A gyártó alapvető kötelezettségei közé tartozik a termékek vagy a kapcsolódó szolgáltatások használata révén generált adatok hozzáférhetővé tétele. Ezzel párhuzamosan biztosítja a rendelet a jogot a felhasználóknak a termékek vagy a kapcsolódó szolgáltatások használata révén generált adatokhoz való hozzáféréshez, továbbá az adatok harmadik felekkel való megosztásához. Biztosítania kell továbbá a gyártónak az interoperabilitást.

A Data Act jelentős hatással fog járni az egészségügyi szektorban is, amelynek részletes elemzésére egy másik tanulmányban kerül majd sor. Ebben az ágazatban

az adatmonopólium megszüntetését a közérdek különös súllyal támasztja alá, miközben az innovációra való ösztönzés szintjének csökkenése is különösen érzékeny társadalmi következményekkel jár.

Összegzés

Az adat és információ olyan, jogilag védett érdek, amelyről a jogosult lemondhat, és ezzel forgalomképesévé teheti. A know-how és a személyes adat, bár különböző fejlődés mentén, egyaránt forgalomképes vagyoni elemmé válhat. Az adatok kapcsán a jogban erőteljes hangsúly helyeződik a személyes adatok védelmére, miközben a jogosult hozzájárulásával a személyes adatok is forgalomképes vagyoni elemmé válnak. Az adat nem képez homogén szabályozási tárgyat, és forgalomképesége is jogpolitikai alapon dől el. Ebben kiemelkedő jelentősége van a közérdek prioritásának, mert ez határozza meg, hogy milyen irányban helyes a jognak ösztönzőket biztosítania. A jog belső szerkezeti felépítése, így a tulajdon és a személy közötti különbségtétel nem ad segítséget a forgalomképes és a nem forgalomképes adat közötti különbségtételhez. Az adatok forgalomképesége kapcsán nemcsak a szerződéses jogviszonyok kapnak jelentőséget, hanem a vállalati átalakulások is. Az erős jogvédelem gátolja az egészségügyi szektorban működő magánvállalkozások szerkezeti változásait, és így a piaci hatékonyság ellen hatnak. A tájékozott beleegyezés elvét elsősorban abból a szempontból kell felülvizsgálni, hogy az egészségügyi adat felhasználásához hozzájárulást kérő piaci szereplő maga sem tud teljes körű tájékoztatást adni a várható további felhasználásokról. További megfontolást igényel a hozzájárulás korlátainak és visszavonhatóságának a meghatározása.

A forgalomképes és a nem forgalomképes adatok közötti különbségtétel jogpolitikai alapú. Valójában nem az adat az, aminek az átadására jogi értelemben sor kerül, hanem az adatok felhasználásához adja meg a jogosult a hozzájárulását. A beleegyezés a társadalmi kapcsolatoknak és a jognak is komplex és elmosódó kontúrokkal leírható jelensége, az adatok felhasználása szempontjából pedig az teszi kulcsfontosságúvá, hogy a „privacy”-alapú adatvédelmi megközelítés az adatokat a személyiség részének tekinti. Az egészségügyi adatok kapcsán szinte természetesen adódik a közvélekedés számára az, hogy azok – éppen az érzékenységük miatt – feltétlen védelmet kell hogy kapjanak. Az egészségügyi adatok sajátossága azonban az is, hogy a felhasználásukkal mások életének vagy egészségének a védelmét lehet hatékonyabbá tenni. A felhasználás viszont olyan piaci szereplők közvetítésével válsul meg, akiknek a számára ez haszonszerzéssel járó üzleti tevékenység, miközben a felhasználás közérdek is. Ezért már önmagában annak a kérdésnek a megválaszolása is jogpolitikai döntést igényel, hogy az adatjogosult megtagadhatja-e az adatainak a továbbításához és feldolgozásához való hozzájárulást akkor, ha ezzel másokat, vagy esetleg a társadalom szélesebb körét segíti a gyógyulásban vagy abban, hogy

csökkentsék a megbetegedés kockázatát. Ebben az esetben ugyanis az ehhez fűződő közérdek felülírja az adatok védelmét megalapozó magánérdeket.

Felhasznált irodalom

- Beverley-Smith, Huw – Ansgar Ohly – Agnès Lucas-Schloetter: *Privacy, Property and Personality*. Cambridge, Cambridge University Press, 2005.
- Cheung, Anne S. Y.: Moving Beyond Consent for Citizen Science in Big Data Health and Medical Research. *Northwestern Journal of Technology and Intellectual Property*, 16. (2018), 1. 15–4.
- Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on Certain Aspects Concerning Contracts for the Supply of Digital Content and Digital Services. L 136/1 (2019. május 22.).
- European Commission: *Proposal for a Regulation of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of data (Data Act)*. COM(2022)68 végleges (2022. február 23.)
- Harmathy, Attila: On Certain Aspects of Privacy. *Annales Universitatis Scientiarum Budapestinensis de Rolando Eötvös Nominatae. Sectio Iuridica*, 46. (2005), 5–27.
- Kim, Nancy S.: *Consentability. Consent and Its Limits*. Cambridge, Cambridge University Press, 2019.
- Menyhárd Attila: Forgalomképes személyiség? In Menyhárd Attila – Gárdos-Orosz Fruzsina (szerk.): *Személy és személyiség a jogban*. Budapest, Wolters Kluwer, 2016. 65–82.
- Paefgen, Franziska: *Der von Art. 8 EMRK gewährleistete Schutz von staatlichen Eingriffen in die Persönlichkeitsrechte im Internet*. Berlin–Heidelberg, Springer, 2016.
- Radin, Margaret Jane: Property and Personhood. *Stanford Law Review*, 34. (1982), 5. 957–1015.
- Tattay Levente: *A közszereplők személyiségi jogai*. Budapest–Pécs, Dialóg Campus Kiadó, 2007.

Vákát

Pümkösty András

A nagy adathalmazok felhasználásának etikai kérdései – avagy szükség van-e adatetikára?



Az adat nélkülözhetetlen bemeneti forrása a technológiai fejlődésnek. A mesterségesintelligencia-alapú megoldások a tanító adatok, valamint az algoritmusok minőségén múlnak. A nagy technológiai vállalatok üzleti modellje számos esetben a kiterjedt adatfelhasználásra épül. Az európai uniós jogalkotás egyre nagyobb hangsúlyt fektet – az adatvédelmi megközelítés mellett – az adat gazdasági jelentőségének kiaknázására, mégis kevés figyelem hárult a magyar diskurzusban az adatok felhasználásának etikai kérdéseire. Jelen cikk a nagy adathalmazokkal (big data) kapcsolatos etikai dilemmákat rendszerezi, amely megközelítésben kitér az üzleti etika, alkalmazott etika szempontjai mellett az akadémiai adatetika megalapozásának igényére. A cikk amellet érvel, hogy az adatetika művelése hozzájárulhat a technológiával kapcsolatos helyes bizalom kialakításához, egyúttal fontos hozzájárulást jelent a megfelelő technológiai szabályozás megalkotásához.

Bevezetés

Alapvető kérdés, hogy vajon a technológia és tudomány fejlődésével együtt halad-e az etikai gondolkodás fejlődése? Vajon egyáltalán szükség van-e az etikai gondolkodás fejlődésére, vagy elegendő, ha az emberiség bízik a hihetetlen lehetőségeket biztosító technológiai fejlődésben? Úgy érezhetjük, hogy egyfelől egyre inkább átszövik az életünket a digitalizáció adta vívmányok és kényelmi szolgáltatások, másfelől pedig egyre kevésbé értjük mindezek hátterét, és még kevésbé vagyunk képesek reálisan megítélni például a mesterséges intelligenciában rejlő lehetőségeket és kockázatokat. Ennek a problémának egyfajta leképeződése az, hogy milyen szélső értékek között ingadozik a mesterséges intelligenciával kapcsolatos tudósítások hangvétele és a lehetséges kockázatok megfogalmazása.¹ Egyfelől éppen a kockázatok felmérésének képessége segíthet a kutatáshoz (innovációhoz) való helyes hozzáállás kialakításához, másfelől a digitalizációnak az emberre, valamint a társadalomra gyakorolt hatásának szisztematikus reflexiója segítheti a pontosabb megértést és a megfelelő hozzáállás kialakítását.

¹ Pálffy Dániel Ábel: „Fennáll a lehetőség, hogy kiirtjuk az emberiséget” – hátborzongató beszélgetés a mesterséges intelligenciával. *Mandiner*, 2023. március 25.

Ennek a kiegyensúlyozottnak az egyik alapvető eszköze az etikai gondolkodás művelése. Az etika definíciója szerint „[o]lyan gyakorlati érvelésben használt fogalmak tudománya, mint jó, helyes, kötelesség, kötelezettség, erény, szabadság, racionalitás és döntés”.² Továbbá az etika „háttértudománya azoknak a fogalmaknak, amelyekben alapuló érveket fogalmazhatunk meg ezen előbbi fogalmakra vonatkoztatva, mint objektivitás, szubjektivitás, relativizmus, szkepticizmus”.³ Fontos különbségtétel továbbá az etikai és a morális megközelítés elhatárolása.⁴ Az etika a filozófiai gondolkodás részeként a racionalitáson alapuló módszerrel, kizárólag az emberi értelem képességeit felhasználva, az ész szerinti gondolkodás törvényszerűségei alapján⁵ közelít a vizsgált valóságokhoz, éppen ezért ennek a megközelítésnek az alkalmazása segít elkerülni a hiedelmeken és egyéb meghatározottságokon alapuló narratívák ütközését. Az etikai vizsgálat megelőző feltétele a normatív szabályozás kialakításának,⁶ különösen új jelenségek esetén. Az etikai megközelítés jelentősége tehát nem a normativitásából következik, hanem éppen annak kialakításának az alapja. A jelentősége abban áll, hogy segít meghatározni azokat a kereteket és fogalmakat, célkitűzéseket, amelyekre támaszkodva normatív szabályrendszert ki lehet alakítani. Könnyen belátható a fogalomalkotás szükségessége egy olyan terület kapcsán, ahol alapvető kihívás egy-egy új alapfogalom meghatározása.⁷

Ennek az elvi keretnek a kialakításánál a kiindulópontunk a digitális transzformáció jelensége, amelynek a kulcseleme kétségtávol az *adat*. A legtágabb megközelítési keret pedig az érett „információs társadalom”⁸ fogalmának meghatározása. Jelen írás ebben a keretben igyekszik elhelyezni az adatetika jelentőségét. Az írás 1. a technológiával kapcsolatos helyes bizalmat, valamint 2. az adatetika szerepét a helyes bizalom kialakításában, majd 3. az adatetika általános kereteit tárgyalja.

² Oxford Reference: Ethics; lásd Simon Blackburn: *The Oxford Dictionary of Philosophy*. Oxford, Oxford University Press, 2008 (saját fordítás).

³ Blackburn (2008): i. m.

⁴ Blackburn (2008): i. m.

⁵ Török Csaba: *Bölcsességkeresők*. Budapest, L'Harmattan, 2008. 33.

⁶ Stefan Larsson: On the Governance of Artificial Intelligence through Ethics Guidelines. *Asian Journal of Law and Society*, 7. (2020), 3. 437–451.

⁷ A mesterségesintelligencia-rendszerek fogalmát az EU MI-rendelettervezetének I. melléklete tartalmazza. Európai Bizottság: *Javaslat. Az Európai Parlament és a Tanács rendelete a mesterséges intelligenciára vonatkozó harmonizált szabályok (a mesterséges intelligenciáról szóló jogszabály) megállapításáról és egyes uniós jogalkotási aktusok módosításáról*. COM(2021)206 végleges (2021. április 21.).

⁸ Luciano Floridi: Mature Information Societies – a Matter of Expectations. *Philosophy & Technology*, 29. (2016), 1. 1–4.

A technológiával kapcsolatos helyes bizalom kialakítása

A bizalom⁹ egy rendszer szereplői közötti interakciókat elősegítő tényező, akár emberi szereplőkről, mesterséges aktorokról, vagy a kettő kombinációjáról van szó (hibrid rendszer).¹⁰ A bizalom megléte az adott rendszeren belül meglévő kapcsolatokhoz kötődik, és azokat befolyásolja, mint például üzletkötés, tárgyalás, kommunikáció és megbízás adása.¹¹ Mariarosaria Taddeo szerint a bizalom önmagában nem kapcsolat, hanem a *kapcsolatoknak egy tulajdonsága*, olyan dolog, amely megváltoztatja a kapcsolatok működését.¹² Francis Fukuyama meglátása szerint a bizalom az egyik legfontosabb társadalmi erény, így a társadalmak sikerességének a kulcsát a bizalom magas szintjének kialakításában látja.¹³ Álláspontját a krízisidőszakokban is fenntartva úgy fogalmaz a válságidőszakból való kilábalásról szóló reflexiójában,¹⁴ hogy a bizalom meglétén dől el a társadalmak sorsa.¹⁵ Taddeo kifejti, hogy adott kapcsolat tulajdonságaként a bizalom megváltoztatja a kapcsolat működését azzal, hogy egy adott szereplő számára, aki a bizalom mellett dönt, minimalizálja egy adott cél elérése érdekében történő erőfeszítést és az ezzel kapcsolatos elköteleződést.¹⁶ Ez alapvetően kétféle módon történhet. A bizalommal viseltető félnek nem kell megtennie a célja elérése érdekében nélkülözhetetlen cselekvést, amennyiben alappal bízhat abban, hogy az ehhez szükséges közreműködő fél azt kivitelezni fogja. Másfelől a meglévő bizalom kapcsán dönthet úgy, hogy nem ellenőrzi a közreműködő teljesítményét (megspórolja az ezzel kapcsolatos erőfeszítéseket).¹⁷ Mariarosaria Taddeo a következőképpen definiálja a bizalmat:

„Tételezzünk fel egy adott cél elérése szempontjából elsőrendű funkcionális kapcsolatok halmazát, valamint, hogy a kapcsolatokban két ágens vesz részt úgy, hogy egyiküknek (a megbízónak) el kell érnie az adott célt, míg a másik (a megbízottnak) képes elvégezni bizonyos feladatot a cél elérése érdekében. Ha a megbízó úgy dönt, hogy a megbízott által elvégzett feladaton keresztül éri el célját, és ha a megbízó a megbízottat megbízható (trustworthy)

⁹ Egy olyan hozzáállás, amely alapján jó teljesítményt várunk el egy másik féltől, akár hűség, jóindulat, igazság vagy ígéretetek tekintetében. A bizalom mint egyfajta láthatatlan ragasztó fontossága, amely a társadalmat összefűzi, akkor a leginkább látható, amikor elveszik. Blackburn (2008): i. m.

¹⁰ Mariarosaria Taddeo: *Trusting Digital Technologies Correctly. Minds and Machines*, 27. (2017), 4. 565.

¹¹ Taddeo (2017): i. m. 565.

¹² Taddeo (2017): i. m. 565.

¹³ Francis Fukuyama: *Bizalom. A társadalmi erények és a jólét megteremtése*. Ford. Somogyi Pál László. Budapest, Európa Könyvkiadó, 2007.

¹⁴ Francis Fukuyama: *The Thing That Determines a Country's Resistance to the Coronavirus. The Atlantic*, 2020. március 30.

¹⁵ Leimeiszter Barnabás: *A bizalom meglétén dől el a társadalmak sorsa – Fukuyama a járvány következményeiről. Mandiner*, 2020. április 10.

¹⁶ Taddeo (2017): i. m. 565.

¹⁷ Taddeo (2017): i. m. 565.

ügynöknek tartja, akkor a kapcsolatnak megvan az a tulajdonsága, hogy előnyös a megbízó számára. Az ilyen tulajdonság egy másodrendű tulajdonság, amely befolyásolja az ügynökök közötti elsőrendű kapcsolatokat, és ezt bizalomnak nevezzük.”¹⁸

Egy rendszer működéséhez elengedhetetlen a bizalom facilitáló szerepe. Bizalom nélkül a delegálás sokkal nehezkesebben működne, valamint folytonos ellenőrzést feltételezne,¹⁹ ez pedig egyúttal szükségtelen beavatkozás lenne egy adott rendszer működéséhez elengedhetetlen feladatelosztásba.²⁰ Taddeo felteszi a kérdést, hogy vajon milyen lenne egy olyan társadalom, amelyben nincs bizalom az orvosok, a tanárok, a sofőrök irányába? Ez a gyakorlatban azt követelné meg a társadalom tagjaitól, hogy az idejük és az erőforrásaik jelentős részét arra fordítsák, hogy ellenőrizzék mások feladatának az elvégzését, mindezt a saját feladataik elvégzésének rovására tudnák megtenni.²¹ Fontos kiemelni, hogy nem minden rendszer kíván meg egyenlő mértékű bizalmat a működéséhez. Rövid és hosszú távon a túl kevés bizalom korlátozó hatással lehet az adott rendszer belső dinamikájára, de a túl sok bizalom a rendszer összeomlásához vezethet a megfelelő kontroll és koordináció hiányában.²² A bizalom *helyes szintjének* a beállítása az igazi kérdés a rendszer jellemzőire és a szereplők várakozásaira tekintettel.

A digitalizáció előrehaladtával ez a vizsgált tágabb rendszer az *információs társadalom*. Ebben a rendszerben kulcsfontosságú a bizalom helyes szintjének kialakítása, ami egyfajta érettséget feltételez. Az érett társadalmakban a technológiai fejlődéssel kapcsolatos diszkusszió a kiegyensúlyozottság irányába haladhat. Luciano Floridi definíciója szerint „[a]z érett információs társadalmak olyan társadalmak, amelyekben a digitális lehetőségek a társadalom minden aspektusának elvárt háttérét jelentik, szemben azokkal a társadalmakkal, amelyekben az ilyen lehetőségek újak vagy váratlanok”.²³ A társadalmak információs technológiákkal szembeni érettségét alapvetően a *várakozásaik* alapján lehet meghatározni.²⁴ Az információs társadalmak érettségének elemzési szintjei alapulhatnak a tagjainak reflektálatlan és implicit elvárásaira, a kvantitatív mérési eredményekre, valamint a kvalitatív értékelésből levont következtetésekre.²⁵ A várakozásokkal összefüggésben Floridi az oktatást, a megértést és az innovációt tartja kulcsfontosságúnak.²⁶ A bizalom megfelelő szintjének elérése kényes kérdés, és figyelembe

¹⁸ Taddeo (2017): i. m. 565.

¹⁹ Taddeo (2017): i. m. 566.

²⁰ Taddeo (2017): i. m. 566.

²¹ Taddeo (2017): i. m. 566.

²² Taddeo (2017): i. m. 566.

²³ Corinne Cath et al.: Artificial Intelligence and the ‘Good Society’: The US, EU, and UK Approach. *Science and Engineering Ethics*, 24. (2018), 2. 507.

²⁴ Floridi (2016): i. m. 1.

²⁵ Floridi (2016): i. m. 2.

²⁶ Floridi (2016): i. m. 3.

kell venni ebben a rendszert magát (érett információs társadalmak), a megbízó elvárásait (az emberek által delegált feladatokat), valamint a megbízottak természetét (például digitális technológiák) is.²⁷

Az adatetika szerepe a bizalom és a várakozások kialakításában

Napjainkban globális szinten rendkívül kiterjedt diszkusszió övezi a mesterséges intelligencia alkalmazásának elvi kereteit. Figyelemre méltó a Harvard Egyetem Berkman Klein Center kutatása,²⁸ amely igyekezett szintetizálni globális szinten az MI-re vonatkozó etikai és jogi megközelítések elvi alapjait,²⁹ és azt vizuálisan, „térképszerűen” is megjeleníteni.³⁰ Az Európai Unióban igen élénk vita zajlott a mesterséges intelligenciáról szóló rendelettervezet³¹ elfogadása előtt, amely az új és világviszonylatban egyedülálló normatív szabályozás elvi alapjait igyekezett feltárni. A mesterséges intelligenciával foglalkozó magas szintű szakértői csoport 2019. április 8-án tette közzé a megbízható mesterséges intelligenciára vonatkozó etikai iránymutatást, amely a megbízható mesterséges intelligencia alapját és megvalósíthatóságát vizsgálta,³² majd ezt követően közel két év múlva megjelent az európai uniós szabályozás a mesterséges intelligencia vonatkozásában, amely egy kockázat-alapú megközelítést alkalmaz. A szabályozás tehát a kockázatok kiiktatásával kívánja elősegíteni a bizalmat a mesterségesintelligencia-alapú megoldásokban, amely beleilleszkedik Mariarosaria Taddeo megközelítésébe is a technológiával kapcsolatos helyes bizalom kialakításával összefüggésben. A rendelettervezet által alkalmazott kockázattípusok az 1. elfogadhatatlan kockázattal, 2. nagy kockázattal, illetve 3. alacsony vagy minimális kockázattal járó MI-alkalmazások.³³ Az elfogadhatatlan kockázattal járó megoldásokat tiltja a rendelettervezet, míg a többi kockázati szint esetén eltérő szintű kötelezettséget ró az üzembentartóra a kockázat megfelelő kezelése érdekében. Nyitott kérdés marad ugyanakkor, hogy mit nevez a szabályozás

²⁷ Taddeo (2017): i. m.

²⁸ Jessica Fjeld – Adam Nagy: Principled Artificial Intelligence. Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI. *Berkman Klein Center*, 2020. január 15.

²⁹ Jessica Fjeld et al.: *Principled Artificial Intelligence. Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI*. The Berkman Klein Center for Internet & Society Research Publication Series, 2020.

³⁰ Principled Artificial Intelligence.

³¹ Európai Bizottság: *Javaslat. Az Európai Parlament és a Tanács rendelete a mesterséges intelligenciára vonatkozó harmonizált szabályok (a mesterséges intelligenciáról szóló jogszabály) megállapításáról és egyes uniós jogalkotási aktusok módosításáról*. COM(2021)206 végleges (2021. április 21.).

³² European Commission: *Ethics Guidelines for Trustworthy AI*. 2019. április 8.

³³ Európai Bizottság: *Javaslat. Az Európai Parlament és a Tanács rendelete a mesterséges intelligenciára vonatkozó harmonizált szabályok (a mesterséges intelligenciáról szóló jogszabály) megállapításáról és egyes uniós jogalkotási aktusok módosításáról*. COM(2021)206 végleges (2021. április 21.).

mesterséges intelligenciának, a definíció egy nyitott mellékletre utal, amely praktikus jogtechnikai megoldást jelent. A lista bővítésével viszonylag rugalmasan tud reagálni a szabályozás a technológiai fejlődésre.

Adatvezérelt társadalom

Már közhelyszerű az a megállapítás, hogy az adat az új olaj.³⁴ Európa is kezd ráébredni az adatokban rejlő gazdasági potenciál kiaknázásának szükségességére. Az európai adatstratégia kifejezett célja,³⁵ hogy a gazdasági szereplők számára hozzáférhetővé tegye a kormányzati szektorban keletkező adatokat, illetve hogy kialakítsa a méltányos hozzáférés kereteit a vállalkozások által generált, valamint az általuk kezelt adatokhoz. Az Európában bevett adatvédelmi megközelítés mellett tehát egyre hangsúlyosabban megjelenik az adatokban rejlő gazdasági előnyök kiaknázásának igénye.³⁶ Számos jogi aktust, illetve tervezetet fogadott el az Európai Unió az elmúlt időszakban, amelyek az adatokhoz való hozzáférést igyekeznek elősegíteni, úgy, hogy közben az európai alkotmányos hagyományban a sajátos európai értékekből táplálkozó adatvédelmi szempontok se sérüljenek. Figyelemre méltó lesz látni, hogyan történik majd ennek a dilemmának a feloldása: az európai szabályozó a GDPR alapjogvédelmi megközelítése mellett miként tudja ezt a gazdasági szempontú érdeket megjeleníteni, és az eltérő jogi érdekeket kiegyenlíteni.

A nyílt hozzáférésű és a kormányzati szektorban keletkező adatok újrahasznosítását kívánja elősegíteni az Open Data irányelv,³⁷ amely 2019. július 6-án lépett életbe, és váltotta fel a korábbi közszféra újrahasznosításáról szóló (PIS) irányelvet.³⁸ A PIS irányelv az információk újrafelhasználásának gazdasági vonatkozásaira összpontosít, arra ösztönzi az uniós országokat, hogy a lehető legtöbb információt tegyék elérhetővé újrafelhasználás céljából. Idetartoznak a minisztériumok, állami ügynökségek, önkormányzatok és a többnyire állami hatóságok, például meteorológiai intézetek által finanszírozott vagy azok ellenőrzése alatt álló szervezetek által birtokolt anyagok.³⁹ Az Open Data irányelv bevezeti a *nagy értékű adatkészletek* fogalmát,

³⁴ The World's Most Valuable Resource Is No Longer Oil, But Data. *The Economist*, 2017. május 6.

³⁵ Az európai adatgazdaság kiépítése. *EUR-Lex*.

³⁶ Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet). L 119/1 (2016. május 4.).

³⁷ Az Európai Parlament és a Tanács (EU) 2019/1024 irányelve (2019. június 20.) a nyílt hozzáférésű adatokról és a közszféra információinak további felhasználásáról (átdolgozás). L 172/56 (2019. június 26.).

³⁸ Az Európai Parlament és a Tanács 2003/98/EK irányelve (2003. november 17.) a közszféra információinak további felhasználásáról. L 345/90 (2003. december 31.).

³⁹ European Commission: *European Legislation on Open Data*.

amelyeknek újrafelhasználása jelentős előnyökkel jár a társadalom és a gazdaság számára. Ezekre külön szabályok vonatkoznak, amelyek biztosítják, hogy ingyenesen, géppel olvasható formátumban elérhetőek legyenek, és a hozzáférést alkalmazás-programozási felületeken (API) keresztül biztosítják. A nagy értékű adatkészletek tematikus hatályát az irányelv melléklete tartalmazza.⁴⁰ Az adatkormányzási rendelet⁴¹ tervezetét 2020. november 25-én fogadták el.⁴² A rendelet célja, hogy több adatot tegyen elérhetővé, és megkönnyítse az adatmegosztást az ágazatok és az uniós országok között annak érdekében, hogy az adatokban rejlő lehetőségeket az európai polgárok és vállalkozások jobban kiaknázhassák.⁴³ Az adatmegosztási rendeletet⁴⁴ 2022. február 23-án fogadták el, amely méltányos hozzáférést kíván biztosítani a dolgok internete által generált adatok felhasználása tekintetében is, és helyzetbe hozza a kis- és középvállalkozásokat, hogy az adatok adta gazdasági potenciálból ők is részesedhessenek üzleti tervezésük, innovatív megoldások révén.

Az adatetikai diskurzus szükségessége

Egy adatvezérelt társadalomban egyre inkább előtérbe kerülnek az adatok felhasználásának etikai kérdései. Az adatok meghatározó bemeneti forrást jelentenek a vállalatok számára, de a közigazgatásban és akár a szakpolitika kialakításában is adatelemzéssel racionalizálhatók a folyamatok. Egyes technológiai vállalatok üzleti modelljének lényege a személyes adatok felhasználásával nyújtott kényelmi szolgáltatások. A mesterségesintelligencia-alapú megoldások hatékonysága is nagyban a tanító adatok minőségén múlik. Nem véletlen tehát az adatokhoz való hozzáállás megváltozása Európában,⁴⁵ illetve jelzésértékű, hogy az Egyesült Államokban 2016-tól kezdve folyamatosan a három legkeresettebb állás között van az adatelemző (data scientist).⁴⁶ Adatvédelmi szempontból a személyes adatoknak⁴⁷ van jelentősége,

⁴⁰ A 13. cikk (1) bekezdésében említett nagy értékű adatkészletek tematikus kategóriáinak jegyzéke: 1. térinformatikai adatok, 2. földmegfigyelési és környezeti adatok, 3. meteorológiai adatok, 4. statisztikák, 5. vállalati és vállalattulajdonosi adatok, 6. mobilitási adatok.

⁴¹ Európai Bizottság: *Javaslat. Az Európai Parlament és a Tanács rendelete az európai adatkormányzásról (Adatkormányzási rendelet)*. COM(2020)767 végleges (2020. november 25.).

⁴² A rendelet a kihirdetést követő 20. napon lépett hatályba, és a hatálybalépést követően 12 hónappal kell alkalmazni.

⁴³ European Commission: *European Data Governance Act*.

⁴⁴ Európai Bizottság: *Javaslat. Az Európai Parlament és a Tanács rendelete a méltányos adathozzáférésre és adatfelhasználásra vonatkozó harmonizált szabályokról (adatmegosztási jogszabály)*. COM(2022)68 végleges (2022. február 23.).

⁴⁵ Európai Bizottság: Európai adatstratégia.

⁴⁶ Best Jobs in America 2021. *Glassdoor*.

⁴⁷ GDPR 4. cikk 1. pont alapján „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

és a védett alapjog a magánszféra (védelme). Az adatok elkülöníthetők személyes és nem személyes adatokra, a magánszféra védelme értelemszerűen az előző csoportra terjed ki. Ennek az érdeknek a védelme kapcsán az adatok anonimizálását⁴⁸ javasolják első körben. Technikai értelemben ugyanakkor vitatott, hogy az anonimizálás mennyire hatékony eszköz, mivel a nagy adathalmazok esetében könnyen elképzelhető érzékeny információk kinyerése, ilyen tartalmú adatok visszaállítása.⁴⁹ Csupán a mobiltelefonokból származó anonimizált adatok esetén 70%-os pontossággal meg lehet jósolni a személy korát egyéves differenciával, a nemét 70–80%-os pontossággal, de egy indonéz szolgáltató jelzése alapján a vallást is meg tudják állapítani abból, hogy valaki hogyan használja a telefonját.⁵⁰ A brit Információs Biztos Hivatala arra hívja fel a figyelmet, hogy a nagy adathalmazok korában az anonimizáció egyre kevésbé hatékony.⁵¹ A technika sikeressége alapvetően vitatott. Ann Cavoukian és Daniel Castro arra a következtetésre jutnak, hogy a deidentifikáció lehetséges.⁵² Egy brit információbiztosi jelentés által idézett MIT-tanulmány szerint, amely 1,1 millió ember háromhavi bankkártyahasználatának adatait vizsgálta, négy tranzakció időpontjából és helyszínéből az adathalmazban szereplő személyek 90%-át azonosítani lehet.⁵³ Az eredmény hitelessége ez esetben is vitatott, mindenesetre nagyon nehéz lenne kizárni az utólagos azonosítás lehetőségét a nagy adathalmazok korában, különösen ha más forrásból elérhető adatok is rendelkezésre állnak.⁵⁴ Az adatgazdaság piaci viszonyai között az adatok beszerzése jellemzően adatbrókerektől történik.⁵⁵ Az Európai Bizottság éppen azon az alapon mulasztotta el több ízben a vállalkozások összefonódásakor felhalmozódó adatok értékelését a piaci erő (kizáró magatartás lehetőségének) megállapításánál kellő súllyal beszámítani, hogy az adatok más forrásból is beszerezhetők.⁵⁶

A mesterségesintelligencia-alapú megoldások szintén a nagy adathalmazokból indulnak ki, és jellemzőjük a rendkívül kiterjedt adatfelhasználás. Az öntanuló algoritmusok a tanító adatok felhasználásával képesek az adott műveletet ellátni. Mindez egyre több olyan alapvető területen fejti ki a hatását, mint az emberi

adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható.

⁴⁸ Information Commissioner's Office: *Big Data, Artificial Intelligence, Machine Learning and Data Protection*. 2017. 130. pont.

⁴⁹ Information Commissioner's Office (2017): i. m. 133. pont.

⁵⁰ Linnet Taylor: The Ethics of Big Data as a Public Good: Which Public? Whose Good? *Philosophical Transactions: Mathematical Physical and Engineering Sciences*, 374. (2016), 2083. 4.

⁵¹ Information Commissioner's Office (2017): i. m. 133. pont.

⁵² Ann Cavoukian – Daniel Castro: *Big Data and Innovation, Setting the Record Straight: De-Identification Does Work*. 2014.

⁵³ Information Commissioner's Office (2017): i. m. 133. pont.

⁵⁴ Information Commissioner's Office (2017): i. m. 133. pont.

⁵⁵ Stacy-Ann Elvy: Paying for Privacy and the Personal Data Economy. *Columbia Law Review*, 117. (2017), 6. 1397.

⁵⁶ Case No COMP/M.4731 – Google/ DoubleClick. 365. pont.

kommunikáció, vállalati és közigazgatási hatékonyság, digitális gazdaság, illetve komplex döntések előkészítése. Ezeknek közös bemeneti feltétele: az adat, amelyre épül az algoritmikus döntéshozatal, valamint az MI-megoldások.

A Facebook (Meta) „érzelmi fertőzés kísérlete” iskolapéldája annak, hogy az adatokkal végzett kutatások milyen etikai kérdéseket vethetnek fel.⁵⁷ 2014-ben publikáltak egy kísérletet, amely azt szemléltette, hogy az érzelmi állapotok valóban terjednek az online környezetben is.⁵⁸ A kísérletet a Facebook adatelemző csapata (Core Data Team) és két akadémiai kutató végezte. A kísérlet lényege az volt, hogy manipulálták a hírfolyamban megjelenő, az ismerősök által posztolt üzeneteket, és a két meghatározott csoport esetében csökkentették a számukra megjelenő pozitív, illetve a negatív töltetű tartalmakat. A kutatás tárgya az volt, hogy mindez vajon miként befolyásolja a felhasználókat saját érzelmi állapotuk kifejezésében. A kísérletbe a cég 689 003 felhasználót vont be. A kutatók szignifikáns összefüggést találtak aközött, hogy milyen érzelmi tartalmú posztoknak vannak kitéve a felhasználók, és hogy ők maguk milyen érzelmi töltetű posztokat generálnak. Mintegy hárommillió poszt és 122 millió szó elemzése azt mutatta, hogy azok, akiknek a hírfolyamában a pozitív töltetű tartalmakat csökkentették, maguk is több negatív tartalmú állapotkifejezést (status update) osztanak meg, és kevesebb pozitív tartalmat. Ezzel fordítottnak, akiknél a negatív állapotjelentéseket csökkentették, azok több pozitív jelzést adtak az állapotukról, és kevesebb negatív állapotfrissítést. Továbbá, minél kevesebb érzelmi töltetű tartalomnak voltak kitéve a felhasználók, maguk is annál kevesebb szót használtak az állapotfrissítéseikben (status update).⁵⁹ A kutatás megállapította, hogy az érzelmi állapotok átadhatók „érzelmi fertőzés” által az egyik emberről a másikra, anélkül, hogy a személy ennek tudatában lenne.⁶⁰ Az érzelmi fertőzés tényét korábban már bizonyították, de hogy ez történhet emberek közötti közvetlen interakción kívül is, valamint hogy akár az online közösségi média felületén keresztül is, az újdonság volt.⁶¹

A Facebook-kísérlet ugyanakkor súlyos etikai aggályokat vetett fel, nem csupán a manipulációval végzett kísérlet miatt, de a beleegyezés hiánya miatt is.⁶² A kísérletet az általános szerződési feltételekre való hivatkozással végezték, amelyben szerepelt a „kutatás” kitétel is, ugyanakkor mint kiderült, a kutatásba való beleegyezés

⁵⁷ Jukka Jouhki et al.: Facebook’s Emotional Contagion Experiment as a Challenge to Research Ethics. *Media and Communication*, 4. (2016), 4.

⁵⁸ Adam D. I. Kramer – Jamie E. Guillory – Jeffrey T. Hancock: Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks. *Proceedings of the National Academy of Sciences*, 111. (2014), 24. 8788–8790.

⁵⁹ Jukka Jouhki et al.: Facebook’s Emotional Contagion Experiment as a Challenge to Research Ethics. *Media and Communication*, 4. (2016), 4. 1.

⁶⁰ Jouhki et al. (2016): i. m. 1.

⁶¹ Jouhki et al. (2016): i. m. 2.

⁶² Jouhki et al. (2016): i. m.

fordulata csak négy hónappal a kísérlet megkezdése után került bele a feltételekbe.⁶³ Egyesek felvetik az embereken végzett kísérlet problematikáját is.⁶⁴ A szakmai közvéleményben a kísérlet kapcsán éles vita bontakozott ki az adattudomány kutatás-etikai kérdéseit illetően. A felvetett problémák mellett alapvető jelentőségű adottság, hogy az adat kiemelkedő gazdasági jelentősége következtében magánvállalatok óriási mennyiségben birtokolnak személyes adatokat.

Az emberi természet kitettségének mértéke az online térben talán még nem teljesen egyértelmű a szakmai közönség számára. Meg kell vizsgálni az olyan híreket is, amelyek a gép-ember interakciójában az emberi szereplő különös sérülékenysége mutatnak rá. Egy friss belga lapértésülés szerint egy krízisben lévő férfi öngyilkosságot követett el egy chatbottal folytatott, számára bizalmas és rendszeressé vált beszélgetés következtében.⁶⁵ A GPT-J nyelvi modellen alapuló Eliza nevű chatbot a beszélgetés egy pontján az öngyilkosság gondolatában megerősítette a férfit, aki később azt el is követte.⁶⁶ A férfi pszichiátere megerősítette a gép közrehatását a férfi döntésében.⁶⁷

Az adatetika kihívása

Kutatásetikai szempontból alapvető kihívást jelent, hogy a nagy adathalmazok elsősorban a magánszereplőknél halmozódnak fel, így az akadémiai szempontok csak lassan és áttételesen tudnak érvényesülni az etikai kérdések kialakításánál. Éljenjáró adattudományi kutatásokat nem véletlenül a nagy technológiai vállalkozások képesek kivitelezni. Ebben a környezetben egyes nagy technológiai cégek komoly erőfeszítéseket tesznek, hogy befolyásolják az adatetika értelmezési kereteit és fejlődési irányait. A Facebook például a Müncheni Műszaki Egyetemen finanszírozza a Mesterséges Intelligencia Etikai Kutatóintézetet,⁶⁸ de a technológiai vállalkozások – érdekelt szereplőként – aktívan részt vesznek a normatív szabályozás kialakításában is. Thomas Metzinger, az Európai Bizottság mesterséges intelligenciával foglalkozó magas szintű szakértői csoportjának filozófus tagja nem optimista a vállalkozások motivációját illetően a szabályozás etikai alapjainak kialakításában. Az Európai Unió mesterséges intelligencia szabályozására vonatkozó tervezetének előzménye a szakértői csoport 2019. április 8-án kiadott, már korábban tárgyalta,

⁶³ Alex Hern: Facebook T&Cs Introduced ‘Research’ Policy Months After Emotion Study. *The Guardian*, 2014. július 1.

⁶⁴ Jouhki et al. (2016): i. m. 4.

⁶⁵ Lauren Walker: Belgian Man Dies by Suicide Following Exchanges with Chatbot. *The Brussels Times*, 2023. március 28.

⁶⁶ Zách Dániel: Egy csetbot bátorítása után lett öngyilkos egy belga férfi. *Telex*, 2023. április 3.

⁶⁷ Kéfer Ádám: Öngyilkos lett egy fiatal családapa, miután hetekig beszélgetett a mesterséges intelligenciával. *Index*, 2023. március 30.

⁶⁸ Institute for Ethics in Artificial Intelligence.

etikai irányelveket tartalmazó dokumentuma. Metzinger szerint a testület iparági szereplői azzal a motivációval vettek részt munkájában, hogy elhúzzák az etikai diskurzust, és ezzel is minél inkább késleltessék a hatékony európai normatív szabályozás megszületését.⁶⁹ Metzinger kiemelte, hogy a szakértői csoportnak mindössze négy olyan tagja volt, akik az etika területén formális akadémiai képzésben vettek részt. Állítása szerint ők mindent elkövettek, hogy a politikaalkotás és szabályozás alapjául szolgáló etikai elvek mielőbb megszülethessenek.

További kihívást jelent az érvényes etikai keretek kialakításában az „etikai mosdatás” (ethics washing) jelensége. Ez azt jelenti, hogy számos piaci szereplő a technológiai szektorban azért hoz nyilvánosságra etikai irányelveket, hogy „elmossák” a tevékenységükkel kapcsolatos aggodalmakat.⁷⁰ Az etika ilyen hozzáállással való művelésétől nem idegen az egyes elvek közötti olyan stratégiai válogatás (shopping), amely a legkevésbé korlátozza az adott szereplő fellépését, mégis azt képes kommunikálni, hogy hozzájárul a közjó kialakításához.⁷¹ Gijs van Maanen szerint a pesszimista válasz erre a problémára, hogy alternatív eszközökkel és módszerekkel kényszerítsék ki a technológiai szektor részéről az etikai határok betartását, mint például az adatigazságosság⁷² vagy a biztonságos terepnek számító emberi jogi megközelítés. Míg az optimista megközelítésben az etikai keretek pontosabb kifejtése és meghatározása segíthet a domináns szereplők visszaéléseinek elkerülésében.⁷³

Az adatetika általános keretei

Az üzleti adatetika megközelítése

Linnet Taylor és Lina Dencik kritikai mélyelemzésükben⁷⁴ arra jutnak, hogy a piaci szereplők motivációit az etikai diskurzusban való részvételük kapcsán alapvetően a fogyasztói bizalom helyreállítása határozza meg. Más megközelítésben a vállalkozások részéről az adatetika tematizálására vonatkozó igyekezet a vállalkozások társadalmi felelősségvállalásának újfajta kommunikálására is felhasználható, amely egyenesen versenyelőnyt eredményez.⁷⁵

Általában véve a piaci szereplők perspektívája az adatetikai kérdésekkel összefüggésben defenzívnek mondható. Sok esetben a gazdasági szereplők egyre inkább azzal

⁶⁹ European Parliament Webplayer Dedicated to Live Events.

⁷⁰ Gijs van Maanen: AI Ethics, Ethics Washing, and the Need to Politicize Data Ethics. *Digital Society*, 1. (2022), 2. 8.

⁷¹ Maanen (2022): i. m.

⁷² Linnet Taylor: Global data justice. *Communications of the ACM*, 62. (2019), 6. 22–24.

⁷³ Taylor (2019): i. m.

⁷⁴ Linnet Taylor – Lina Dencik: Constructing Commercial Data Ethics. *Technology and Regulation*, 2. (2020), 1–10.

⁷⁵ Data Ethics – The New Competitive Advantage.

az igénnyel lépnek fel, hogy az adatok felhasználására vonatkozó etikai gondolkodást befolyásolják, amely hozzáállást jellemzően a technológiai determinista álláspont határoz meg, miszerint az innováció definíciószerűen jó, így a hangsúly az adatok gazdasági értékének kiaknázásán van.⁷⁶ Ezzel együtt nem ritkák az adatszivárgással vagy adatkezeléssel kapcsolatos, felháborodást kiváltó hírek.⁷⁷ Ezek egyes esetekben kikezdi a vállalati szektor hitelességét, de számos kezdeményezés irányul vállalati adatprojektek esetében az etikai szempontok tervezési fázisban történő megjelenítésére (ethical by design).⁷⁸

Vállalati szempontból Taylor és Dencik elhatárolja egymástól a mikro- és makroszinten jelentkező etikai kérdéseket. A mikroszinten az egyes személyekkel kapcsolatban merül fel, hogy hogyan közelítsenek az adatokhoz munkájuk és eljárásaik során.⁷⁹ Ez fogja meghatározni a vállalkozások esetében a belső szabályokat és etikai irányelveket az adathalmazokkal való eljárásokra vonatkozóan, és e megközelítést jellemzően az általános kutatásetikai kérdések alakítják ki. Mindez nem a szervezeti szintű hozzáállásra mutat rá, hanem az egyes adattudós kötelességét hangsúlyozza, a megfelelőséggel összefüggésben.⁸⁰ Ez ugyanakkor paradox helyzeteket is eredményezhet bizonyos esetekben, amikor az egyes munkavállaló megfelel szűk értelemben vett kötelezettségének, de tágabb összefüggésben a vállalat adatkezelési gyakorlata etikai kérdéseket vet fel.⁸¹ A makroetikai szint ezzel szemben a privát vállalati szektor policy szintje, amely arra kérdezi rá, hogy a technológia szabályozása miként valósuljon meg, illetve az adatokkal kapcsolatos politikai nézőpontot tárgyalja.⁸²

Alkalmazott adatetikai kérdések

Számos területen jelentkezik az adatetika hozzájárulása az etikai szempontból is értelmezhető dilemmák eldöntésénél. Annika Richterich kísérletet tesz ezeknek az összegyűjtésére, amit alapul véve bemutatok néhány problémakört a nagy adathalmazok vonatkozásában, csupán a problémafelvetés igényével.

- A biztonság garantálása és a magánszféra védelme. A személyes adatok védelme a magánszférához fűződő jog biztosításának alapja, ugyanakkor a rendfenntartó szervezetek alapvető információigénye van a biztonsági

⁷⁶ Taylor–Dencik (2020): i. m. 1.

⁷⁷ Facebook–Cambridge Analytica botrány: Zuckerberg válaszoljon az európaiaknak. *Európai Parlament*, 2018. április 19.

⁷⁸ Tom Jongen: How to Make Your Data Project Ethical by Design. *Towards Data Science*, 2021. június 11.

⁷⁹ Taylor–Dencik (2020): i. m. 3.

⁸⁰ Taylor–Dencik (2020): i. m. 3.

⁸¹ Taylor–Dencik (2020): i. m. 3.

⁸² Taylor–Dencik (2020): i. m. 4.

kockázatok kiszűrésére.⁸³ A téma széles körű szakirodalmi feldolgozása kiterjed a szolgáltatások elszámlálhatóságára is a modern technológiák és adatok felhasználására vonatkozóan.⁸⁴ Richterich szerint ugyanakkor a biztonság és magánszféra szembeállítása téves dichotómia.⁸⁵

- Nyílt adat (open data) kezdeményezés.⁸⁶ A biztonság és magánszféra védelme közötti ellentét, a kormányzati megfigyelések, valamint a vállalkozások hasonló gyakorlatai kiváltották azokat az igényeket, amelyek normatív módon igazolják a nagy adathalmazok működési kereteit. Az átláthatóság előmozdítása megköveteli az információk nagyarányú feltárását, ami magában hordozza az eljárások és technikai megoldások nyilvánosságát, akár akadémiai, kormányzati, céges, vagy éppen egyéni eljárásokról van szó. A nyílt adathasználat fogalma gyakran kapcsolódik az elszámlálhatóság gondolatához is. A nyílt adat fogalmával az átláthatóság a nagy adathalmazokra vetítve is megjelent: a nyílt adat az, ami szabadon használható, újra hasznosítható és újra osztható bárki által. A nyílt adat kezdeményezésnek nagy támogatottsága van Európában.
- Adatfilantrópia.⁸⁷ A vállalati szektorban nagyon ritka a nagy adathalmazok – üzleti szempontokon túl történő – megosztása. Az adatfilantrópia a nagy adathalmazok megosztására irányuló kezdeményezés. Ezt nem csupán a gazdasági értéke miatt, hanem mint a közjóhoz való hozzájárulást keretezik. Az egyik zászlóshajó-kezdeményezés az ENSZ Global Pulse kezdeményezése, amely keretében a nagy adathalmazokat fenntartható fejlesztésekre és humanitárius akciókra fordítva osztják meg.
- Tájékoztatáson alapuló beleegyezés.⁸⁸ Az emberekre vonatkozó kísérletek esetén alapvetés a tájékoztatáson alapuló beleegyezés, ugyanakkor hasonló követelmény irányadó az adatkezeléssel összefüggésben is. A felhasználók beleegyezésének jogi értelemben is ki kell terjednie a vállalkozások szolgáltatása során nyújtott adatkezelésre. Jogi eljárások szintjén is komoly vita folyik a beleegyezés érvényességéről, különösen erőfölényes vállalatok esetében.

⁸³ GDPR 2. cikk (2) bekezdés d) pont alapján „[e] rendelet nem alkalmazandó a személyes adatok kezelésére, ha azt: az illetékes hatóságok bűncselekmények megelőzése, nyomozása, felderítése, vád-eljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzik, ideértve a közbiztonságot fenyegető veszélyekkel szembeni védelmet és e veszélyek megelőzését”.

⁸⁴ Pál Vadász – Zsolt Zódi: The Accountability of Intelligence and Law Enforcement Agencies in Information Search Activities. In Noella Edelmann et al. (szerk.): *Electronic Participation. ePart 2021*. Cham, Springer, 2021. 210–220.

⁸⁵ Annika Richterich: Big Data: Ethical Debates. In Annika Richterich: *The Big Data Agenda. Data Ethics and Critical Data Studies*. London, University of Westminster Press, 2018. 35.

⁸⁶ Richterich (2018): i. m. 37–40.

⁸⁷ Richterich (2018): i. m. 40–42.

⁸⁸ Richterich (2018): i. m. 42–45.

A kérdés átvezet a felhasználók döntési autonómiájához a digitális szolgáltatásokkal összefüggésben.

- Algoritmikus elfogultság.⁸⁹ A nagy adathalmazokban található elfogultsággal összefüggésben merül fel az algoritmikus elfogultság vizsgálata. Sok esetben az adathalmazok impliciten tartalmazzák azokat a mintázatokat, amelyek a társadalomban megvannak. Ugyanakkor a jellemző megoldás, miszerint egy felhasználó vagy elfogadja a felkínált feltételeket, vagy nem használja az adott szolgáltatást, azzal a következménnyel is járhat, hogy az adatvédelmileg tudatosabb személyek adatai kikerülnek a nagy mintázatokból, ezt is nevezzük tudatossági paradoxnak (awareness paradox).

Akadémiai adatetikai szempontok

Az adatetika (data ethics) elvi kereteit Luciano Floridi és Mariarosaria Taddeo dolgozták ki 2016-ban, amelyet az etika új ágaként határoztak meg.⁹⁰ Az adatetika azzal az ambícióval lép fel, hogy az adatokhoz kapcsolódó etikai kérdéseket vizsgálja és értékelje (az adatgenerálást, -rögzítést, -kezelést, -felhasználást, -terjesztést, -megosztást), ideértve az algoritmusokat (mesterséges intelligencia, mesterséges ágensek, gépi tanulás és robotika) és az ezekre vonatkozó eljárásokat (felelősségteljes innováció, programozás, hekkelés és kódolás) annak érdekében, hogy kialakítsa és támogassa a morálisan jó megoldásokat (helyes eljárásokat és értékeket).⁹¹ Az adatetika épít a számítástechnika és információs etika által nyújtott alapokra, ugyanakkor a kutatásának hangsúlyait az etikai kérdések tételezése során az információ-központúságból az adatközpontúság irányába pozicionálja.⁹²

Floridi és Taddeo kifejti, hogy az adattudomány hatalmas lehetőségeket hordoz magában a magán- és társadalmi élet, valamint a környezet fejlesztésében,⁹³ ugyanakkor ezek a lehetőségek egyúttal súlyos etikai kihívásokkal párosulnak. Megjegyzik, hogy az egyre növekvő mennyiségű adat kiterjedt felhasználása – amelyek gyakran személyes, ha nem érzékeny nagy adathalmazok (big data) –, illetve az egyre gyakoribb algoritmusokra történő hagyatkozás az adatok elemzésében, annak érdekében, hogy azok választásokat jelöljenek ki és döntéseket hozzanak,⁹⁴ továbbá számos automatizált eljárás esetében az emberi beavatkozás fokozatos

⁸⁹ Richterich (2018): i. m. 45–49.

⁹⁰ Luciano Floridi – Mariarosaria Taddeo: What Is Data Ethics? *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 374. (2016), 2083.

⁹¹ Floridi–Taddeo (2016): i. m.

⁹² Floridi–Taddeo (2016): i. m.

⁹³ Példaként említik az okosvárosok fejlesztését, vagy a szén-dioxid-kibocsátás által okozott problémák kezelését.

⁹⁴ Ideértve a gépi tanulást, mesterséges intelligenciát és robotikát.

csökkenése, sőt az emberi felügyelet elhagyása felvetik a méltányosság, felelősség, emberi jogok tiszteletének sürgető kérdéseit.⁹⁵ Álláspontjuk szerint ezeket az etikai kihívásokat eredményesen lehet kezelni az adattudományok részéről, és az adatetika nagy kihívása éppen az, hogy a társadalmi elutasítás és jogi tiltás között található szűk ösvényre navigáljon, hogy ezen adattudományi megoldások etikai értéktartalmát maximalizálhassák a társadalmi előnyök érdekében.⁹⁶ Az adattudomány az információs forradalom legutóbbi fázisa. Az adattudomány által állított etikai kihívások – építve az információs etika megelőző 30 éves eredményeire – elvi síkon egy háromaspektusú kutatással orvosolhatók, ahol a kutatás irányainak a felrajzolásában a három tengely az adatetika (ethics of data), az algoritmusok etikája (ethics of algorithm) és az eljárások etikája (ethics of practices).⁹⁷

Az *adatetika* a nagy adathalmazok gyűjtésével és elemzésével összefüggésben jelentkező etikai kérdésekkel foglalkozik, úgymint a big data alkalmazása biomedicina-kutatásokban és a társadalomtudományokban, valamint a profilalkotás, online hirdetés, adatfilantrópia és a nyílt adatok etikai vonatkozásai. Itt kulcskérdés a magánszemélyek újraazonosíthatósága az adatbányászat segítségével, a nagy adathalmazok szivárgása, egyesítése és újrahasznosítása, valamint a csoportos magánszféra (group privacy) sérelmének lehetősége. A bizalom és átláthatóság úgyszintén fontos szerepet játszanak ebben, felismerve az adattudományokkal kapcsolatos általános ismeretek és tudatosság hiányát a társadalom jelentős részéről.⁹⁸

Az *algoritmusok etikája* széles értelemben az algoritmusok autonómiájának egyre növekvő komplexitásával foglalkozik (beleértve a mesterséges intelligenciát, mesterséges ügynököket és az internetbotokat), különös tekintettel a gépi tanuláson alapuló applikációkra. Ezen a területen a kihívást a morális felelősség és a tervezők, valamint az adattudósok elszámoltathatósága jelenti az előre nem látható és nem kívánt következmények, vagy akár az elmulasztott lehetőségek miatt.⁹⁹

Az *eljárások etikája* (beleértve a szakmai etikát és a köteleességetikát) a személyek és szervezetek adatkezelésre vonatkozó eljárásainak és politikáinak kialakításával kapcsolatos felelősség kérdését veti fel, beleértve az adattudósokét, azzal a céllal, hogy meghatározzák a felelősségteljes innováció, a fejlesztések és felhasználás etikai kereteit és szakmai kódexeit, amelyek így egyszerre biztosíthatják az adattudomány fejlődésének kereteit, valamint az egyének és csoportok jogait.¹⁰⁰

⁹⁵ Floridi–Taddeo (2016): i. m. 2.

⁹⁶ Floridi–Taddeo (2016): i. m. 2.

⁹⁷ Floridi–Taddeo (2016): i. m. 3.

⁹⁸ Floridi–Taddeo (2016): i. m. 3.

⁹⁹ Floridi–Taddeo (2016): i. m. 3.

¹⁰⁰ Floridi–Taddeo (2016): i. m. 3.

Befejezés

Az adat szerepe egyre inkább felértékelődik annak gazdasági, társadalmi jelentősége és üzleti felhasználásának elterjedt volta miatt. A technológiai fejlődés nagyban támaszkodik az adatok felhasználására, különösen a mesterségesintelligencia-alapú megoldások esetében. Az érett információs társadalmakban a technológiával kapcsolatos várakozások kiegyensúlyozottságot mutatnak, és helyes módon építkező bizalmon alapulnak. A helyes bizalom a kockázatok megfelelő ismeretén és az azokat csökkenteni képes szabályozás kialakításán alapul. Az új technológiai megoldásokkal összefüggésben szükségesnek látszik a szabályozás, amelynek elvi alapjait az etikai elvek tisztázása képes kijelölni.

Az adatetika a nagy adathalmazok széles körű automatizált felhasználásának következtében kibontakozó etikai irányzat. Az adatok felhasználásának keretei jogi eszközökkel széleskörűen szabályozottak, de számos, még nyitott etikai szempontú kérdés marad. A jogi szabályozás elsősorban a személyes adatok védelmére, a magánszféra biztosítására helyezi a hangsúlyt az általános adatvédelmi rendelet keretei között. Ugyanakkor további masszív jogalkotás van kibontakozóban Európában a nagy adathalmazok gazdasági felhasználásának elősegítése érdekében. Adatvédelmi szempontból kézenfekvő megoldásnak látszik a nagy adathalmazok anonimizálása, ugyanakkor – a jelen technológiai keretek között – vitatott, hogy lehet-e végérvényesen anonimizálni személyes adatokat. Ismert továbbá, hogy egyes nagy technológiai vállalatok üzleti modellje az adatvagyon maximalizálásának igényén alapul, ami egyrészt további etikai kérdéseket vet fel, másfelől kihívás elé állítja a hagyományos jogági kereteket is.¹⁰¹ A társadalmaink biztonsági igényeinek fenntartására szolgáló adatkezelés de facto kívül esik az adatvédelmi kereteken, és így szükségszerűen az említett kérdésekkel együtt etikai vizsgálat tárgya. Mindez a jelen társadalmunkban az adatetika művelésének szükségességét jelzi. Jelen írás az adatetikai megközelítés alapvető kereteit tárgyalja, amely hozzájárulhat az érett információs társadalmak¹⁰² eléréséhez és a digitális jóllét (digital well being) elősegítéséhez.¹⁰³

Felhasznált irodalom

Az európai adatgazdaság kiépítése. *EUR-Lex*. Online: https://eur-lex.europa.eu/content/news/building_EU_data_economy.html?locale=hu

¹⁰¹ C-252/21. sz. ügy: Az Oberlandesgericht Düsseldorf (Németország) által 2021. április 22-én benyújtott előzetes döntéshozatal iránti kérelem – Facebook Inc. és társai kontra Bundeskartellamt (A Bíróság 2021).

¹⁰² Floridi (2016): i. m.

¹⁰³ Christopher Burr – Mariarosaria Taddeo – Luciano Floridi: The Ethics of Digital Well-Being: A Thematic Review. *Science and Engineering Ethics*, 26. (2020), 4. 2313–2343.

- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet). L 119/1 (2016. május 4.)
- Az Európai Parlament és a Tanács (EU) 2019/1024 irányelve (2019. június 20.) a nyílt hozzáférésű adatokról és a közsféra információinak további felhasználásáról (átdolgozás). L 172/56 (2019. június 26.)
- Az Európai Parlament és a Tanács 2003/98/EK irányelve (2003. november 17.) a közsféra információinak további felhasználásáról. L 345/90 (2003. december 31.)
- Best Jobs in America 2021. *Glassdoor*. Online: www.glassdoor.com/List/Best-Jobs-in-America-2021-LST_KQ0,25.htm
- Blackburn, Simon: *The Oxford Dictionary of Philosophy*. Oxford, Oxford University Press, 2008. Online: www.oxfordreference.com/display/10.1093/acref/9780199541430.001.0001/acref-9780199541430
- Burr, Christopher – Mariarosaria Taddeo – Luciano Floridi: The Ethics of Digital Well-Being: A Thematic Review. *Science and Engineering Ethics*, 26. (2020), 4. 2313–2343.
- Cath, Corinne – Sandra Wachter – Brent Mittelstadt – Mariarosaria Taddeo – Luciano Floridi: Artificial Intelligence and the ‘Good Society’: The US, EU, and UK Approach. *Science and Engineering Ethics*, 24. (2018), 2. 505–528.
- Cavoukian, Ann – Daniel Castro: *Big Data and Innovation, Setting the Record Straight: De-Identification Does Work*. 2014. Online: www2.itif.org/2014-big-data-deidentification.pdf
- Elvy, Stacy-Ann: Paying for Privacy and the Personal Data Economy. *Columbia Law Review*, 117. (2017), 6. Online: <https://columbialawreview.org/content/paying-for-privacy-and-the-personal-data-economy/>
- Európai Bizottság: *Európai adatstratégia*. Online: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_hu
- Európai Bizottság: *Javaslat. Az Európai Parlament és a Tanács rendelete a mesterséges intelligenciára vonatkozó harmonizált szabályok (a mesterséges intelligenciáról szóló jogszabály) megállapításáról és egyes uniós jogalkotási aktusok módosításáról*. COM(2021)206 végleges (2021. április 21.)
- Európai Bizottság: *Javaslat. Az Európai Parlament és a Tanács rendelete az európai adatkormányzásról (Adatkormányzási rendelet)*. COM(2020)767 végleges (2020. november 25.)
- Európai Bizottság: *Javaslat. Az Európai Parlament és a Tanács rendelete a méltányos adathozzáférésre és adatfelhasználásra vonatkozó harmonizált szabályokról (adatmegosztási jogszabály)*. COM(2022)68 végleges (2022. február 23.)
- European Commission: *Ethics Guidelines for Trustworthy AI*. 2019. április 8. Online: <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>
- European Commission: *European Data Governance Act*. Online: <https://digital-strategy.ec.europa.eu/en/policies/data-governance-act>
- European Commission: *European Legislation on Open Data*. Online: <https://digital-strategy.ec.europa.eu/en/policies/legislation-open-data>
- Facebook-Cambridge Analytica botrány: Zuckerberg válaszoljon az európaiaknak. *Európai Parlament*, 2018. április 19. Online: www.europarl.europa.eu/news/hu/headlines/society/20180418STO02004/facebook-cambridge-analytica-botran-y-zuckerberg-valaszoljon-az-europaiaknak
- Fjeld, Jessica – Adam Nagy: Principled Artificial Intelligence. Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI. *Berkman Klein Center*, 2020. január 15. Online: <https://cyber.harvard.edu/publication/2020/principled-ai>

- Fjeld, Jessica – Nele Achten – Hannah Hilligoss – Adam Nagy – Madhulika Srikumar: *Principled Artificial Intelligence. Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI*. The Berkman Klein Center for Internet & Society Research Publication Series, 2020. Online: <https://doi.org/10.2139/ssrn.3518482>
- Floridi, Luciano: Mature Information Societies – a Matter of Expectations. *Philosophy & Technology*, 29. (2016), 1. 1–4. Online: <https://doi.org/10.1007/s13347-016-0214-6>
- Floridi, Luciano – Mariarosaria Taddeo: What Is Data Ethics? *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 374. (2016), 2083. Online: <https://doi.org/10.1098/rsta.2016.0360>
- Fukuyama, Francis: *Bizalom. A társadalmi érények és a jólét megteremtése*. Ford. Somogyi Pál László. Budapest, Európa Könyvkiadó, 2007.
- Fukuyama, Francis: The Thing That Determines a Country's Resistance to the Coronavirus. *The Atlantic*, 2020. március 30. Online: www.theatlantic.com/ideas/archive/2020/03/thing-determines-how-well-countries-respond-coronavirus/609025/
- Hern, Alex: Facebook T&Cs Introduced 'Research' Policy Months After Emotion Study. *The Guardian*, 2014. július 1. Online: www.theguardian.com/technology/2014/jul/01/facebook-data-policy-research-emotion-study
- Information Commissioner's Office: *Big Data, Artificial Intelligence, Machine Learning and Data Protection*. Online: <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>
- Institute for Ethics in Artificial Intelligence. Online: www.ieai.sot.tum.de/
- Jongen, Tom: How to Make Your Data Project Ethical by Design. *Towards Data Science*, 2021. június 11. Online: <https://towardsdatascience.com/how-to-make-your-data-project-ethical-by-design-99629dcd2443>
- Jouhki, Jukka – Epp Lauk – Maija Penttinen – Niina Sormanen – Turo Uskali: Facebook's Emotional Contagion Experiment as a Challenge to Research Ethics. *Media and Communication*, 4. (2016), 4. Online: <https://doi.org/10.17645/mac.v4i4.579>
- Kéfer Ádám: Öngyilkos lett egy fiatal családapa, miután hetekig beszélgetett a mesterséges intelligenciával. *Index*, 2023. március 30. Online: <https://index.hu/kulfold/2023/03/30/chatbot-chatgpt-openai-mesterseges-intelligencia-ongyilkossag-belgium/>
- Kramer, Adam D. I. – Jamie E. Guillory – Jeffrey T. Hancock: Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks. *Proceedings of the National Academy of Sciences*, 111. (2014), 24. 8788–8790. Online: <https://doi.org/10.1073/pnas.1320040111>
- Larsson, Stefan: On the Governance of Artificial Intelligence through Ethics Guidelines. *Asian Journal of Law and Society*, 7. (2020), 3. 437–451. Online: <https://doi.org/10.1017/als.2020.19>
- Leimeiszer Barnabás: A bizalom meglétén dől el a társadalmak sorsa – Fukuyama a járvány következményeiről. *Mandiner*, 2020. április 10. Online: https://mandiner.hu/cikk/20200409_nem_a_politikai_rendszer_tipusan_mulik_a_sikeres_valsagkezeles_francis_fukuyama_a_koronavirusrol
- Maanen, Gijs van: AI Ethics, Ethics Washing, and the Need to Politicize Data Ethics. *Digital Society*, 1. (2022), 2. Online: <https://doi.org/10.1007/s44206-022-00013-3>
- Pálffy Dániel Ábel: „Fennáll a lehetőség, hogy kiirtjuk az emberiséget” – hátborzongató beszélgetés a mesterséges intelligenciával. *Mandiner*, 2023. március 25. Online: https://mandiner.hu/cikk/20230317_mesterseges_intelligencia_emberiseg_chatgpt

- Richterich, Annika: Big Data: Ethical Debates. In Annika Richterich: *The Big Data Agenda. Data Ethics and Critical Data Studies*. London, University of Westminster Press, 2018. 33–52. Online: <https://doi.org/10.2307/j.ctv5vddsw>
- Taddeo, Mariarosaria: Trusting Digital Technologies Correctly. *Minds and Machines*, 27. (2017), 4. 565–568. Online: <https://doi.org/10.1007/s11023-017-9450-5>
- Taylor, Linnet: The Ethics of Big Data as a Public Good: Which Public? Whose Good? *Philosophical Transactions: Mathematical Physical and Engineering Sciences*, 374. (2016), 2083.
- Taylor, Linnet: Global Data Justice. *Communications of the ACM*, 62. (2019), 6. 22–24. <https://doi.org/10.1145/3325279>
- Taylor, Linnet – Lina Dencik: Constructing Commercial Data Ethics. *Technology and Regulation*, 2. (2020), 1–10. Online: <https://doi.org/10.26116/techreg.2020.001>
- The World's Most Valuable Resource Is No Longer Oil, But Data. *The Economist*, 2017. május 6. Online: www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data
- Török Csaba: *Bölcsességkeresők*. Budapest, L'Harmattan, 2008.
- Vadász, Pál – Zsolt Zódi: The Accountability of Intelligence and Law Enforcement Agencies in Information Search Activities. In Noella Edelman et al. (szerk.): *Electronic Participation. ePart 2021*. Cham, Springer, 2021. 210–220. Online: https://doi.org/10.1007/978-3-030-82824-0_16
- Walker, Lauren: Belgian Man Dies by Suicide Following Exchanges with Chatbot. *The Brussels Times*, 2023. március 28. Online: www.brusselstimes.com/430098/belgian-man-commits-suicide-following-exchanges-with-chatgpt
- Zách Dániel: Egy csetbot bátorítása után lett öngyilkos egy belga férfi. *Telex*, 2023. április 3. Online: <https://telex.hu/tech/2023/04/03/chatbot-mestersegesintelligencia-etika-szoftverfejlesztes>

Vákát

A precíziós medicina és a demokrácia kölcsönhatásai



Az elmúlt két évtizedben hatalmas léptékben fejlődött az orvostudomány. A genetikai-genomikai tudományos fejlődés elhozta a genomszerkesztés korszakát, megteremtve ezzel a génterápia biztonságos és széles körű alkalmazásának lehetőségét. Első olvasatra meglepő lehet a precíziós medicina kérdéskörét abból a szempontból vizsgálni, hogy hat-e, hathat-e a demokráciára, és vice versa. Jelen tanulmány mégis arra vállalkozik, hogy bizonyítsa, szoros kölcsönhatás áll fenn a kettő között.

Bevezetés

Az elmúlt két évtizedben hatalmas léptékben fejlődött az orvostudomány. A genetikai-genomikai tudományos fejlődés elhozta a genomszerkesztés korszakát, megteremtve ezzel a génterápia biztonságos és széles körű alkalmazásának lehetőségét. Az átfogó (multi-)biomarker-tesztelés lehetővé teszi a pontos diagnózis felállítását, a hatékonyabb terápiát, beleértve az adekvát gyógyszeres kezelést is. A legígéretesebbnek a monogén és tumoros megbetegedések terápiás lehetőségei ígérkeznek. Egyre többen fogunk tehát hallani a precíziós medicináról, amely az általános definíció szerint „egy új feltörekvő megközelítés a kialakulóban lévő vagy manifestálódott betegség megelőzésére vagy gyógyítására, amely figyelembe veszi az egyén genetikai sajátosságait, környezetét és életmódját”.¹ A precíziós orvoslás azonban magában hordozza az egészségügyi egyenlőtlenségek súlyosbodásának kockázatát is, különösen a kisebbségi csoportok, valamint a szerény jövedelemmel rendelkezők körében, hiszen a hátrányos körülmények között élők és a kisebbségek világszerte gyakran szembesülnek diszkriminációval az egészségügyben, és az átlagnál rosszabb egészségügyi ellátásban részesülnek.² A társadalmi polarizáció erősödése azonban a hosszú távú gazdasági fejlődést, ezáltal a demokrácia stabilitását is veszélyezteti. Az egészséghez való jog az emberi méltóság, az emberi jogok és a demokratikus

¹ Pilar Garrido et al.: Proposal for the Creation of a National Strategy for Precision Medicine in Cancer: A Position Statement of SEOM, SEAP, and SEFH. *Clinical and Translational Oncology*, 20. (2018), 4. 443–447; Yin Paradies: A Systematic Review of Empirical Research on Self-reported Racism and Health. *International Journal of Epidemiology*, 35. (2006), 4. 888–901.

² Kashyap Patel – Maharshi Patel – Hirangi Mukhi: Despite Advances in Precision Medicine, Disparities Persist. *Targeted Therapies in Oncology*, 9. (2020), 16.

normák érvényesülésének egyik alapvető dimenziója.³ Az egészségben leélt hosszú élet önmagában vett érték az egyének számára, társadalmi és egyéni szinten is a jólétnek egyik alapvető összetevője, amelyet a társadalmi-gazdasági tényezők és a kormányzati politikák meghatározóan befolyásolnak.⁴ A 2000-es évek elejétől az Európai Unió egészségpolitikájában is az a cél dominál, hogy a tagállamok kormányai a jó egészséget és egészségügyi rendszert a gazdasági növekedés egyik kulcsának lássák,⁵ ezáltal a stabilitás egyik összetevőjeként tekintsenek rá. A Covid-19-járvány alatt is bebizonyosodott, milyen szoros kölcsönhatások vannak az egészségügy és a stabilitás között. Az egészségügyi egyenlőtlenségek csökkentése, illetve a szakadék mélyülésének megakadályozása tehát alapvető jelentőségű számunkra. A precíziós medicina segítségével új alapokra helyeződő orvostudomány is csak akkor válthatja be ígéreteit, ha képes szembenézni ezekkel a kihívásokkal.

Az egészségügyi egyenlőtlenségek mibenléte

Az egészséget az ember egyéni genetikai adottságai és életmódja mellett a személyes, társadalmi, gazdasági és környezeti tényezők széles köre határozza meg.⁶ A fő tényezők a következők: jövedelem és társadalmi helyzet; foglalkoztatás és munkakörülmények; oktatás; gyermekkori élmények; fizikai környezet; szociális támogatási hálózatok; személyes viselkedés és megküzdési készség; egészségügyi ellátáshoz való hozzáférés; biológia és genetika; nem; és a kultúra.⁷ Az egészségi állapotban nem csupán az egyének, de a közösségek között is vannak eltérések. Az egyes társadalmi, demográfiai vagy földrajzi lakosságcsoportok egészségében jelentkező egy vagy több szisztematikus különbséget egészségügyi egyenlőtlenségeknek nevezzük.⁸ Az egész-

³ Havasi Éva: A megtört egészség. A hazai lakosság egészségi állapotának egyenlőtlenségei, különös tekintettel a szegényekre. *Népegészségügy*, 89. (2002), 2. 80–92.

⁴ Orosz Éva – Kollányi Zsófia: Egészségi állapot, egészség-egyenlőtlenségek nemzetközi összehasonlításban. In Kolosi Tamás – Tóth István György (szerk.): *Társadalmi Ríport 2016*. Budapest, TÁRKI, 2016. 334–357.

⁵ Commission of the European Communities: *White Paper – Together for Health: A Strategic Approach for the EU 2008–2013*. COM(2007)630 végleges (2007. október 23.).

⁶ Eisingerné Balassa Boglárka: Az egészségügyi kiadások és a moralitás közötti összefüggések vizsgálata Magyarországon és az EU 28-ak viszonylatában. In Szakály Zsolt (szerk.): *Egészség SPORT Gazdaság II*. Győr, Mobilis Közhasznú Nonprofit Kft., 2020. 74–87; Eisingerné Balassa Boglárka – Csákvári Tímea – Ágoston István: Az egészségbiztosítási gyógyszerkiadások alakulása Magyarországon. *Orvosi Hetilap*, 160. (2019), 1. 49–54.

⁷ WHO: Review of Social Determinants and the Health Divide in the WHO European Region. Final Report.

⁸ B. Starfield: Basic Concepts in Population Health and Health Care. *Journal of Epidemiology and Community Health*, 55. (2001), 7. 452–454.

seget befolyásoló tényezők számbavételével levonható az a következtetés, hogy egyes egyenlőtlenségek biológiai, míg mások társadalmi okokra vezethetők vissza.

2012-ben a WHO/Európa elfogadta az *Egészségügy 2020-as szakpolitikai keretét*, amelynek célja jelentősen javítani az egészséget és előremozdítani a lakosság jólétét; csökkenteni az egészségügyi egyenlőtlenségeket; megerősíteni a közegészségügyet és biztosítani az emberközpontú egészségügyi rendszereket, amelyek egyetemesek, méltányosak, fenntarthatóak és jó minőségűek.⁹ Az Európai Unió számára ma az egyik legégetőbb teendő a különböző társadalmi-gazdasági csoportok között, illetve az EU különböző részei között mutatkozó egészségügyi egyenlőtlenségek felszámolása jelenti. 2013. december 11-én a Bizottság közzétette az *Egészségügyi egyenlőtlenségek az EU-ban* című jelentését.¹⁰ A dokumentum három fő megállapítást tett: először is az átlagos élettartam rövidebb a kelet- és közép-európai országokban; másodsor, a társadalmi grádiens az egészségügyben meredekebb keleten, mint nyugaton; harmadszor pedig az országon belüli várható élettartam lényegesen alacsonyabb az alacsonyabban iskolázottaknál, mint a felsőoktatási végzettséggel rendelkezők között.

2020-ban az Európai Parlament jelentése nem csupán a tagállamok közötti egészségügyi egyenlőtlenségekre világított rá, hanem arra is, hogy az országokon belül az eltérő társadalmi-gazdasági csoportok egészségi állapotában is jelentős különbségek vannak, amelyek az életmódbeli eltérésekre is visszavezethetők: egészségtelen táplálkozás, elhízás, szűrővizsgálatokon való ritkább megjelenés stb.¹¹ Az Eurostat 2017-es megállapításait idézve¹² felhívta a jelentés a figyelmet arra is, hogy az uniós lakosok 45%-a számolt be arról, hogy az egészségügyi ellátással kapcsolatos kiadások jelentős terhet jelentenek a háztartásuk számára. Azok körében, akik nem jutnak megfelelő egészségügyi ellátáshoz, nem kapják meg a szükséges gyógyszereket, ez a körülmény a legtöbb esetben az anyagi helyzetükre volt visszavezethető.¹³

Az Amerikai Egyesült Államokban az egészségügyi egyenlőtlenségeket elsősorban a faji és etnikai hovatartozásra, a nemre, a szexuális irányultságra és nemi identitásra, valamint a fogyatékosági státuszra vezetik vissza.¹⁴

⁹ WHO (é. n.): i. m.

¹⁰ European Commission: Health Inequalities in the EU. Final Report of a Consortium. 2013.

¹¹ European Commission (2013): i. m.

¹² The Burden of Healthcare on Households' Budgets. *Eurostat*, 2019. február 19.

¹³ European Commission (2013): i. m.

¹⁴ National Academies of Sciences, Engineering, and Medicine; Health and Medicine Division; Board on Population Health and Public Health Practice; Committee on Community-Based Solutions to Promote Health Equity in the United States: *Communities in Action. Pathways to Health Equity*. Washington, D. C., National Academies Press, 2017.

Az egészségügyi egyenlőtlenségek és a demokrácia kölcsönhatásai

A lakosság egészségének javításához nélkülözhetetlenek az egészségügyi és más szektorokban hozott megfelelő döntések.¹⁵ Számos kutatási eredmény alapján ismert, hogy az egészségüghöz közvetlenül nem kapcsolódó szakpolitikák sokszor nagyobb hatást gyakorolnak a lakosság egészségi állapotára, mint az egészségügy maga.¹⁶ Az emberiség történelme a jólét növekedése mellett a várható élettartam figyelemre méltó növekedésének tanúja volt. A gazdasági fellendülés mellett az oktatási rendszer fejlődését is közvetlen összefüggésbe hozzák a halandóság csökkenésével.¹⁷ Az elmúlt 15 évben egyre több kutató vizsgálta, vajon a politikai berendezkedés kihatással van-e a várható élettartamra. Timothy Besley és Masayuki Kudamatsu 2006-ban megjelent tanulmánya szerint „[e]rős korreláció van a demokratikus intézmények és az egészségügy között. Demokráciában az emberek tovább élnek.”¹⁸ Thomas J. Bollyky és munkatársai 2019-ben a *The Lancet*-ben közzétették le tanulmányukat, amelyben 170 állam adatai alapján vizsgálták meg a demokrácia és az okspecifikus halálozás¹⁹ közötti összefüggéseket.²⁰ Megállapították, hogy „[a] szív- és érrendszeri betegségek, közlekedési balesetek, rákos megbetegedések, a cirrhosis és egyéb nem fertőző betegségek okozta halandóságban bekövetkezett változásokat a demokratikus tapasztalat jobban magyarázza, mint a GDP változása”.²¹ Rafael Dall’Alba és munkatársai szintén a *The Lancet*-ben 2022-ben megjelent tanulmánya arra is felhívja a figyelmet, hogy „[a] kérdés, hogy a demokrácia jót tesz-e az egészségnek, fontos, de nem elégséges kérdés. Sürgősen meg kell vitatni, hogyan lehet hatékonyan elősegíteni a lehető legtöbb szereplő bevonását az egészségpolitikai vitákba

¹⁵ Nogel Mónika: A bizonyítékokon alapuló ellátás és az egészségügyi minőségbiztosítás kapcsolata. *Med. et Jur.*, 8. (2017a), 2. 20–26; Nogel Mónika: A bizonyítékokon alapuló ellátás és az egészségügyi minőségbiztosítás kapcsolata II. *Med. et Jur.*, 8. (2017b), 3. 4–10.

¹⁶ Marc Suhrcke et al.: *The Contribution of Health to the Economy in the European Union*. European Communities, 2005; Bakacs Márta et al.: A halandóságot befolyásoló egyéni biológiai és társadalmi-gazdasági tényezők hatásrendszerének vizsgálata. *Orvosi Hetilap*, 149. (2008), 50. 2371–2376.

¹⁷ Torsten Persson: *Forms of Democracy, Policy and Economic Development*. NBER Working Paper No. 11171. iNational Bureau of Economic Research, 2005.

¹⁸ Timothy Besley – Masayuki Kudamatsu: Health and Democracy. *American Economic Review*, 96. (2006), 2. 313–318.

¹⁹ Az okspecifikus halálozási arányszám (ráta) egy meghatározott ok (betegség, baleset stb.) következtében meghaltakra nézve adja meg a halálozási arányszámot, általában, de nem minden esetben 100 000 főre vetítve. A mutatószám a halálozás okspecifikus összetételének elemzésére alkalmas. A halálokok az egyes országokban nagymértékben eltérhetnek egymástól, de változhatnak időben is, mivel sok tényező befolyásolhatja őket, beleértve az általános közegészségügyi és környezeti jellemzőket. Például Magyarországon 2013-ban a keringési rendszer betegségeiből következően meghaltak okspecifikus halálozási arányszáma 636,6 volt százezer főre vetítve.

²⁰ Thomas J. Bollyky et al.: The Relationships between Democratic Experience, Adult Health, and Cause-specific Mortality in 170 Countries between 1980 and 2016: An Observational Analysis. *The Lancet*, 393. (2019), 10181. 1628–1640.

²¹ Bollyky et al. (2019): i. m.

olyan átlátható eljárásokon keresztül, amelyek erősítik szolidaritást és együttműködést.”²² Az egészséghez való jog és egyéb emberi jogok és a demokrácia közötti összefüggések nyilvánvalók. Az egészségyenlőtlenségek növekedése súlyosan veszélyezteti az ország gazdasági teljesítményét, hosszú távú társadalmi fejlődését, ezért ezeknek az egyenlőtlenségeknek a csökkentése a társadalom számára elengedhetetlen fontosságú.²³ Megfelelő intézkedésekkel – adópolitika, szabályozási kérdések, jóléti szolgáltatások stb. – az emberek egészségi állapota látványosan javítható „indirekt”, az egészségügyi rendszeren kívüli módszerekkel is, mivel így csökkenthetők a köztük lévő egyenlőtlenségek.²⁴ A valóban egyenlőségelvű egészségügy felé vezető első lépést – legyen szó a hozzáférésről vagy az egészségi állapot javításáról és az ezekkel kapcsolatos egyenlőtlenségek csökkentéséről – valószínűleg az alapellátás és a tágran értelmezett közegészségügy fejlesztése jelenthetné.²⁵

A precíziós medicina hatása az egészségre és az egészségügyre (egészségügyi egyenlőtlenségek, egészségnyereség, egészségügyi kiadások)

Az onkológiai kórkepek esetében az Európai Unió tagállamai és az Egyesült Királyság között lényeges eltéréseket tapasztaltak a kutatók a tekintetben, hogy az érintettek mennyiben férnek hozzá a legmodernebb precíziós diagnosztikai és terápiás eszközökhöz. Négy mérőszámot néztek: laboratóriumi hozzáférhetőség, tesztek elérhetősége, tesztek költségterítésének lehetőségei, a megrendelt tesztek száma.²⁶ Megállapították, hogy hiányzik az összhang az államok között a genetika klinikai hasznosságának és költséghatékonyságának megítélésében, ami Európa-szerte negatív hatással van a legújabb diagnosztikai eljárások és terápia hozzáférhetőségére.²⁷ Hiszen, ha a döntéshozók nem hisznek abban, hogy az új diagnosztikai módszerek és terápiás eljárások társadalmi szinten megtérülnek, kevésbé hajlandóak ezeket anyagilag támogatni, hiányoznak majd az ez irányú népegészségügyi programok. Hátrányosan befolyásolhatja a precíziós orvosláshoz való hozzáférést az is, ha a népesség alacsonyabb iskolázottságú, a társadalom egészségügyi és biológiai

²² Rafael Dall’Alba – Marco André Germanò – Cristianne Famer Rocha: Yes, Democracy Is Good For Our Health – But Which Democracy? *The Lancet*, 399. (2022), 10338. 1864.

²³ Kollányi Zsófia Katalin: *Az egészségi állapot társadalmi és gazdasági összefüggésrendszere*. PhD-értekezés. ELTE TÁTK Szociológia Doktori Iskola, 2016.

²⁴ Tanyi Attila – Kollányi Zsófia: *Egészségpolitika és Etika*. Budapest, DEMOS Hungary, 2008.

²⁵ Tanyi–Kollányi (2008): i. m.

²⁶ International Quality Network for Pathology (IQN Path) – European Cancer Patient Coalition (ECPC) – European Federation of Pharmaceutical Industries and Associations (EFPIA): *Unlocking the Potential of Precision Medicine in Europe – Improving Cancer Care through Broader Access to Quality Biomarker Testing*. 2021.

²⁷ Katherine Payne – Lieven Annemans: Reflections on Market Access for Personalized Medicine: Recommendations for Europe. *Value in Health*, 16. (2013), 6. S32–S38.

ismeretei nem kielégítőek, nem kellően tájékozottak a lehetőségeikről, illetve ha az egészségügyi személyzet nem rendelkezik kellő mélységű ismeretekkel a legújabb módszerek alkalmazási lehetőségeiről, hatékonyságáról, vagy épp nincs meg a kellő bizalom irántuk. Éppen ezért nagyobb hangsúlyt kell fektetni a precíziós orvoslásra az orvosképzés és posztgraduális képzés során,²⁸ és a társadalmat is befogadóvá kell tenni az új lehetőségek iránt. Ennek előfeltétele a természettudományos (biológiai, genetikai, kémiai) ismeretek bővítése és az egészségügyi ellátórendszerbe vetett bizalom növelése, az orvos-beteg közötti bizalmon alapuló kapcsolat megerősítése. Az egyén szintjén ugyanakkor még nem elegendő a precíziós medicina felé nyitni. Ha a társadalombiztosítás²⁹ által finanszírozott formában nem elérhetőek ezek a lehetőségek, akkor csak azok engedhetik meg maguknak, akik saját forrásból ki tudják fizetni. Így a szociális szakadék tovább mélyül, a hátrányos helyzetűek egészségi állapota, az egészségben eltöltött éveik száma és várható élettartamuk továbbra is szignifikánsan elmarad a jobb körülmények között élő rétegtől. Tehát ilyen módon a fennálló egészségügyi egyenlőtlenségek tovább mélyülnek. Holott a precíziós medicina hozzájárulhat a korai diagnózishoz, a gyorsabb gyógyuláshoz, ahhoz, hogy a lakosság várható élettartama nőjön, és minél több évet töltsenek egészségesen: egyszóval az egészségnyereséghez. Az egészségnyereség elérése mint fókusz az egyén és társadalom szintjén is természetes, az ellátást finanszírozó oldalán mégis bonyolult kérdéseket vet fel. Kaló Zoltán és munkatársai az alábbiakra hívják fel a figyelmet: „Makroszinten fontos, hogy a rendelkezésre álló erőforrásokból a lehető legtöbb egészségnyereséget állítsunk elő, ezt allokatív hatékonyságnak nevezzük. Az allokatív hatékonyságot az egyes technológiák befogadásához vagy finanszírozási protokolljához kapcsolódó döntések szintjén a költséghatékonysági és a költségvetési hatásvizsgálatok hivatottak elősegíteni. A közgazdasági célfüggvények mellett egy új technológia értékelésénél a finanszírozónak egyéb szempontokat is mérlegelnie kell, mint a népegészségügyi prioritások vagy a méltányosság kérdése.”³⁰ A szerzők megkülönböztetik a precíziós medicina kiadáscsökkentő és -növelő hatásait is. Előbbiek között a validált diagnosztikai teszteknek tulajdonítanak jelentőséget, amelyekkel megspórolhatóak a szükségtelen vizsgálatok és kezelések költségei, az elhúzódó differenciáldiagnosztika. Hangsúlyozzák, hogy a precíziós medicinának hála rövidülhet a terápia, a mellékhatások elmaradása szükségtelenné teszi az egyébként

²⁸ International Quality Network for Pathology (IQN Path) – European Cancer Patient Coalition (ECPC) – European Federation of Pharmaceutical Industries and Associations (EFPIA) (2021): i. m.

²⁹ Németh Noémi et al.: A heveny szívinfarktus okozta országos epidemiológiai és egészségbiztosítási betegségteher Magyarországon. *Orvosi Hetilap*, 162. (2021), 1. 6–13; Boncz Imre et al.: A közfinanszírozott laboratóriumi szolgáltatások egészségpolitikai tapasztalatai Magyarországon egészségbiztosítási adatok elemzésével. *Orvosi Hetilap*, 161. (2020), 12. 468–473.

³⁰ Kaló Zoltán et al.: A személyre szabott orvoslás egészség-gazdaságtani vonatkozásai, azaz csökkentik-e a személyre szabott technológiák az egészségügyi kiadásokat? *Interdiszciplináris Magyar Egészségügy*, 13. (2014), 5. 41–45.

felmerülő további vizsgálatokat és kezelést.³¹ A kiadásnövelő tényezők között említik a szerzők a diagnosztika és terápia költségeit és az esetlegesen nyert életevek alatt szerzett új vagy fennmaradó krónikus betegségek miatti többletköltségeket.³² A szerzők kiemelik: „A személyre szabott orvoslás nem jelenthet költségmegtakarítást, ez a medicina egyik leginnovatívabb területétől nem is várható el, azt azonban továbbra is fontos hangsúlyozni, hogy a többlet egészségnyereséget minden esetben elfogadható többletköltséggel kell előállítanunk, azaz a forrásainkat költséghatékonyan kell felhasználnunk. [...] Fontos kiegészítés, hogy az egészségre ma már legtöbbször erőforrásként is tekintünk, mely mind egyéni, mind társadalmi szinten gazdasági előnyökkel párosul. Az egészséges embereknek magasabb a termelékenysége, és megtakarítási rátája, magasabb iskolai végzettséggel rendelkeznek, így jobb anyagi helyzetben vannak. Hosszabb ideig maradnak aktívak, így kevésbé terhelik összességében a szociális ellátórendszert. A felsorolt tényezők pozitívan hathatnak az egészségügyi kassza bevételi oldalára, kismértékben megteremtve a lehetőséget a megnövekedett kiadások finanszírozására.”³³

Konklúzió

Az egészség önmagában vett érték az egyén és a társadalom számára.³⁴ Az egészséges népesség gazdaságilag aktív,³⁵ és kevésbé terheli meg a szociális ellátórendszert.³⁶ A jólét, a magasabb iskolázottság és a demokratikus berendezkedés igazoltan pozitív hatással van az egészségre. Ezzel ellentétben az egészségügyi egyenlőtlenségek – amelyeket okozhat a kisebbségekkel szembeni diszkrimináció, az általános rosszabb életszínvonal, az egészséges életmódhoz és az egészségügyi ellátáshoz való anyagi lehetőségek korlátozottsága miatti hozzáférés hiánya – hátrányosan hatnak az egyén egészségére és a közegészségügyre is. Ebbe a szoros kölcsönhatásokkal átszőtt rendszerbe kell az orvostudomány egyik legígéretesebb vívmányát, a precíziós medicinát beilleszteni. A precíziós medicina egyértelműen növeli az egészségügyi kiadásokat, de emellett az egészségnyereséget is. Az állami források költséghatékony,

³¹ Kaló et al. (2014): i. m.

³² Kaló et al. (2014): i. m.

³³ Kaló et al. (2014): i. m.

³⁴ Kovács Gábor – Nogel Mónika – Fáskerty Éva: *Egészségügyi és szociális jogi kézikönyv*. Győr, Universitas-Győr Nonprofit Kft., 2017a; Kovács Gábor – Nogel Mónika – Fáskerty Éva: *Egészségügyi és szociális jog*. Győr, Universitas-Győr Nonprofit Kft., 2017b.

³⁵ Boncz Imre – Kovács Gábor: Az Egészségbiztosítási Alap munkaerőpiaci kapcsolódásai Magyarországon. *Orvosi Hetilap*, 160. (2019), 1. 3.

³⁶ Kovács Gábor: A rokkantság, megváltozott munkaképesség, rehabilitációs ellátások változása Magyarországon 1990 és 2015 között. *Orvosi Hetilap*, 160. (2019), 1. 29–36; Nogel Mónika: Az Egészségbiztosítási Alap táppénzes trendjei Magyarországon 1997 és 2017 között. *Orvosi Hetilap*, 160. (2019), 1. 37–42.

népegészségügyi prioritásokat szem előtt tartó, méltányos felhasználása hozzájárulhat ahhoz, hogy a precíziós medicina ne szélesítse tovább az egészségügyi egyenlőtlenségeket. Nyilvánvaló, hogy ennek a folyamatnak először a feltételeit kell megteremteni, és összességében nehéz feladatnak ígérkezik.

Felhasznált irodalom

- Bakacs Márta – Vitrai József – Várhalmi Zoltán – Kaposvári Csilla – Hermann Dóra – Kabos Sándor – Löw András: A halandóságot befolyásoló egyéni biológiai és társadalmi-gazdasági tényezők hatásrendszerének vizsgálata. *Orvosi Hetilap*, 149. (2008), 50. 2371–2376. Online: <http://doi.org/10.1556/OH.2008.28497>
- Besley, Timothy – Masayuki Kudamatsu: Health and Democracy. *American Economic Review*, 96. (2006), 2. 313–318.
- Bollyky, Thomas J. – Tara Templin – Matt Cohen – Diana Schoder – Joseph L. Dieleman – Simon Wigley: The Relationships Between Democratic Experience, Adult Health, and Cause-specific Mortality in 170 Countries Between 1980 and 2016: An Observational Analysis. *The Lancet*, 393. (2019), 10181. 1628–1640. Online: [https://doi.org/10.1016/S0140-6736\(19\)30235-1](https://doi.org/10.1016/S0140-6736(19)30235-1)
- Boncz Imre – Kovács Gábor: Az Egészségbiztosítási Alap munkaerőpiaci kapcsolódásai Magyarországon. *Orvosi Hetilap*, 160. (2019), 1. 3–5. Online: <https://doi.org/10.1556/650.2019.31410>
- Boncz Imre – Sebestyén Andor – Endrei Dóra – Ágoston István – Csákvári Tímea – Kovács L. Gábor – Miseta Attila: A közfinanszírozott laboratóriumi szolgáltatások egészségpolitikai tapasztalatai Magyarországon egészségbiztosítási adatok elemzésével. *Orvosi Hetilap*, 161. (2020), 12. 468–473. Online: <https://doi.org/10.1556/650.2020.31683>
- Commission of the European Communities: *White Paper – Together for Health: A Strategic Approach for the EU 2008–2013*. COM(2007)630 végleges (2007. október 23.)
- Dall’Alba, Rafael – Marco André Germanò – Cristianne Famer Rocha: Yes, Democracy Is Good for Our Health – But Which Democracy? *The Lancet*, 399. (2022), 10338. 1864. Online: [https://doi.org/10.1016/S0140-6736\(22\)00833-9](https://doi.org/10.1016/S0140-6736(22)00833-9)
- Eisingerné Balassa Boglárka: Az egészségügyi kiadások és a morálitás közötti összefüggések vizsgálata Magyarországon és az EU 28-ak viszonylatában. In Szakály Zsolt (szerk.): *Egészség SPORT Gazdaság II*. Győr, Mobilis Közhasznú Nonprofit Kft., 2020. 74–87.
- Eisingerné Balassa Boglárka – Csákvári Tímea – Ágoston István: Az egészségbiztosítási gyógyszerkiadások alakulása Magyarországon. *Orvosi Hetilap*, 160. (2019), 1. 49–54. Online: <https://doi.org/10.1556/650.2019.31394>
- European Commission: *Health Inequalities in the EU. Final Report of a Consortium*. 2013. Online: <https://op.europa.eu/en/publication-detail/-/publication/e3d84056-2c24-4bd3-92db-2cb71a0d0bc4/language-en>
- Garrido, Pilar – Azucena Aldaz – Ruth Vera – Miguel Angel Calleja – E. De Álava – Miguel Martin – Xavier Matias-Guiu – José Palacios: Proposal for the Creation of a National Strategy for Precision Medicine in Cancer: A Position Statement of SEOM, SEAP, and SEFH. *Clinical and Translational Oncology*, 20. (2018), 4. 443–447. Online: <https://doi.org/10.1007/s12094-017-1740-0>

- Havasi Éva: A megtört egészség. A hazai lakosság egészségi állapotának egyenlőtlenségei, különös tekintettel a szegényekre. *Népegészségügy*, 89. (2002), 2. 80–92.
- International Quality Network for Pathology (IQN Path) – European Cancer Patient Coalition (ECPC) – European Federation of Pharmaceutical Industries and Associations (EFPIA): *Unlocking the Potential of Precision Medicine in Europe – Improving Cancer Care through Broader Access to Quality Biomarker Testing*. 2021. Online: <https://ecpc.org/wp-content/uploads/2021/03/unlocking-the-potential-of-precision-medicine-in-europe-23022021.pdf>
- Kaló Zoltán – Boncz Imre – Dank Magdolna – Kóczyán Kristóf – Molnár Mária Judit – Nagy Balázs – Németh György – Pitter János – Zelei Tamás: A személyre szabott orvoslás egészség-gazdaságtani vonatkozásai, azaz csökkentik-e a személyre szabott technológiák az egészségügyi kiadásokat? *Interdiszciplináris Magyar Egészségügy*, 13. (2014), 5. 41–45.
- Kollányi Zsófia Katalin: *Az egészségi állapot társadalmi és gazdasági összefüggérendszer*. PhD-értekezés. ELTE TÁTK Szociológia Doktori Iskola, 2016.
- Kovács Gábor: A rokkantság, megváltozott munkaképesség, rehabilitációs ellátások változása Magyarországon 1990 és 2015 között. *Orvosi Hetilap*, 160. (2019), 1. 29–36. Online: <https://doi.org/10.1556/650.2019.31372>
- Kovács Gábor – Nogel Mónika – Fáskerty Éva: *Egészségügyi és szociális jogi kézikönyv*. Győr, Universitas-Győr Nonprofit Kft., 2017a.
- Kovács Gábor – Nogel Mónika – Fáskerty Éva: *Egészségügyi és szociális jog*. Győr, Universitas-Győr Nonprofit Kft., 2017b.
- National Academies of Sciences, Engineering, and Medicine; Health and Medicine Division; Board on Population Health and Public Health Practice; Committee on Community-Based Solutions to Promote Health Equity in the United States: *Communities in Action. Pathways to Health Equity*. Washington, DC, National Academies Press, 2017. Online: www.ncbi.nlm.nih.gov/books/NBK425844/
- Németh Noémi – Endrei Dóra – Elmer Diána – Csákvári Tímea – Horváth Lilla – Kajos Luca Fanni – Cziráki Attila – Boncz Imre: A heveny szívinfarktus okozta országos epidemiológiai és egészségbiztosítási betegségteher Magyarországon. *Orvosi Hetilap*, 162. (2021), 1. 6–13. Online: <http://doi.org/10.1556/650.2021.32153>
- Nogel Mónika: A bizonyítékokon alapuló ellátás és az egészségügyi minőségbiztosítás kapcsolata. *Med. et Jur.*, 8. (2017a), 2. 20–26.
- Nogel Mónika: A bizonyítékokon alapuló ellátás és az egészségügyi minőségbiztosítás kapcsolata II. *Med. et Jur.*, 8. (2017b), 3. 4–10.
- Nogel Mónika: Az Egészségbiztosítási Alap táppénzes trendjei Magyarországon 1997 és 2017 között. *Orvosi Hetilap*, 160. (2019), 1. 37–42. Online: <https://doi.org/10.1556/650.2019.31391>
- Orosz Éva – Kollányi Zsófia: Egészségi állapot, egészség-egyenlőtlenségek nemzetközi összehasonlításban. In Kolosi Tamás – Tóth István György (szerk.): *Társadalmi Ríport 2016*. Budapest, TÁRKI, 2016. 334–357.
- Paradies, Yin: A Systematic Review of Empirical Research on Self-reported Racism and Health. *International Journal of Epidemiology*, 35. (2006), 4. 888–901. Online: <http://doi.org/10.1093/ije/dyl056>
- Patel, Kashyap – Maharshi Patel – Hirangi Mukhi: Despite Advances in Precision Medicine, Disparities Persist. *Targeted Therapies in Oncology*, 9. (2020), 16. Online: www.targetedonc.com/view/despite-advances-in-precision-medicine-disparities-persist

- Payne, Katherine – Lieven Annemans: Reflections on Market Access for Personalized Medicine: Recommendations for Europe. *Value in Health*, 16. (2013), 6. S32–S38. Online: <http://doi.org/10.1016/j.jval.2013.06.010>
- Persson, Torsten: *Forms of Democracy, Policy and Economic Development*. NBER Working Paper No. 11171. National Bureau of Economic Research, 2005.
- Starfield, B.: Basic Concepts in Population Health and Health Care. *Journal of Epidemiology and Community Health*, 55. (2001), 7. 452–454.
- Suhrcke, Marc – Martin McKee – Regina Sauto Arce – Svetla Tsoleva – Jørgen Mortensen: *The Contribution of Health to the Economy in the European Union*. European Communities, 2005.
- Tanyi Attila – Kollányi Zsófia: *Egészségpolitika és etika*. Budapest, DEMOS Hungary, 2008.
- The Burden of Healthcare on Households' Budgets. *Eurostat*, 2019. február 19. Online: <https://ec.europa.eu/eurostat/web/products-eurostat-news/-/DDN-20190219-1>
- WHO: *Review of Social Determinants and the Health Divide in the WHO European Region. Final Report*. Online: <https://apps.who.int/iris/bitstream/handle/10665/108636/9789289000307-eng.pdf?sequence=1&isAllowed=y>

Domokos Márton

Hogyan segíthetik a mesterséges intelligenciával kapcsolatos „emberi jogi hatásvizsgálatok” a demokráciát?



A mesterségesintelligencia-rendszerek szabályozása körében jelenleg az Európai Unió MI-rendelet-tervezete a legismertebb jogalkotási kezdeményezés, ugyanakkor az MI-rendszerek alapjogokra gyakorolt hatásának elemzésével kapcsolatban korábban már született egy szabályozási eszköz: 2020. április 8-án az Európa Tanács Miniszteri Bizottsága ajánlást bocsátott ki az algoritmikus rendszerek emberi jogokra gyakorolt hatásairól. Az ajánlás kulcsfontosságú eleme, hogy az alapjogi kockázatok azonosítása érdekében az MI-rendszerek fejlesztése és alkalmazása során úgynevezett „emberi jogi hatásvizsgálatok” elvégzését ajánlja az államok és a magánszektor szereplői számára. Ennek az írásnak a célja, hogy bemutassa az ajánlást, kiemelve az ajánlás rendelkezéseinek megvalósításával és az emberi jogi hatásvizsgálatok lefolytatásával kapcsolatos esetleges gyakorlati kihívásokat. Ezen túlmenően példaként ismertetünk egy holland algoritmikus rendszert, amelynek a használatát az illetékes bíróság alapjogi aggályok miatt megtiltotta. Az írásban azt is megvizsgáljuk, hogy az ajánlás rendelkezéseit követve hogyan lehetett volna esetleg csökkenteni ennek a rendszernek a kockázatait.

Bevezetés

A gépi tanulási képességekkel rendelkező mesterségesintelligencia- (MI-) rendszerek egyaránt lehetnek pozitív és negatív hatással a demokrácia működésére és minőségére. Az alapul fekvő technológiában jelentős potenciál rejlik a társadalmilag hasznos innováció és a gazdasági fejlődés szempontjából, de fontos, hogy az MI-rendszerek használata ne sértse az alapjogok gyakorlását, ne vezessen társadalmi és munkaerőpiaci egyenlőtlenségekhez, alkalmazóiik pedig adott esetben szem előtt tartásuk a különleges szükségletekkel bíró személyek igényeit. Az automatizált döntéshozatali folyamatok során ezért meg kell teremteni a teljes körű demokratikus részvételt, felügyeletet és átláthatóságot, különösen abban az esetben, ha az MI-rendszerek használata kedvezőtlen lehet egy-egy személy, bizonyos csoportok vagy a lakosság egészének alapjogaira. Magyarország Alaptörvénye is kifejezetten előírja, hogy biztosítani kell „a demokratikus közvélemény kialakulásához szükséges szabad tájékoztatás feltételeit” – ehhez ugyanakkor ismerni kell az egyes MI-rendszerek pontos hatását.

Az MI-rendszerek szabályozásával kapcsolatban jelenleg a legismertebb jogalkotási kezdeményezés az Európai Unió mesterséges intelligenciára vonatkozó

rendelettervezete¹ (a továbbiakban: MI Rendelettervezet), amelynek tárgyalása és véglegesítése még folyamatban van. Az MI-rendszerek alapjogokra gyakorolt hatásának elemzésével kapcsolatban azonban korábban már született egy szabályozási eszköz: 2020. április 8-án az Európa Tanács (Council of Europe) Miniszteri Bizottsága ajánlást (a továbbiakban: Ajánlás) bocsátott ki az algoritmikus rendszerek emberi jogokra gyakorolt hatásairól.² Az Ajánlás kulcsfontosságú eleme, hogy az alapjogi kockázatok azonosítása érdekében az MI-rendszerek fejlesztése és alkalmazása során úgynevezett „emberi jogi hatásvizsgálatok” elvégzését ajánlja az államok és a magánszektor szereplői számára. (Az Ajánlás egyébként az EU MI Rendelettervezetével ellentétben még nem az „MI-rendszer” fogalmát, hanem az „algoritmikus rendszer” fogalmát használja – a különbség jogi jelentőségére a következő pontban térünk ki, és ha nem kifejezetten az Ajánlást tárgyaljuk, inkább az MI-rendszer fogalmát használjuk.)

Az emberi jogi hatásvizsgálatok alapvető célja, hogy folyamatosan biztosítsák az alapjogok védelmével kapcsolatos felelősséget és elszámoltathatóságot, az adott MI-rendszer használatának megtervezése, feladatainak meghatározása, a használatához szükséges adatok kiválasztása, gyűjtése és elemzése, ezt követően pedig a rendszer tesztelése, telepítése, majd működésének folyamatos ellenőrzése során.

Ennek az írásnak a célja, hogy bemutassa az Ajánlást, kiemelve az Ajánlás rendelkezéseinek megvalósításával és az emberi jogi hatásvizsgálatok lefolytatásával kapcsolatos esetleges gyakorlati kihívásokat. Ezen túlmenően példaként ismertetünk egy holland algoritmikus rendszert, amelynek használatát az illetékes bíróság alapjogi aggályok miatt megtiltotta. Az írásban azt is megvizsgáljuk, hogy az Ajánlás rendelkezéseit követve hogyan lehetett volna esetleg csökkenteni ennek a rendszernek a kockázatait.

Az algoritmikus rendszerek jogi meghatározásának kihívásai

Az algoritmikus rendszerek, illetve az MI-rendszerek jogi meghatározásával kapcsolatban az elmúlt években számos konstruktív vitára került sor. Mivel a pontos definíció hiánya nehézséget okozhat annak eldöntésében, hogy egy-egy rendszer az alkalmazandó szabályozás hatálya alá tartozik-e, és ezért szükséges-e a kapcsolódó kockázatok felmérése és kezelése, érdemes közelebbről megvizsgálni, megfelelő-e erre a célra az Ajánlás által használt definíció, és milyen gyakorlati kihívások merülhetnek fel értelmezése, valamint használata során.

¹ Council of the European Union: *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*. Third Presidency Compromise Text (2022. szeptember 23.).

² Hivatalos magyar fordítást nem sikerült azonosítani, a hivatkozott rendelkezések ezért saját fordításban szerepelnek.

Az Európa Tanács Ajánlása az „algoritmikus rendszereket” az alábbiak szerint határozza meg: „olyan alkalmazások, amelyek – gyakran matematikai optimalizálási technikákat alkalmazva – egy vagy több feladatot látnak el, mint például az adatok gyűjtése, kombinálása, tisztítása, rendezése, osztályozása és következtetések levonása, valamint kiválasztás, rangsorolás, ajánlások készítése és döntéshozatal. Az algoritmikus rendszerek egy vagy több algoritmusra támaszkodva teljesítik követelményeiket az alkalmazási környezetükben, és olyan módon automatizálják a tevékenységeket, amely lehetővé teszi adaptív szolgáltatások létrehozását méretarányosan és valós időben.”³

Mivel az MI-rendszerek jogi meghatározásával kapcsolatban a legfontosabb irányadó szabályozási eszköz várhatóan az EU MI Rendelete lesz, az alábbiakban az Ajánlásban használt definíciót az EU MI Rendelettervezetében használt fogalom meghatározással hasonlítjuk össze.

- a) Az Ajánlás által használt definíció kevésbé konkrét, mint az MI Rendelettervezet fogalom meghatározása. Az MI Rendelettervezet például utal arra, hogy az MI-rendszerek bizonyos szintű autonómiával rendelkeznek, valamint gépi és/vagy ember által biztosított adatok és inputok segítségével, emberek által meghatározott célok elérése érdekében működnek. Ezek a szempontok mind fontos elemei lehetnek az MI-rendszer működésének, az Ajánlás azonban nem tesz róluk említést az algoritmikus rendszer meghatározása során – a gyakorlatban ez esetleg szűkítheti az Ajánlás hatálya alá eső algoritmikus rendszerek körét.
- b) Az Ajánlás ugyanakkor számos példát említ az algoritmikus rendszerek felhasználási körére, ami segíthet pontosabban meghatározni, mi is minősülhet ilyen rendszernek. Külön kiemeli például, hogy ezek a rendszerek a nagyobb pontosság, célzottság és következetesség révén lehetőséget kínálnak az általuk kínált szolgáltatások teljesítményének növelésére, új megoldások nyújtására, továbbá javíthatják az információk kategorizálását és keresetességét – ez jelentős előrelépést tehet lehetővé olyan területeken, mint az orvosi diagnosztika, a közlekedésszervezés és a logisztika.⁴ A lehetséges felhasználási módok közül az Ajánlás említi az egészségüggyel kapcsolatos adatelemzéseket, a forgalom-észszerűsítést, a rendőrségi és határellenőrzési előrejelzéseket, a pénzmosás és a csalás elleni küzdelmet, valamint munkaügyi, foglalkoztatási és oktatási célokat. A fentiek csak példák – ezzel szemben az MI Rendelettervezet igyekszik kimerítően felsorolni azokat a „magas kockázatú” MI-rendszereket, amelyeknek az alkalmazása esetén

³ Council of Europe: Recommendation CM/Rec(2020)1 of the Committee of Ministers to Member States on the Human Rights Impacts of Algorithmic Systems (2020. április 8.). (Európa Tanács: a Miniszteri Bizottság ajánlása az algoritmikus rendszerek emberi jogokra gyakorolt hatásairól – Ajánlás) A. cikk (Hatály és kontextus), 2. pont.

⁴ Ajánlás, A. cikk (Hatály és kontextus), 3. pont.

kiemelt elszámoltathatósági kötelezettségeket határoz meg. Az Ajánlás a példálódzó megközelítéssel inkább azt támogatja, hogy az algoritmikus rendszerek üzemeltetői esetről esetre határozzák meg ezeknek a rendszereknek az alapjogokra gyakorolt hatását, de az érintett alapjogok felsorolásán⁵ túl nem részletezi konkrétan a kapcsolódó kockázatokat – pedig ez hasznos lehet az Ajánlást használó államok és a magánszektor szereplői számára az általuk fejlesztett, illetve használt rendszerekkel kapcsolatos emberi jogi hatásvizsgálatok elvégzése során.

- c) Ezen túlmenően, az Ajánlás az algoritmikus rendszereknek inkább az adatfelhasználási funkciójára fókuszál – kiemeli például, hogy ezek a rendszerek általában nagy adathalmazok mintáinak felderítésével működnek, és statisztikai modelleken alapulnak, amelyek olyan, úgynevezett „visszacsatolási köröket” (*feedback loops*) tartalmazhatnak, amelyek fenntarthatják, megismételhetik és megerősíthetik a rendszerben már meglévő torzításokat, hibákat és feltételezéseket. Az adatfelhasználási funkció azonban csak egy az algoritmikus rendszerek feladatai közül, így kérdéses, hogy indokolt-e ilyen részletességgel kiemelni a definícióban.

Mindent összevetve: az algoritmikus rendszerek Ajánlás-béli definíciójának absztraktabb jellege miatt fennáll annak a veszélye, hogy a gyakorlatban az érintett állami vagy magánszektorban működő szereplők vitatni fogják, hogy egy-egy rendszer az Ajánlás hatálya alá tartozik-e, ez pedig megnehezítheti a kapcsolódó kockázatok felmérését, és ezzel összefüggésben az emberi jogi hatásvizsgálatok lefolytatását. A meghatározás konkrét elemeinek hiánya ugyanakkor nagyobb döntési szabadságot is adhat alkalmazóinak, mert lehetővé teszi, hogy egy-egy algoritmikus rendszer kockázatait az érdekeltek esetről esetre mérhessék fel, és ne kerüljön sor az adott rendszer automatikus besorolására valamilyen szabályozási kategóriába.

Az Ajánlásban foglalt részletes iránymutatások az államok és a magánszektor számára

Az Ajánlás mind az államok, mind a magánszektor szervezetei számára fontos iránymutatásokat határoz meg az algoritmikus rendszerek alapjogokra gyakorolt hatásaival kapcsolatban. Az emberi jogi hatásvizsgálatok lefolytatása során kulcsfontosságú figyelembe venni, hogy az ezeknek az iránymutatásoknak való megfelelés mennyiben teljesül az adott rendszer használata során. Ezért mielőtt rátérünk arra,

⁵ Például a tisztességes eljáráshoz való jog, a magánélethez és adatvédelemhez való jog, a gondolat-, lelkiismereti és vallásszabadsághoz való jog, a véleménynyilvánítás szabadságához való jog, a gyülekezési szabadsághoz való jog, az egyenlő bánásmódhoz való jog, valamint a gazdasági és szociális jogok.

hogyan a gyakorlatban mi egy ilyen hatásvizsgálat metodológiája, összefoglaljuk, hogy melyek az államok releváns adatvédelmi, átláthatósági és elszámoltathatósági feladatai, valamint hogyan alakul a magánszektor felelőssége ezzel kapcsolatban.

Az államok adatvédelmi feladatai

Az algoritmikus rendszerek használata során végzett adatkezelések jogi megfelelőségét az Ajánlás kiemelt prioritásként kezeli. Az Ajánlásban meghatározott adatvédelmi kötelezettségek túlmutatnak a GDPR által meghatározott és 2018 óta a szervezetek napi folyamatainak részévé vált elszámoltathatósági kötelezettségeken, sőt, az Ajánlás legtöbbször nem tesz különbséget aközött, hogy az alapul fekvő adatkezelés során személyes vagy nem személyes adatok kezelésére kerül-e sor.

Az Ajánlás például kifejezetten nevesíti az algoritmikus rendszer kifejlesztéséhez és működtetéséhez szükséges adatkészletek minőségének értékelésével összefüggő kötelezettségeket, és javasolja, hogy az államok az értékelések alapján megfelelő intézkedéseket tegyenek az algoritmikus rendszerek esetleges káros hatásainak megelőzése és hatékony minimalizálása érdekében. Az adatkészlet összeállítása során minél szélesebb körben figyelembe kell venni az érintett személyek körének jellemzőit és reprezentációját (demográfiai csoport, politikai vélemény, társadalmi helyzet stb.), valamint az adatok felhasználásának tervezett kontextusát. Külön figyelmet kell fordítani arra, hogy az anonimizált vagy álnevesített adatok felhasználása során ne legyen lehetőség az érintett személyek újbóli azonosítására, és fenn kell tartani a jogi megfelelést, ha az adatkezelés során – akár csak következtetés útján – a felhasznált adatkészletek segítségével új adatkategóriák jönnek létre.

További fontos szempont az Ajánlásban, hogy az algoritmikus rendszerek tesztelését lehetőség szerint személyes adatok felhasználása nélkül kell elvégezni, kellően figyelembe véve a rendszer lakosságra és környezetükre gyakorolt külső hatásait, és azt is, hogy a tesztelési minták vagy a tesztelés „kimenetei” a rendszer eredeti fejlesztési céljától eltérő kontextusban is felhasználásra kerülhetnek – például más algoritmikus rendszerek fejlesztéséhez.⁶ A tesztelések során végzett adatkezeléseket már jelenleg is kiemelt figyelemmel kísérik az adatvédelmi hatóságok⁷ – az Ajánlás ezzel kapcsolatos megállapításai további részletes iránymutatást nyújthatnak a jogi megfeleléshez.

⁶ Ajánlás, B. cikk, 3.4 alpont (Az adatkészletek és a rendszer externáliáinak értékelése).

⁷ Lásd például az Európai Unió Bíróságának a C-77/21. sz. ügyben hozott ítéletét. Az alapügyben a Nemzeti Adatvédelmi és Információszabadság Hatóság 2020. május 18-i határozatában 100 000 000 forint bírságot szabott ki, mert a Digi Távközlési és Szolgáltató Kft. megsértette többek között a GDPR 5. (1) b) és e) pontját azzal, hogy egy tesztadatbázist a szükséges tesztek lefuttatása és a hiba kijavítása után nem törölt azonnal, és az abban rögzített nagyszámú személyes adatot a következő közel 18 hónapban cél nélkül tárolta.

Az adatkészletek és modellek forrásának és minőségének hitelesítése érdekében az államoknak regionális és nemzetközi szabványokon alapuló tanúsítási rendszereket kell kialakítaniuk. Az ilyen biztosítékoknak a beszerzési folyamatok részét is kell képezniük, és meg kell felelniük az algoritmikus rendszerek meghatározott felhasználási módjait tiltó szabályoknak⁸ – idetartozhatnak például az MI Rendelettervezetben kifejezetten felsorolt tiltott MI-gyakorlatok. Ez a szabványosítási kezdeményezés illik az MI-vel kapcsolatos nemzetközi szabályozási trendbe – 2022 elején a Nemzetközi Szabványügyi Szervezet (ISO) is ISO/IEC DIS 23894 néven új szabványt kezdett kidolgozni az MI-vel kapcsolatos kockázatok kezelésére vonatkozóan, ami a kockázatértékeléshez általános útmutatást nyújtó ISO 31000:2018 szabványra épül, elfogadása pedig jelenleg vizsgálati szakaszban van.

Az érintettek jogai és jogorvoslati lehetőségei közül az Ajánlás – szintén túlmutatva a GDPR-ban meghatározott szabályokon – kiemeli, hogy az érintetteknek könnyen elérhető és hatékony eszközöket kell biztosítani az algoritmikus rendszer által tett megállapítások és döntések elleni kifogások benyújtására. Az Ajánlás kiemeli azt is, hogy a kifogások kivizsgálását követően létrejövő eredmények nemcsak a konkrét esetekben kell hogy korrekciós intézkedésekhez vezessenek, hanem magukba a rendszerekbe is be kell ezeket építeni, a jogsértő eredmények megismétlődésének elkerülése érdekében. Mindezek előfeltétele, hogy az algoritmikus rendszerek használatát, folyamatát, logikáját, indokolását és lehetséges eredményét egyéni és kollektív szinten időben, elfogulatlanul, könnyen olvasható és hozzáférhető módon meg kell magyarázni az érintettek számára – ez várhatóan a jelenlegi adatkezelési tájékoztatókhoz hasonló módon fog történni. Lehetőséget kell biztosítani az érintett meghallgatására, a döntés megfelelő felülvizsgálatára, és biztosítani kell a nem automatizált döntés lehetőségét.⁹ Az érintettek információs önrendelkezési jogának korlátozásával kapcsolatban ugyanakkor figyelemre méltó, hogy az Ajánlás megemlíti: a demokratikus társadalmakban szükséges mértékben jogszabály korlátozhatja az érintettek információs önrendelkezési jogának a gyakorlását.¹⁰ Ez tulajdonképpen azt jelenti, hogy az érintettek nem biztos, hogy megkaphatják a (GDPR-ban is előírt) teljes körű tájékoztatást adataiknak az algoritmikus rendszer használata során történő kezeléséről, és az adatok helyesbítésével, törlésével kapcsolatos, valamint az automatizált döntéshozatal ellen való tiltakozási jogukat sem feltétlenül gyakorolhatják korlátozás nélkül.¹¹ Ezeknek a jogoknak a korlátja lehet például, ha a döntéshozatal során alkalmazott metodológia jogszabály vagy szerződés által védett bizalmas információ, vagy ha teljes körű feltárása veszélyeztetné a döntéshozatal céljának elérését.

⁸ Ajánlás, B. cikk, 3.2 alpont (A biztosítékok beépítése).

⁹ Ajánlás, B. cikk, 4.3 alpont (Kifogások benyújtása).

¹⁰ Ajánlás, B. cikk, 2.1 alpont (Információs önrendelkezés).

¹¹ Ajánlás, B. cikk, 2.2 alpont (Adatkészletek).

Végül az Ajánlás az adatvédelmi kérdések körében kiemeli az adatkezeléshez használt infrastruktúra-fejlesztések szükségességét. Ennek oka, hogy az Ajánlás szerint az adatok és az adatfeldolgozási kapacitások növekvő központosítása (beleértve a felhőalapú szolgáltatások használatát is) és az infrastruktúrával kapcsolatos választási lehetőség hiánya negatívan befolyásolhatja az emberi jogi kötelezettségeknek való megfelelést. Ezért az államoknak elő kell segíteniük az alternatív, biztonságos és védett infrastruktúrák fejlesztését annak biztosítása érdekében, hogy a magas színvonalú adatkezelési kapacitások továbbra is elérhetőek maradjanak a köz- és magánszereplők számára egyaránt.¹² A gyakorlatban ez azt jelenti, hogy az algoritmikus rendszerek használata során érdemes lehet mellőzni egy-egy típusú infrastruktúra kötelező használatának előírását, és mindenekelőtt biztosítani kell a kiberbiztonsági szempontból megfelelő (általában felhőalapú) szolgáltatások közötti választási lehetőséget. Az infrastruktúra fejlesztése során figyelembe kell venni a környezeti hatásokat is, és meg kell tenni a szükséges lépéseket a természeti erőforrások és az energia felhasználásának optimalizálása érdekében.¹³

Az államok átláthatósági és elszámoltathatósági feladatai

Az Ajánlás is kiemelt fontosságúként említi, hogy az államoknak megfelelő és arányos szintű átláthatóságot kell kialakítaniuk az általuk használt algoritmikus rendszerek fejlesztése és beszerzése során. Az államok által vagy az államok számára végzett emberi jogi hatásvizsgálatoknak nyilvánosan hozzáférhetőnek kell lenniük,¹⁴ és a szellemi tulajdonra vagy üzleti titokra vonatkozó jogi keretek nem akadályozhatják az átláthatóságot. A gyakorlatban emiatt meg kell találni az egyensúlyt, hogy az algoritmikus rendszerek működéséről szóló tájékoztatás során a fejlesztők bizalmas információit csak a szükséges mértékben tárják fel, de úgy, hogy ez még ne akadályozza az érintettek közérthető tájékoztatását a rendszer működéséről.

Az algoritmikus rendszereknek az emberi jogokat „nagymértékben veszélyeztető” döntéshozatali folyamatokban való alkalmazása során különösen magas követelményeket kell támasztani a folyamatok és a kimenetek megmagyarázhatósága tekintetében.¹⁵ Az államoknak biztosítaniuk kell, hogy minden olyan kiválasztási folyamat vagy algoritmikus rendszerek által hozott vagy támogatott döntés, amely „jelentős hatással” lehet az emberi jogok gyakorlására, a kezdeti interakció során egyértelműen és hozzáférhető módon azonosítható és nyomon követhető legyen.¹⁶ Az Ajánlás által használt terminológia alapján a szükséges intézkedésekkel

¹² Ajánlás, B. cikk, 2.3 alpont (Infrastruktúra).

¹³ Ajánlás – Előszó.

¹⁴ Ajánlás, B. cikk, 5.3 alpont (Szakértelem és felügyelet).

¹⁵ Ajánlás, B. cikk, 4.1 alpont (Az átláthatóság szintjei).

¹⁶ Ajánlás, B. cikk, 4.2 alpont (Az algoritmikus döntéshozatal azonosíthatósága).

összefüggő követelmények meghatározásakor figyelembe kell venni az algoritmikus rendszer hatásait és veszélyeit – a „nagyértékben veszélyeztető” és a „jelentős hatás” feltételeit ugyanakkor az Ajánlás nem definiálja, szemben az MI Rendelettervezettel, amely kifejezetten felsorolja a „magas kockázatú” MI-rendszereket. Az Ajánlás így nagyobb döntési szabadságot ad az abban meghatározott szempontokat alkalmazó államoknak az adott algoritmikus rendszer besorolása tekintetében, viszont a kapcsolódó emberi jogi hatásvizsgálat már magához a besoroláshoz és az egyes kockázatok és veszélyek azonosításához is elengedhetetlen.

Az államoknak azt is biztosítaniuk kell, hogy megfelelő forrásokkal rendelkező független intézmények megfelelően felügyeljék az érintett egyének vagy csoportok által az egyes algoritmikus rendszerek ellen benyújtott kifogásokat, és hogy független szakértő ellenőrizzen minden magas kockázatú algoritmikus rendszerekkel kapcsolatos emberi jogi hatásvizsgálatot. A jelentős emberi jogi hatásokkal járó algoritmikus rendszerek beszerzésében, fejlesztésében, üzemeltetésében és értékelésében részt vevő valamennyi érintett munkatárs megfelelő képzésben kell hogy részesüljön, és tisztában kell lenniük azzal, hogy feladatuk nemcsak technikai vizsgálat, hanem az alapjogok betartásának biztosítása is.¹⁷ A független intézmények és szakértők alkalmazása, valamint az érintett személyzet képzése jelentősebb anyagi és emberi erőforrás előteremtését igényli majd az államok részéről, az így rendelkezésre álló szakértelem azonban a jövőben megkerülhetetlen lesz az algoritmikus rendszerek jogi megfelelőségének biztosítása érdekében. Ezen túlmenően az államoknak részt kell venniük a témával összefüggő nyilvános vitákban, és ennek során meg kell vitatni, hogy a közszolgáltatások mely területeit nem lehet algoritmikus rendszerekkel meghatározni, eldönteni vagy optimalizálni.¹⁸ Egy ilyen „tiltólista” létrehozatala ismét csak az EU MI Rendelettervezetében kifejezetten felsorolt tiltott MI-gyakorlatokhoz hasonlít – azzal, hogy az államoknak ebben a tekintetben az Ajánlás nagyobb szabadságot biztosít.

*Az államok által végzett kockázatfelmérések és emberi jogi hatásvizsgálatok
gyakorlati kérdései*

Az emberi jogi hatásvizsgálatok tekintetében az Ajánlás általános jelleggel rögzíti az államok kötelezettségét, hogy az algoritmikus rendszerek beszerzése előtt, a fejlesztésük során, a rendszeres mérőföldköveknél és a kontextusspecifikus alkalmazásuk során rendszeresen és konzultatív módon emberi jogi hatásvizsgálatokat végezzenek. Az Ajánlás szerint az emberi jogi hatásvizsgálatokat kötelezővé kell tenni minden olyan algoritmikus rendszer esetében, amely „magas kockázatot” jelent az emberi

¹⁷ Ajánlás, B. cikk, 5.5 alpont (Személyzeti irányítás).

¹⁸ Ajánlás, B. cikk, 5.7 alpont (Nyilvános vita).

jogokra nézve.¹⁹ Az emberi jogokat nagymértékben veszélyeztető algoritmikus rendszerek esetében a hatásvizsgálatoknak tartalmazniuk kell a rendszerek által a meglévő társadalmi, intézményi vagy kormányzási struktúrákra gyakorolt lehetséges hatások értékelését, és egyértelmű ajánlásokat kell tartalmazniuk az alapjogokat érintő nagymértékű kockázatok megelőzésére vagy mérséklésére.²⁰

Az előző pontokban már említettük, hogy az EU MI Rendelettervezete hasonló kontextusban használja a „magas kockázatú MI” fogalmát. Az Ajánlás szerint „magas kockázatú” egy algoritmikus rendszer, amikor azt olyan eljárásokban vagy döntésekben használják, amelyek súlyos következményekkel járhatnak az egyénekre nézve, vagy olyan helyzetekben, ahol az alternatívák hiánya az emberi jogok megsértésének különösen nagy valószínűségét eredményezi, többek között az elosztási igazságtalanság bevezetésével vagy felerősítésével. Míg az EU MI Rendelettervezete a mellékletében kifejezetten felsorolja a „magas kockázatú” MI-rendszereket, az Ajánlás csak példákat említ: egy algoritmikus rendszer alkalmazása különösen magas kockázatot jelenthet az emberi jogokra nézve, ha azt az államok a közszolgáltatás vagy a közpolitika megvalósítása érdekében használják, és az egyénnek nincs lehetősége arra, hogy lemondjon róla, vagy a lemondásra vonatkozó döntés negatív következményeket von maga után. Hasonlóan magas kockázatot jelent az Ajánlás szerint az algoritmikus rendszerek hatóságok vagy magánszemélyek által a döntéshozatali folyamatok keretében történő használata különös súllyal vagy jogi következménnyel bíró helyzetekben – például az algoritmikus rendszereknek az igazságszolgáltatás területén jogi elemzés, előrejelzés vagy egyéni kockázatértékelés céljából történő alkalmazása.²¹ Az Ajánlás szerint a „magas kockázatú” algoritmikus rendszereket nagy körültekintéssel és az Emberi jogok európai egyezményének 6. cikkében foglalt tisztességes eljárás garanciáival összhangban kell bevezetni.²²

Az Ajánlás az úgynevezett „jelentős emberi jogi hatásokkal járó számítási tesztek” (*computational experimentation*) esetén rögzíti, hogy az államok csak emberi jogi hatásvizsgálat lefolytatását követően végezhetik el azokat, és a pozitív kimenetelű hatásvizsgálatot követően még előzetesen ki kell kérni a résztvevők szabad, konkrét, tájékozott és egyértelmű hozzájárulását, továbbá biztosítani kell a hozzájárulás visszavonásának lehetőségét. Az Ajánlás emellett előírja az államok számára, hogy tiltsák meg a megtevesztő vagy az érintetteket kihasználó hatású kísérleteket.²³ Az EU MI Rendelettervezete is ezt a megközelítést követi, az Ajánlás ugyanakkor nem definiálja jobban, mit tekint „jelentős emberi jogi hatásokkal járó számítási tesztnek” – pozitív, hogy a kérdés eldöntését az Ajánlás az államok szabad, kockázatalapú döntésére bízza, de a gyakorlatban ez értelmezési

¹⁹ Ajánlás, B. cikk, 5.1 alpont (Szabványok).

²⁰ Ajánlás, B. cikk, 5.2 alpont (Emberi jogi hatásvizsgálatok).

²¹ Ajánlás, A. cikk (Hatály és kontextus), 11. pont.

²² Ajánlás, B. cikk, 3.6 alpont (Alternatív és párhuzamos megközelítések).

²³ Ajánlás, B. cikk, 3.1 alpont (Számítógépes kísérletezés).

nehézségekhez is vezethet. További kihívásokat okozhat, hogy kizárólag a számítási tesztek azok, ahol az Ajánlás az érintettek előzetes hozzájárulásának beszerzését írja elő – ebben a tekintetben úgy tűnik, az Ajánlás az algoritmikus rendszerek használatához a GDPR-hoz hasonlóan jogalapot próbál előírni, de nehezítheti ennek mindennapi alkalmazását, ha az Ajánlás csak a hozzájárulást említi jogalapként, és kizárólag egy típusú algoritmikus rendszer esetében – a GDPR ebben a tekintetben rugalmasabb, és ezt a rendszert érdemes lehet alkalmazni algoritmikus rendszerek esetén, függetlenül attól, hogy személyes adatok kezelésére kerül-e sor.

Az emberi jogi hatásvizsgálatok metodológiája hasonló a GDPR 35. cikkében meghatározott adatvédelmi hatásvizsgálatok metodológiájához. Az érdekelteknek dokumentálniuk kell az algoritmikus rendszer alkalmazásának kontextusát, jogalapját, célját, pontosságát, hatásait és mértékét, valamint annak a kockázatát is, hogy ezeket a rendszereket rosszindulatú felek támadhatják vagy megzavarhatják. Az algoritmikus rendszerek lehetséges emberi jogi hatásai mértékének értékelése során figyelembe kell venni a rendszer által kezelt adatok mennyiségét, jellegét és értékét, továbbá a rendszer tervezett használatára során az alapjogok megsértésének valószínűségét, és lehetséges súlyosságát is.²⁴

Az Ajánlás az államok által végzett kockázatfelmérések körében kifejezetten megemlíti azt is, hogy a közszolgáltatások nyújtásában és más „magas kockázatú” tevékenységek során az algoritmikus rendszer teljesítményét és kimenetét más lehetőségekkel összehasonlítva kell értékelni. Ez a megközelítés nagyban segíti az átláthatóságot, jogilag pedig hasonló a GDPR alapján elvégzendő „érdekmérlegelési tesztekhez”, ahol mérlegelni kell, hogy egy-egy adatkezelés esetén rendelkezésre állnak-e alternatív, az érintett szempontjából kevésbé korlátozó megoldások, amelyekkel az adatkezelői érdek elérhető, illetve rendelkezésre állnak-e megoldások, amelyekkel személyes adatok kezelése nélkül, kevesebb személyes adat kezelésével, vagy személyes adatok egyéb módon történő kezelésével érhető el az adott cél.

Az emberi jogi hatásvizsgálatok lefolytatása azonban nemcsak az alapjogok védelme szempontjából fontos – a megfelelően dokumentált hatásvizsgálat segít meghatározni az algoritmikus rendszer működtetésében részt vevő felek felelősségi körét is. Ez különösen akkor lehet lényeges, ha a rendszer működtetésében állami és magánszektorbéli szervezetek egyaránt részt vesznek – például, ha egy állami szerv az általa végzett közszolgáltatást részben vagy egészben kiszervezi egy vagy több szolgáltatónak. Ha a magánszektor szereplői algoritmikus rendszereken alapuló, az emberi jogok hatékony gyakorlásához nélkülözhetetlennek minősülő szolgáltatásokat nyújtanak, az Ajánlás kiemeli, hogy az államoknak meg kell őrizniük az alternatív megoldások jövőbeli életképességét, és biztosítaniuk kell az érintett egyének és csoportok számára az ilyen szolgáltatásokhoz való folyamatos hozzáférést. Az Ajánlás külön elővigyázatosságot javasol arra az esetre, ha több algoritmikus rendszer működik ugyanabban a környezetben, és a rendszerek működése esetleg

²⁴ Ajánlás, A. cikk (Hatály és kontextus), 9. pont.

kölcsönösen függ egymástól. A közszolgáltatások nyújtása során az államoknak ki kell használniuk a magánszolgáltatások beszerzésének vagy igénybevételének mechanizmusát, de az algoritmikus rendszerek használata és egymással való kölcsönhatásuk tekintetében fenn kell tartani a felügyeletet, a know-how-t, a tulajdonjogot és az ellenőrzést.²⁵ Tekintettel arra, hogy az algoritmikus rendszerek fejlesztése a magánszektor oldalán is komoly befektetést igényel, az Ajánlás fenti rendelkezésének betartása során kiemelt figyelemmel kell lenni az érintett magánszolgáltató jogaira is – észszerű elvárás lehet például, hogy az általa biztosított know-how és tulajdonjog védelmét szerződéses rendelkezésekkel erősítsék meg.

Az algoritmikus rendszerekkel összefüggő alapjogok – a magánszektor felelőssége

Míg az államok számára az Ajánlás az algoritmikus rendszerekkel összefüggésben már a vonatkozó alcímben is kifejezetten előírja az emberi jogok és alapvető szabadságok védelmét és előmozdítását, a magánszektor számára inkább felelősségi köröket határoz meg.

Felelősségük részeként a magánszektor szereplőinek folyamatos, proaktív és reaktív, dokumentált lépéseket kell tenniük annak biztosítására, hogy innovatív tevékenységeik során ne okozzanak emberi jogi visszaéléseket, illetve ne járuljanak hozzá azokhoz.²⁶ Az algoritmikus rendszerek tervezése, fejlesztése, tesztelése és alkalmazásuk értékelése érdekében belső folyamatokat kell kidolgozni, és dokumentálni az esetleges technikai hibákat, valamint a rendszerek által esetlegesen okozott jogi, társadalmi és etikai hatásokat. Az emberi jogi hatásvizsgálatokban és az algoritmikus rendszerek nyomon követésében részt vevő valamennyi érintett munkatárs számára képzést kell biztosítani, hogy megfelelően megismerjék az alapjogokkal kapcsolatos felelősségi köröket, ideértve többek között a személyes adatok védelmére és a magánélet védelmére vonatkozó előírásokat.²⁷ A fentieknek való megfeleléshez a gyakorlatban megfelelő belső eljárásokat kell kialakítani – a GDPR-nak való megfeleléshez szükséges eljárásrendek kialakítását követően azonban ez vélhetően már nem lesz újdonság az érintett szervezetek számára.

A magánszektor szereplői felelősségének mértéke független a méretüktől, ágazatuktól, működési környezetüktől, tulajdonosi struktúrájuktól vagy tevékenységük jellegétől, de a felelősségi kérdések meghatározásához szükséges eszközök jellege és összetettsége az általuk biztosított algoritmikus rendszer által az emberi jogokra gyakorolt potenciális hatás mértékétől függően változhat.²⁸ Az Ajánlás szerint

²⁵ Ajánlás, B. cikk, 5.6 alpont (A rendszerek kölcsönhatása).

²⁶ Ajánlás, C.1 cikk (Általános alkalmazási elvek), 1.1 alpont (Az emberi jogok tiszteletben tartásának felelőssége).

²⁷ Ajánlás, C.5 cikk (Óvintézkedések), 5.2 alpont (A személyzet képzése).

²⁸ Ajánlás, C.1 cikk (Általános alkalmazási elvek), 1.2 alpont (Az intézkedések skálája).

a magánszektor szereplőinek is be kell tartaniuk az állami szereplők számára az algoritmikus rendszerek folyamatos felülvizsgálatára, a demokratikus részvételre és tudatosságra, az információs önrendelkezésre, a számítási kísérletekre, a tesztelésre és az algoritmikus döntéshozatal azonosíthatóságára meghatározott előírásokat. Ennek oka, hogy ha az algoritmikus rendszerek tervezése, fejlesztése és folyamatos telepítése a magánszektor és az állami szektor szereplői között szoros együttműködésben történik, akkor az alapjogi hatás „horizontálissá” válik.²⁹ Emiatt fontos lesz tehát az információcsere az állami szereplők és a magánszektor szereplői között, hogy a magánszolgáltatók fejlesztéseik elvégzése során tisztában legyenek az állami szereplők számára irányadó szabályokkal, és a két szektorra irányadó előírások „interoperábilisek” legyenek egymással.

A magánszektor szereplőinek szintén biztosítaniuk kell – a korábban bemutatott átláthatósági követelményekhez hasonlóan – az algoritmikus rendszereik jellegével és működésével, valamint az általuk kezelt adatokkal kapcsolatos tájékoztatást. Idetartozik különösen, hogy milyen valós és potenciális hatása van a szóban forgó rendszernek, melyek a rendszer használatának várható eredményei, melyek az alkalmazandó panaszeljárások és határidők, hogyan tiltakozhatnak az érintettek adataik kezelése ellen, valamint hogyan vitathatják az egyes kimeneteket. Az algoritmikus rendszerek működésével kapcsolatos tájékoztatóknak tartalmazniuk kell továbbá a rendszer jellemzőinek módosítására rendelkezésre álló lehetőségeket. Ezek az előírások ismét csak meghaladják a GDPR hasonló előírásait. Az Ajánlás értelmében az érintetteket felhasználóbarát formában értesíteni kell a rendszer használati feltételeinek változásairól, és adott esetben kérni kell hozzájárulásukat a változáshoz. Ez a megközelítés nagyjában hasonlít az általános szerződési feltételek módosításával kapcsolatos fogyasztóvédelmi előírásokhoz. Az Ajánlás sajnos nem tartalmaz további részleteket azzal kapcsolatban, hogy mik lehetnek a vonatkozó esetek, annyit azonban rögzít, hogy a hozzájárulás elmaradása nem vezethet az alapvető szolgáltatások elérhetetlenné válásához.³⁰

Az adatkezelés jogalapjaként a magánszektor számára meghatározott iránymutatások körében az Ajánlás kizárólag az érintettek hozzájárulását említi.³¹ Az előző pontban említettekhez hasonlóan itt sem teljesen egyértelmű, hogy az Ajánlás más, a GDPR által lehetővé tett adatkezelési jogalapot is elismer-e az algoritmikus rendszerek használata vonatkozásában, mert a hozzájárulást jogalként a nyomkövetési, tárolási és teljesítménymérő eszközök használata során alkalmazott algoritmikus rendszerek esetében is kiemeli. Ezzel összefüggésben az Ajánlás az algoritmikus rendszerek beállításai kapcsán azt is rögzíti, hogy a nyomkövetési beállításokat alapértelmezettként opt-out módban kell beállítani – ennek alapján

²⁹ Ajánlás, C.1 cikk (Általános alkalmazási elvek), 1.3 alpont (További kulcsfontosságú szabványok).

³⁰ Ajánlás, C.4 cikk (Átláthatóság, elszámoltathatóság és hatékony jogorvoslatok), 4.1 alpont (Szolgáltatási feltételek).

³¹ Ajánlás, C.2 cikk (Adatkezelés), 2.1 alpont (Hozzájárulási szabályok).

lehet következtetni arra, hogy bizonyos beállítások viszont működhetnek a felhasználó hozzájárulása nélkül is, például az algoritmikus rendszert használó szervezet jogos érdeke alapján. Gyakorlati szempontból ugyanakkor túlmutat a GDPR rendelkezésein az Ajánlás azon rendelkezése, miszerint ha a felhasználói adatok kezelésének korlátozása, az adatok törlése vagy (például adatbiztonsági célból történő) karanténba helyezése esetén az adatokat hibásan vagy aránytalanul használják fel, megfelelő eljárási garanciákat és gyors jogorvoslati lehetőségeket kell biztosítani az érintettek számára.³²

Az Ajánlás értelmében az algoritmikus rendszereken végzett elemzés és modellezés során a magánszektor szereplőinek is tisztában kell lenniük a felhasznált adatok minőségével, jellegével és eredetével összefüggő kockázatokkal, annak biztosítása érdekében, hogy az adatkészletek és modellek hibáit, torzításait és esetleges diszkriminációját az adott kontextusban megfelelően kezeljék.³³ Ez hasonlít az államok adatvédelmi feladatai körében tárgyalt, az adatkészletek minőségéhez kapcsolódó felelősségéhez. Az algoritmikus rendszereknek az egyének személyes adatain történő értékelését és tesztelését kellően sokszínű és reprezentatív mintapopulációkkal kell végezni. Ez azt jelenti, hogy tilos például egyetlen demográfiai csoportot alapul venni vagy megkülönböztetni, és le kell állítani, illetve ki kell javítani az adott algoritmikus rendszert, ha fejlesztése, tesztelése vagy alkalmazása egyénekre, csoportokra és környezetükre kockázatokat vagy költségeket telepít.³⁴ Kérdés azonban, hogy indokolt-e az Ajánlásnak ez a szigorú előírása – azaz lehetséges-e a gyakorlatban olyan algoritmikus rendszert fejleszteni, amelynek a működése során semmilyen kockázat vagy költség nem keletkezik az érintett személyek oldalán; vagy megengedhető-e az ilyen kockázat vagy költség, ha az algoritmikus rendszer használatával kapcsolatos lehetséges előnyök összességében kiegyensúlyozzák ezeket a hátrányokat. Az Ajánlás említ is egy olyan esetet példaként, amikor az algoritmikus rendszerek bizonyos értékeket másokkal szemben előnyben részesíthetnek, például az általános nyereséget az egyedi veszteségekkel szemben; azzal, hogy erre csak egyértelmű, átlátható, elszámoltatható és az érintettek által ellenőrizhető módon kerülhet sor, és nem járhat kedvezőtlen hatásokkal, különösen a kisebbségek és a marginalizált vagy hátrányos helyzetű csoportok számára.³⁵

Az Ajánlás alapján a magánszektor szereplőinek azt is biztosítani kell, hogy az érintettek ne csak vitathassák a kimeneteket, hanem javítási javaslatokat teheszenek, és egyéb hasznos visszajelzéseket adhassanak.³⁶ Ezen túlmenően, a magánszektor szereplőinek nyilvánosságra kell hozniuk az érintettek által benyújtott

³² Ajánlás, C.2 cikk (Adatkezelés), 2.2 alpont (Adatvédelmi beállítások).

³³ Ajánlás, C.2 cikk (Elemzés és modellezés), 3.1 alpont (Az adatok és a modell minősége).

³⁴ Ajánlás, C.2 cikk (Elemzés és modellezés), 3.1 alpont (Mintapopulációk).

³⁵ Ajánlás, A. cikk (Hatály és kontextus), 7. pont.

³⁶ Ajánlás, C.4 cikk (Átláthatóság, elszámoltathatóság és hatékony jogorvoslatok), 4.2 alpont (Kifogások benyújtása).

panaszok számáról és típusáról, valamint a panaszok eredményéről szóló információkat.³⁷ Ennek célja az Ajánlás szerint az, hogy az eredmények ne csak konkrét esetekben vezessenek korrekciós intézkedésekhez, hanem magukba a rendszerekbe is beépüljenek. Az Ajánlás általánosságban nagy hangsúlyt helyez a megfelelő panaszmechanizmusok és hatékony jogorvoslatok kiépítésére, de a gyakorlatban kérdéses, hogy a korrekciós intézkedések beépítéséhez miért szükséges az alapul fekvő információk nyilvánosságra hozatala. Egy-egy algoritmikus rendszer hibás működésével kapcsolatos információ adott esetben a fejlesztő, illetve az üzemeltető üzleti titka, amelynek felfedése negatív hatással lehet a szervezet piaci hírnevére, a hibás működés korrekciója ugyanakkor – indokolt esetben, ha az érintetteket nem éri hátrány – elvégezhető lehet a nyilvánosság bevonása nélkül is.

A magánszektor szereplői az emberi jogi hatásvizsgálatokat a lehető legnyíltabban és az érintett egyének és csoportok aktív bevonásával kell hogy végezzék. Az Ajánlás szerint a magas kockázatú algoritmikus rendszerek telepítése esetén a folyamatban lévő emberi jogi hatásvizsgálatok eredményeit, a kockázatsökkentés meghatározott technikáit, valamint a vonatkozó nyomonkövetési és felülvizsgálati eljárásokat nyilvánosan hozzáférhetővé kell tenni, a jogszabályok által biztosított titokvédelmi előírások sérelme nélkül.³⁸ Az algoritmikus rendszerek fejlesztőinek üzleti titkai tehát védettek, de az illetékes hatóságok számára hozzáférhetőek kell hogy legyenek. Ha az algoritmikus rendszerek alkalmazása az emberi jogok szempontjából magas kockázatú, például mikrocélzási folyamatok esetén, a magánszektor szereplőinek lehetőséget kell biztosítani arra, hogy az érintett felügyeleti hatóságokkal konzultáljanak a kockázatok kezelésére (például a kapcsolódó szolgáltatások újratervezésére) vonatkozóan. A fenti konzultációs kötelezettségek szintén hasonlóak a már említett adatvédelmi hatásvizsgálatok esetén irányadó eljáráshoz – állami oldalról szükséges azonban ehhez az érintett felügyeleti hatóságok kijelölése és működési feltételeik biztosítása. Mindemellett a magánszektor szereplőinek az algoritmikus rendszereket rendszeres független szakértői felülvizsgálat és felügyelet alá kell vetniük³⁹ – ehhez az érintett személyekkel való rendszeres konzultáció, folyamatos minőségbiztosítási ellenőrzés és valós idejű auditálás szükséges. Mindezek során a korábban már említett regionális és nemzetközi szabványok segíthetnek.

Végezetül érdemes megemlíteni az Ajánlás által a magánszektor szereplői számára javasolt kutatási feladatokat. Az algoritmikus rendszerek telepítésével járó lehetséges kockázatok vizsgálatával kapcsolatban az Ajánlás alapvetően két kutatási területet határoz meg: az algoritmikus rendszerek hatásának értékelésére szolgáló mechanizmusok kidolgozása, valamint a hátrányos helyzetű és alulreprezentált népességcsoportok igényeinek kielégítését célzó algoritmikus rendszerek fejlesztése.

³⁷ Ajánlás, C.4 cikk (Átláthatóság, elszámoltathatóság és hatékony jogorvoslatok), 4.3 alpont (Átláthatóság).

³⁸ Ajánlás, C.5 cikk (Óvintézkedések), 5.3 alpont (Emberi jogi hatásvizsgálatok).

³⁹ Ajánlás, C.5 cikk (Óvintézkedések), 5.1 alpont (Folyamatos értékelés).

A magánszektor szereplőinek finanszírozniuk kell és közzé kell tenniük az algoritmikus rendszerekben rejlő, az emberi jogokra gyakorolt pozitív hatás és a közös előmozdítására irányuló potenciál értékelése, tesztelése és fejlesztése céljából végzett független kutatásokat.⁴⁰ A kezdeményezés pozitív, de kérdés, hogy mennyire indokolt az érintett szervezetektől elvárni, hogy a jelentős anyagi és emberi erőforrás ráfordításával készített kutatásokat megosszák a nyilvánossággal – és így versenytársaikkal. Az Ajánlás azt is javasolja, hogy a magánszektor szereplői a megfelelő felek – független kutatók, a média és a civil társadalmi szervezetek – számára biztosítsanak hozzáférést a számukra releváns, egyénekre vonatkozó adatokhoz és metaadat-adatbázisokhoz, beleértve a törlendő adatokhoz való hozzáférést is.⁴¹ A nehézség itt is hasonló a kutatásokhoz való hozzáférésnél említett kérdéshez – az adatbázisok összeállítása jelentős ráfordítást igényelhet az érintett szervezet oldalán, ezért azt nem biztos, hogy kész megosztani más felekkel, még a szükséges adatvédelmi és titoktartási rendelkezések betartása mellett sem.

A „SyRI-ügy” tanulságai

Amint az a fentiekből kiderült, az Ajánlásban foglaltak gyakorlati megvalósítása több kérdést is felvet, és az elkövetkező években dől majd el, hogy ezeket hogyan tudják kezelni az államok és a magánszektor szereplői, valamint milyen hatással lesznek az Ajánlás rendelkezései az MI-rendszerek fejlesztésére. Az ilyen rendszerekkel kapcsolatos joggyakorlat egyelőre még nem kiforrott, érdemes viszont röviden megemlíteni a Systeem Risico Indicatie („rendszerkockázat jelzése” – SyRI) elnevezésű holland megoldást, mert több tanulsággal is szolgál arra vonatkozóan, hogy egy hasonló rendszer fejlesztése és üzemeltetése során milyen alapjogi kihívások merülhetnek fel.

A SyRI-t a jóléti állam hatékonyságának növelése és ezzel egyidejűleg a juttatásokkal való visszaélések (például az adó- és társadalombiztosítási csalások, valamint az illegális munkavégzés) számának csökkentése céljából fejlesztették ki. 2020-ban azonban a Hágai Kerületi Bíróság ECLI: NL: RBDHA:2020:1878 (SyRI) számú döntésében⁴² kimondta, hogy a SyRI alkalmazása sérti az Emberi jogok európai egyezményében is biztosított magánélethez való jogot.⁴³

⁴⁰ Ajánlás, C.6 cikk (Kutatás, innováció és tudatosság), 6.1 alpont (Kutatás).

⁴¹ Ajánlás, C.6 cikk (Kutatás, innováció és tudatosság), 6.2 alpont (Hozzáférés az adatokhoz).

⁴² A Hágai Kerületi Bíróság ECLI:NL:RBDHA:2020:1878 (SyRI) számú döntése a SyRI-vel kapcsolatban: Netherlands Juristen Comité Voor De Mensenrechten et al. v. The State of the Netherlands, no. C-09-550982-HA ZA 18-388, 2020. február 5-i ítélet.

⁴³ Eszerint: 1. Mindenkinek joga van arra, hogy magán- és családi életét, lakását és levelezését tiszteljenben tartsák. 2. E jog gyakorlásába hatóság csak a törvényben meghatározott, olyan esetekben avatkozhat be, amikor az egy demokratikus társadalomban a nemzetbiztonság, a közbiztonság vagy

A SyRI története és háttere

A SyRI elődje, az LSI (Landelijke Stuurgroep Interventieteams – „Nemzeti Beavatkozási Csoport”) 2003 óta lehetővé tette az adatcserét egyes holland hivatalos szervek (önkormányzatok, a társadalombiztosítás szervei, az adóhatóság, a Szociális és Foglalkoztatási Minisztérium, a rendőrség és az ügyészség) között, a munkajogi és társadalombiztosítási jogszabályok hatékonyabb érvényesítése, valamint a jóléti juttatásokkal való visszaélések számának csökkentése céljából. A SyRI-t az LSI helyett hozták létre 2013-ban – a kapcsolódó jogszabály-módosítás alapján a korábbinál több más állami szerv kapott hozzáférést a rendszerhez. Ezt a lehetőséget a holland adatvédelmi hatóság (College Bescherming Persoonsgegevens) már akkor is bírálta⁴⁴ – a hatóság szerint a SyRI segítségével kezelt személyes adatok körét túl tágan határozták meg (vagyis nem felelt meg az adattakarékosság követelményének), a működése során használt kockázati modell nem volt kellően átlátható, és a rendszer nem tartalmazott megfelelő védelmet a személyes adatok különleges kategóriáinak kezelése során. Mindezek ellenére a SyRI használatát engedélyező törvényt (Wet SUWI),⁴⁵ illetve annak módosítását a holland parlament jelentősebb vita nélkül elfogadta.⁴⁶

Maga a jogszabály például a rendszer viszonylag hosszú fennállása ellenére nem definiálta konkrétan a SyRI-t, arról csupán a törvény indokolásából kaphatunk képet:

„A SyRI magában foglalja azt a technikai infrastruktúrát és a hozzá kapcsolódó eljárásokat, amelyek révén az alapul fekvő adatok összekapcsolhatók, majd biztonságos környezetben, anonim módon elemezhetők, kockázatbejelentések generálása érdekében. A kockázatbejelentés azt jelenti, hogy egy jogi vagy természetes személy esetében fennáll egy esetleges csalás, jogellenes felhasználás vagy a jogszabályok megszegésének veszélye, ami miatt vizsgálatot szükséges ellene folytatni. Ez a módszer az ellenőrzés eszköztárának hatékonyabb és eredményesebb felhasználásához vezet.”⁴⁷

az ország gazdasági jóléte érdekében, zavargás vagy bűncselekmény megelőzése, a közegészség vagy az erkölcsök védelme, avagy mások jogainak és szabadságainak védelme érdekében szükséges.

⁴⁴ Holland adatvédelmi hatóság (College Bescherming Persoonsgegevens) – nyilvános kritika a SyRI-vel kapcsolatban: Advies Raad van State inzake het ontwerpbesluit houdende regels voor fraudeaanpak door gegevensuitwisselingen en het effectief gebruik van binnen de overheid bekend zijnde gegevens (Besluit SyRI). *Zoeken in officiële bekendmakingen* – *Overheid.nl*, 2014. szeptember 22.

⁴⁵ A SyRI használatát korábban engedélyező törvény (Wet SUWI): Wet structuur uitvoeringsorganisatie werk en inkomen. *Zoeken in officiële bekendmakingen* – *Overheid.nl*, 2022. január 1.

⁴⁶ A SyRI-vel kapcsolatos parlamenti vita publikált anyaga: Wijziging van de Wet structuur uitvoeringsorganisatie werk en inkomen en enige andere wetten in verband met fraudeaanpak door gegevensuitwisselingen en het effectief gebruik van binnen de overheid bekend zijnde gegevens. No 33 579. *Zoeken in officiële bekendmakingen* – *Overheid.nl*, 2013. június 25.

⁴⁷ Marvin van Bekkum – Frederik Zuiderveen Borgesius: Digital Welfare Fraud Detection and the Dutch SyRI Judgment. *European Journal of Social Security*, 23. (2021), 4. 324. (A szerző fordítása.)

A fentiek alapján a SyRI nem egy önmagában álló MI-rendszer, hanem komplex szociális infrastruktúra volt, amelynek részét képezte az alapul fekvő technológia és az arra épülő eljárások, amelyek során a kockázatokkal kapcsolatos jelzések eljutnak az illetékes hatóságokhoz. Az esetleges visszaélések azonosítására használt kockázati modellt a részt vevő hatóságok és közigazgatási szervek a minisztériummal együttműködve határozták meg. A közigazgatási szervek a birtokukban található adatokat továbbították az Inlichtingenbureau nevű szervezet részére, amely a kapott adatok alapján, a kialakított kockázati modell segítségével azonosította a gyanús tevékenységeket.⁴⁸ A SyRI tehát a különböző hatóságok által egyébként jogszerrően gyűjtött és tárolt személyes adatok összekapcsolását tette lehetővé, és ennek alapján az eredeti adatkezelési céloktól eltérő módon segített levonni következtetéseket az érintettekre vonatkozóan. Például: a vízművek által szolgáltatott vízfogyasztási adatokból következtettek arra, hogy az érintett ténylegesen egyedül lakik-e, vagy sem, és ez alapján mekkora szociális támogatásra jogosult.

Sajnos nem áll rendelkezésre további információ azzal kapcsolatban, hogy a SyRI a gyakorlatban hogyan működött – a kormány még az illetékes bíróság számára sem bocsátott rendelkezésre pontos információt a működési modellel kapcsolatban, attól félve, hogy az esetleg nyilvánosságra kerülő információkat a SyRI kijátszására fogják használni.

A bírósági szakasz

A holland állam ellen egy civil szervezetekből álló csoport indított pert a SyRI alkalmazása kapcsán. A felperesek kérték a Hágai Kerületi Bíróságot, hogy állapítsa meg a SyRI működését lehetővé tevő jogszabály egyes rendelkezéseinek összeegyeztethetlenségét az Emberi jogok európai egyezményének 8. cikkében, valamint más emberi jogi tárgyú nemzetközi egyezményekben biztosított magánélethez való joggal. A fenti hat szervezethez csatlakozott két ismert holland író is – „*Bij Voorbaat Verdacht*” („Előre gyanúsítva”) kampányuk indította el a SyRI-ről való közéleti vitát. Az ENSZ rendkívüli szegénységgel és emberi jogokkal foglalkozó különleges előadója, Philip Alston egy *amicus curiae* levéllel⁴⁹ csatlakozott, amelyben az emberi jogok és a digitális jóléti államok viszonyát tárgyalta a SyRI vonatkozásában is. Alston egyrészt kifejtette, hogy a SyRI-ügy azért jelentős, mert ez az első alkalom, amikor egy felperes emberi jogi alapokon vitatta egy digitális technológia

⁴⁸ Magyarul: „Információs Iroda”. Magánalapítvány formájában működött, mivel szükséges volt egy független szervezet ahhoz, hogy az önkormányzatok és más holland közigazgatási szervek közötti „független elektronikus kapcsolódási pont” legyen.

⁴⁹ Brief by the United Nations Special Rapporteur on Extreme Poverty and Human Rights as Amicus Curiae in the Case of NJCM c.s./De Staat der Nederlanden (SyRI) before the District Court of The Hague (case number: C/09/550982/ HA ZA 18/388). 2019. szeptember 26.

rendszerszintű, kifejezetten a jóléti juttatásokkal való visszaélések észlelésére szolgáló, nagy mennyiségű adat felhasználásával történő használatának jogszerűségét. Másrészt, a SyRI használata során felmerült a diszkrimináció magas kockázata, mivel azt elsősorban és nagyobb arányban a szegény és sérülékeny csoportok tagjaival kapcsolatosan alkalmazták. Végül, de nem utolsósorban pedig figyelemre méltónak tartotta, hogy a felperes civil szervezetek mennyire változatos csoportokat képviselnek, ami alátámasztja a SyRI-vel kapcsolatos társadalmi aggályokat.

Az *amicus curiae* levél szerint a SyRI nem volt hatékony⁵⁰ – az egyes projektek keretében több tízezer személy személyes adatainak elemzése alapján néhány száz „kockázatos” egyént találtak, akik közül mindössze negyvenen valósítottak meg ténylegesen jogsértést, a rendelkezésre álló adatokból pedig az érintett személyek életéről olyan részletes képet lehet kapni, amely a magánélethez való jog védelmének standardjait figyelembe véve már kifejezetten invazív lehet. Ezzel kapcsolatban felmerül ugyanakkor a kérdés, hogy milyen értékek alapján mérhető egy ilyen rendszer hatékonysága, mert negyven jogsértés akár tekinthető jelentős számnak is – de ez szintén olyan kérdés, amit csak az MI-rendszerekkel kapcsolatban folyamatosan kialakuló és fejlődő joggyakorlat fog majd megválaszolni, és a kapcsolódó bírósági eljárás nem erre fókuszált.

Az ügyben a bíróság az Emberi jogok európai egyezményének 8. cikkét a GDPR-ban foglalt alapelvekre is figyelemmel értelmezte. A peres felek abban egyetértettek, hogy a SyRI korlátozza a magánélethez való jogot – a kérdés az volt, hogy e korlátozás megengedhető-e az Emberi jogok európai egyezménye 8. cikkének (2) bekezdése alapján. A magánélethez való jog korlátozásának az Emberi Jogok Európai Bírósága több évtizedes gyakorlata szerint az úgynevezett hármas tesztet kell kiállnia: a korlátozás (1) törvény által előírt, (2) jogszerű célja van, valamint (3) szükséges egy demokratikus társadalomban. A bíróság megállapította, hogy a SyRI alkalmazásának célja jogszerű, mert a társadalombiztosítás rendszere a jóléti állam egyik alappillére, és az ellátásokkal való visszaélések visszaszorítása fontos azok biztosítása érdekében. A bíróság azonban a SyRI alkalmazását nem tekintette egy demokratikus társadalomban szükségesnek, így megállapította a magánélethez való jog sérelmét, valamint azt is, hogy a SyRI használatát lehetővé tevő jogszabály nem teremti meg az Emberi jogok európai egyezménye által megkövetelt „méltányos egyensúlyt” a társadalmi érdek és a magánélethez való jog között.

Az alábbiakban összefoglaljuk a bíróság érvelését, kiemelve, hogy egy hasonló rendszer bevezetése esetén az Ajánlás mely fő rendelkezéseit lehet érdemes figyelembe venni az alapjogi kockázatok csökkentése érdekében:

⁵⁰ Brief by the United Nations Special Rapporteur on Extreme Poverty and Human Rights as Amicus Curiae in the Case of NJCM c.s./De Staat der Nederlanden (SyRI) before the District Court of The Hague (case number: C/09/550982/ HA ZA 18/388). 2019. szeptember 26. 13. és 14. pontok.

- a) A SyRI nagy mennyiségű (117 különböző) adatkategória felhasználásával működött – ez sértette a célhoz kötöttség és adattakarékosság elveit. Ha egy hasonló rendszer bevezetését megelőzően az érintett állam figyelembe veszi az Ajánlásban foglalt, fentebb már ismertetett adatvédelmi feladatokat, valamint konzultál az egyéb érdekelttel (jelen esetben fontolóra veszi a holland adatvédelmi hatóság megállapításait), akkor az adatkategóriák számának csökkentésével esetleg biztosítani lehetett volna a rendszer jogszerűségét.
- b) A jogszabály nem definiálta konkrétan, hogy a SyRI egy program, vagy algoritmusok és más szereplők hálózata, valamint azt sem, hogy az érintetteket hogyan kell tájékoztatni az adatkezelésről. Ezen túlmenően, a kockázati modell és indikátorai sem voltak nyilvánosak, és az sem, hogy a kockázatos személyeket pontosan hogyan azonosítják. Mivel a SyRI használatát lehetővé tevő jogszabály nem eléggé átlátható és ellenőrizhető, nem állapítható meg, hogy a SyRI alkalmazása egy demokratikus társadalomban szükséges és arányos az elérni kívánt törvényes célhoz képest. Egy hasonló rendszer átláthatóságának biztosítása érdekében az Ajánlásban foglalt, korábban már ismertetett kötelezettségeket is teljesíteni kell – a SyRI esetében sajnos erre sem került sor.
- c) A SyRI szükségességének vizsgálata során a Bíróság megállapította, hogy az államnak kiemelt felelőssége van az új technológiák alkalmazása és a potenciális alapjog-korlátozás közötti megfelelő egyensúly kialakításában. A SyRI használata során ugyanakkor magas a diszkrimináció kockázata – a Bíróság megállapítása szerint szinte csak szegényebb környékeken, úgynevezett problémás kerületekben alkalmazták. A SyRI alkalmazása előtt az állam nem végzett továbbá a GDPR 35. cikke alapján kötelező adatvédelmi hatásvizsgálatot sem. Az Ajánlásban foglalt rendelkezések betartása esetén egy hasonló rendszer bevezetésekor az adatvédelmi hatásvizsgálattal párhuzamosan emberi jogi hatásvizsgálatot is kellene végezni – a fenti, *Az államok által végzett kockázatfelmérések és emberi jogi hatásvizsgálatok gyakorlati kérdései* című pontban ismertetett metodológia pedig segíthet azonosítani és csökkenteni például a rendszer használata során felmerülő diszkrimináció kockázatát.

Mindent összevetve a Bíróság megállapította a holland állam jogsértését. Az állam nem fellebbezett az ítélet ellen, és a SyRI-t már nem használják. Az ügyet övező nyilvános vita azonban mindenképp felhívta a figyelmet a digitális jóléti államban működő hasonló MI-rendszerek által felvetett kérdésekre, és az ügy tanulságai remélhetőleg segítik az ilyen rendszerekkel kapcsolatos körültekintőbb szabályozási kezdeményezéseket és gyakorlatokat.

Konklúzió

A SyRI-ügy tanulságai és az Ajánlás megállapításai nyomán mind az államok, mind a magánszektor szervezetei előtt komoly feladatok állnak. Először is, az Ajánlás rendelkezéseit minél szélesebb körben meg kell ismertetni az érdekelt felekkel (például képviselők, állami szervezetek, hatóságok, társadalmi szervezetek és a magánszektor szereplői).

Ezen túlmenően felül kell vizsgálni a meglévő jogszabályokat annak érdekében, hogy azok összhangban legyenek az Ajánlásban foglalt iránymutatásokkal. A jogszabályoknak biztosítaniuk kell, hogy az MI-rendszerek (ideértve az Ajánlás által „algoritmikus rendszerként” definiált rendszereket is) tervezése, fejlesztése és folyamatos alkalmazása az emberi jogokkal és alapvető szabadságokkal összhangban történjen, a pozitív hatások felerősítése és az esetleges negatív hatások megelőzése vagy minimalizálása érdekében. Tekintettel arra, hogy az MI-rendszerek működését nagyon sok jogszabály érintheti, ez rendkívül széles körű jogalkotási munka. A jogalkotás és a jogszabályok végrehajtása során a szükséges konzultációba az átláthatóság érdekében be kell vonni az érintett feleket, különös figyelmet fordítva a kiszolgáltatott csoportok véleményére, annak biztosítása érdekében, hogy az MI-rendszerek tervezéséből, fejlesztéséből és folyamatos alkalmazásából eredő emberi jogi hatásokat átfogóan nyomon kövessék, megvitassák és kezeljék.

Ezzel párhuzamosan az állami szektor szervezetei felül kell hogy vizsgálják az MI-rendszerek beszerzésével, tervezésével, fejlesztésével, telepítésével és működésük nyomon követésével kapcsolatos gyakorlatukat is, annak érdekében, hogy az tiszteletben tartsa az alapjogokat, és az emberi jogi hatásvizsgálatok beépüljenek az egyes eljárásokba. Ugyanezt biztosítani kell a magánszektor szervezetei irányában is. Ennek ellenőrzésére ki kell jelölni az eljáró hatóságokat, és biztosítani kell számukra a szükséges oktatást, erőforrásokat és hatáskört. Hatékony, kiszámítható szabályozási és felügyeleti kereteket kell létrehozni, amelyek megelőzik, felderítik, tiltják és orvosolják az emberi jogok megsértését az MI-rendszerek használata során.

Az MI-rendszerek felhasználói számára szintén biztosítani kell a megfelelő oktatást, hogy megértsék ezeknek a rendszereknek a működését (ideértve az elérhető előnyöket és kockázatokat), és megalapozott döntéseket hozhassanak az ilyen rendszerek használata során.

A jogalkotási folyamat során további kihívás, hogy a tagállamok biztosítsák az összhangot az MI-rendszerek szabályozásával kapcsolatos egyéb jogalkotási kezdeményezésekkel – elsősorban az EU MI Rendelettervezetével, valamint az EU-nak a szerződésen kívüli polgári jogi felelősségre vonatkozó szabályoknak a mesterséges intelligenciához való hozzáigazításáról szóló irányelvtervezetével. Az Európa Tanács egyébként jelenleg is dolgozik egy MI-Egyezményen – a munkacíme a „Mesterséges intelligenciáról, az emberi jogokról, a demokráciáról

és a jogállamiságról szóló Európa tanácsi egyezmény”. Ez a tervek szerint egy, a csatlakozó felek részére jogi kötéserővel rendelkező egyezmény lenne, amelyhez az Európa Tanácson kívüli államok is csatlakozhatnak majd. Ennek előkészítésébe az EU is bekapcsolódott – 2022. augusztus 18-án az Európai Bizottság ajánlást adott ki egy európai tanácsi határozatra, amely felhatalmazná a Bizottságot az Európai Unió nevében az egyezménnyel kapcsolatos tárgyalások megkezdésére.⁵¹ A Bizottság 2022. augusztus 18-án kezdeményezett konzultációját az európai adatvédelmi biztos is véleményezte.⁵²

Az emberi jogi hatásvizsgálatoknak a gyakorlatban való elterjedését az is segítheti, ha az államok és az érdekelt felek megfelelő útmutatásokat és szabványokat dolgoznak ki a kapcsolódó eljárások lefolytatásához. Az emberi jogi hatásvizsgálatok követelménye összhangban van az európai uniós jogalkotási folyamatokkal, és Magyarország Kormányának prioritásaival is. Az Európai Tanács kezdeményezése megjelenik Magyarország Mesterséges Intelligencia Stratégiájában⁵³ is, mint az erős európai együttműködés és globális verseny egyik eleme. Varga Judit igazságügyi miniszter az MI szerepét az igazságszolgáltatás specifikus területén vizsgálta,⁵⁴ figyelemmel a digitalizációval összefüggő emberi jogi garanciákra; az MI-rendszereknek az emberi jogok és a jogállamiság érvényesülésére, továbbá a demokratikus politikai rendszerek működésére gyakorolt hatásait pedig Sztáray Péter, a Külgazdasági és Külügyminisztérium biztonságpolitikáért felelős államtitkára hangsúlyozta⁵⁵ egyik nyilvános előadásában. Az EU szintjén előremutató fejlemény, hogy az MI Rendelettervezet tárgyalásakor a fokozottabb megfelelést igénylő, úgynevezett „magas kockázatú MI-rendszerek” listáját kiterjesztették a demokratikus folyamatokra potenciálisan hatással bíró – például a választási kampányokhoz használt vagy az elektronikus szavazatok számlálását segítő – algoritmusokra.

⁵¹ European Commission: Recommendation for a Council Decision Authorising the Opening of Negotiations on Behalf of the European Union for a Council of Europe Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law. COM(2022)414 végleges (2022. augusztus 18.).

⁵² Wojciech Rafał Wiewiórowski európai adatvédelmi biztos véleménye: Opinion 20/2022 on the Recommendation for a Council Decision authorising the Opening of Negotiations on Behalf of the European Union for a Council of Europe Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law. European Data Protection Supervisor, 2022. október 13.

⁵³ Magyarország Mesterséges Intelligencia Stratégiája 2020–2030. 2020. május.

⁵⁴ A digitalizáció és a mesterséges intelligencia kihívása érinti az igazságszolgáltatási rendszereket is. Magyarország Kormánya, 2021. október 5.

⁵⁵ Sztáray Péter államtitkár a mesterséges intelligencia szabályozásával foglalkozó konferencián. Magyarország Kormánya, 2021. október 27.

Felhasznált irodalom

- A digitalizáció és a mesterséges intelligencia kihívása érinti az igazságszolgáltatási rendszereket is. *Magyarország Kormánya*, 2021. október 5. Online: <https://kormany.hu/hirek/varga-judit-a-digitalizacio-es-a-mesterseges-intelligencia-kihivasa-erinti-az-igazsagszolgalatasi-rendszereket-is>
- Advies Raad van State inzake het ontwerpbesluit houdende regels voor fraudeaanpak door gegevensuitwisselingen en het effectief gebruik van binnen de overheid bekend zijnde gegevens (Besluit SyRI). *Zoeken in officiële bekendmakingen – Overheid.nl*, 2014. szeptember 22. Online: <https://zoek.officielebekendmakingen.nl/stcrt-2014-26306.html>
- Brief by the United Nations Special Rapporteur on Extreme Poverty and Human Rights as Amicus Curiae in the Case of NJCM c.s./De Staat der Nederlanden (SyRI) before the District Court of The Hague (case number: C/09/550982/ HA ZA 18/388). 2019. szeptember 26. Online: www.ohchr.org/sites/default/files/Amicusfinalversionsigned.pdf
- Council of Europe: *Recommendation CM/Rec (2020)1 of the Committee of Ministers to Member States on the Human Rights Impacts of Algorithmic Systems*. Online: https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154.
- Council of the European Union: *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. Third Presidency Compromise Text*. (Title IA, Articles 30–85 and the relevant recitals, Annexes V–IX). (2022. szeptember 23.) Online: <https://artificialintelligenceact.eu/wp-content/uploads/2022/09/AIA-CZ-3rd-Proposal-23-Sept.pdf>
- European Commission: *Recommendation for a Council Decision Authorising the Opening of Negotiations on Behalf of the European Union for a Council of Europe Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law*. COM(2022)414 végleges (2022. augusztus 18.) Online: https://eur-lex.europa.eu/resource.html?uri=cellar:baebce15-1ef5-11ed-8fa0-01aa75ed71a1.0001.02/DOC_1&format=PDF
- Netherlands Juristen Comité Voor De Mensenrechten et al. v. The State of the Netherlands, no. C-09-550982-HA ZA 18-388, 2020. február 5-i ítélet. Online: <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:1878>
- Magyarország Mesterséges Intelligencia Stratégiája 2020–2030*. 2020. május. Online: <https://ai-hungary.com/api/v1/companies/15/files/137203/view>
- Opinion 20/2022 on the Recommendation for a Council Decision Authorising the Opening of Negotiations on Behalf of the European Union for a Council of Europe Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law*. European Data Protection Supervisor, 2022. október 13. Online: https://edps.europa.eu/system/files/2022-10/22-10-13_edps-opinion-ai-human-rights-democracy-rule-of-law_en.pdf
- Sztáray Péter államtitkár a mesterséges intelligencia szabályozásával foglalkozó konferencián. *Magyarország Kormánya*, 2021. október 27. Online: <https://kormany.hu/hirek/sztaray-peter-allamtitkar-a-mesterseges-intelligencia-szabalyozasaval-foglalkozo-konferencian>
- Van Bakkum, Marvin – Frederik Zuiderveen Borgesius: Digital Welfare Fraud Detection and the Dutch SyRI Judgment. *European Journal of Social Security*, 23. (2021), 4. 323–340. Online: <https://doi.org/10.1177/13882627211031257>

Hogyan segíthetik a mesterséges intelligenciával kapcsolatos „emberi jogi hatásvizsgálatok” a demokráciát?

Wet structuur uitvoeringsorganisatie werk en inkomen. *Zoeken in officiële bekendmakingen – Overheid.nl*, 2022. január 1. Online: <https://wetten.overheid.nl/BWBR0013060/2022-01-01>

Wijziging van de Wet structuur uitvoeringsorganisatie werk en inkomen en enige andere wetten in verband met fraudeaanpak door gegevensuitwisselingen en het effectief gebruik van binnen de overheid bekend zijnde gegevens. No 33 579. *Zoeken in officiële bekendmakingen – Overheid.nl*, 2013. június 25. Online: <https://zoek.officielebekendmakingen.nl/kst-33579-7.html>

Vákát

Pirkad a metaverzumban: az új virtuális világ egyes adatvédelmi és társadalmi kérdéseiről



A metaverzum egy sok tekintetben futurisztikus és lenyűgöző virtuális világot kínál, amelyben a felhasználó újszerű módon lesz képes feloldódni a digitális környezetben. A tanulmány arra mutat rá, hogy az új technológia csak részben vet fel újszerű adatvédelmi problémákat. A magánszférát érintő kérdéseken túl néhány olyan területet is elemeztünk röviden, amelyek csupán illusztrációi a metaverzumot, valamint általában az internethasználatot érintő társadalmi kérdések sokaságának.

A metaverzum előképei már léteznek, a virtuális valóságban zajló játékok tapasztalatai sok min-dent előrevetítenek abból, ami a metaverzumot a jövőben jellemezni fogja. Az új virtuális közeg sem-miképpen sem lesz jogon kívüli terület, ott sok más követelmény mellett az adatvédelmi szabályozás is érvényesítendő lesz. A metaverzum a magánszférát sok szempontból érinteni fogja. Az avatárokhoz kapcsolódó adatokat személyes adatnak kell tekinteni, amelyek védelme érdekében intézkedéseket kell majd tenni. Különös jelentősége lesz a *privacy by design* elvnek a rendszer tervezése során.

Az adatkezelők várhatóan sok esetben osztozni fognak az adatkezelői felelősségen más adatke-zelőkkel, és a közös adatkezelői minőség minden bizonnyal számos üzleti modellben érvényesülni fog. Az adatalanyok önkéntelenül is sok személyes adatot fognak feltárni magukról a metaverzumban.

Ahhoz, hogy a metaverzumban a magánszféra megőrizhető legyen, a tervezés során védelmi funkciókat kell beépíteni. Ilyen a fizikai távolságot szimuláló funkció, de sok más intézkedést kell elérhetővé tenni, például a mások figyelme elől elvonulni képes megoldásokat. A klasszikus adat-biztonsági problémák a metaverzumban is jelen lesznek. A hozzáféréskontroll érzékeny kérdéseket vet fel, hiszen a biometrikus azonosítók adott esetben magasabb biztonságot képviselhetnek, míg a kezelésük önmagában is magas kockázatúnak tekintendő.

A metaverzum jogi és magánszféra-védelmi kérdései terén számos további kutatásra lesz szükség a társadalmi hatások pontos feltérképezéséhez.

Bevezetés

Az embert mindig is foglalkoztatta annak gondolata, hogy új világot teremtsen, egy világot a másik világban. Az álmok sokszor nehezen megfejtethető élményvilága gyakran jelentős hatást gyakorolt az ébredés utáni gondolatokra, döntésekre. Az em-beri gondolkodásban kitörölhetetlenül jelen van az a misztikumba hajló vágy, hogy az ember létrehozzon egy olyan közeget, ahol szabadabbnak érezheti magát, a való világban megtapasztalt korlátok elmosódhatnak, és a lehetőségek tárháza szinte meseszerű távlatokat nyit. A technológiával is játszó ember, az örök *homo ludens*

nem kétséges, hogy át kívánja lépni azt a küszöböt, amely a metaverzum irányába mutat. A sikerét előre nehéz megbecsülni, de annyi bizonyos: bele próbál kóstolni, és saját bőrén akarja meg tapasztalni a felhasználók sokasága a metaverzum világát.

Sok évvel ezelőtt egy külföldi utam során az ismeretlen utcákon sétálva fogalmazódott meg bennem a gondolat: milyen nagy segítség lenne egy olyan szolgáltatás, amely a hagyományos térképnél többet nyújtana, és az utcaképet a maga teljességében jelenítené meg, támogatva az ismeretlen helyen járó turistát. Akkor a street view szolgáltatás még nem volt elérhető, és fiatal adatvédelmi jogászként gyorsan el is hessegettem magamtól a gondolatot, hiszen egy ilyen adatfelvétel túlzott beavatkozást jelentene a helyi lakosság magánszférájába – gondoltam akkor. Azóta tudjuk, hogy a gondolat mások fejében is megfordult, és azóta világszerte elérhető és népszerű lett az online térképek utcakép funkciója.

Miért jut ez a metaverzum kapcsán eszembe? Azért, mert akkor, lassan két évtizede úgy éreztem, hogy a street view szolgáltatás az utcán, elszórt módon készített felvételekhez képest jelentős, minőségi lépést jelentene az adatvédelemhez fűződő jog zsugorításában, a magánszféra szűkítésében. A metaverzum kapcsán is felmerül a kérdés: az építőelemek már ismertek, tehát rendelkezésünkre áll a world wide web, vagyis az internet, a világ legutolsó zugairól készült képanyag szintén elérhető, a kiterjesztett és virtuális valóság eszközei szintén kézzelfoghatóak. Innen már csak néhány (igaz, bonyolult) lépés, és mindezek kombinációjából összegeyúrható az a világ, amelyet metaverzumnak nevezünk.

Van-e itt olyan változás, amely azt indokolná, hogy a metaverzumról úgy beszéljünk, mint ami egészen új minőséget hoz létre? Vagy az, ami újnak tűnik, talán nem is annyira idegen és újszerű ahhoz képest, mint amit már ismerünk és a hétköznapiakban meg tapasztaltunk?

Az európai adatvédelmi biztos elemzést végzett annak feltárására, hogy a következő években mely technológiák érdemlik a legnagyobb figyelmet adatvédelmi szempontból. A 2022/23-as jelentés öt technológiát említ: a központi bank digitális fizetőeszközét, az álhírfelismerő rendszert, a szintetikus adatokat, a federált/kollaboratív tanulást (*federated learning*) és a metaverzumot.¹ Témánk nem véletlenül keltette fel az információs társadalmi témákat kutató szakemberek érdeklődését.

Melyek a metaverzum adatvédelmi kérdései? Van-e ezekre helyes, megnyugtató válasz? Az írás kiindulópontjai ezek a kérdések, amelyekre válaszokat keresünk. Az írás közel sem átfogó elemzés, és a szerző nem is törekszik erre. A tanulmány megírásának célja, hogy további hazai kutatásokra és publikációkra sarkallja az olvasót, ha úgy tetszik, vitaindító szereppel született.

¹ Az európai adatvédelmi biztos Tech Sonar jelentése: European Data Protection Supervisor: *Tech Sonar 2022–23 report*. 10.

Mi a metaverzum?

A metaverzum elnevezés Neal Stephenson amerikai író science fiction regényéből származik. Az 1992-ben publikált *Snow Crash*² írja le azt a világot, amelyben az emberek a fizikai világgal párhuzamosan létező metaverzumban is élik az életüket VR (*virtual reality*) eszközök segítségével. A metaverzumban a személyek digitális avatárjukon keresztül jelennek meg, ilyen módon kettőződik meg az ember által tapasztalt világ a digitális világ segítségével.³

A metaverzum leírása természetesen filozófiai kérdések sorát veti fel, mi most itt ebben a tanulmányban mégis elsősorban az egyes ember oldaláról, az ő érdekei és jogai szempontjából közelítünk ehhez az új jelenséghez.

Egyetlen filozófiai jellegű kérdés mégis engedtessek meg a jogász szerzőtől. A számítógép az ember lehetőségeinek javítására hivatott, ezek a képességek, a számítási kapacitás lenyűgöző volta tette annak idején, a 20. században „új technológiává”. A hétköznapi ember számára a számítógép akkor vált életközelié, amikor megjelentek a személyi számítógépek, és a háztartásokban nemcsak a készülékek, hanem a szoftver is irodai asszisztens vagy népszerű digitális játékok formájában az élet részévé vált. A viselhető eszközök, valamint az IoT még egy jelentős lépést jelent az emberközelség útján, a való és a virtuális világ közelítésében.

Amire rá kívánok itt mutatni, az egy olyan tulajdonsága a metaverzumnak, amely a sajátosságainak lényegét adja: az ember már nemcsak a bináris számrendszerrel leírható eszközök használójaként, hanem önmaga is egy bináris „adattömegként” simul bele a környezetébe. A metaverzum annak az élményét kínálja, hogy egyszerre többen tapasztaljuk meg ugyanazt a virtuális világot, és abban egymáshoz is kapcsolódni tudunk, legyen szó játékról, kereskedelemről, virtuális utazásról vagy bármilyen közös tevékenységről.

Jaron Lanier aggodalma juthat itt eszünkbe, aki szerint az utóbbi évtizedekben a technológia mintha lefokozta volna a személyközi interakciókat, pedig itt a legfontosabb kérdés, hogy a technológia hogyan változtatja meg az embert.⁴ Hogyan lehet tehát a metaverzumban úgy mozogni, úgy „létezni”, hogy mindeközben ne csak jogainkat, hanem *emberségünk* lényegét is megőrizzük? Alan F. Westin szintén, és meglehetősen korán, már az 1960-as években felhívta a figyelmet a technológiával együtt járó elembertelenedésre.⁵

² Az összefoglaló forrása: Snow Crash Summary and Study Guide. *SuperSummary*.

³ A szerzővel készült egyik interjúbán úgy vélekedett, hogy a metaverzum *Snow Crash*-ben leírt gondolatát azért is használják fel az új technológia sorvezetőjeként, mert a fejlesztőknek egyszerűbb egy kész koncepcióra építeni, mint egy új elgondolás kidolgozásán hosszasan fáradozni. Úgy fogalmaz: a science fiction író a technológiai iparra legnagyobb hatást gyakorló pozíció. Az interjú elérhető online: Neal Stephenson on the Future of the Metaverse. *YouTube*.

⁴ Jaron Lanier: *You Are Not a Gadget*. London, Penguin Books, 2011. 4.

⁵ Alan F. Westin (szerk.): *Information Technology in a Democracy*. Cambridge, MA, Harvard University Press, 1971.

Próteusz-szindrómaként⁶ említi a tudomány azt a jelenséget, amikor a videójátékban részt vevő személy az avatárjával akarva-akaratlanul azonosul, és a játékban felvett szerepének hatása a való világban is érvényesül.⁷ A játékon belül is megfigyelhető az avatár hatása a viselkedésre, így például normál testsúlyú avatárral rendelkező játékosok nagyobb eséllyel fognak sportolni, vagy a magasabb avatárok mögötti játékosok nagyobb önbizalommal rendelkeznek, mint a náluk kisebb társaik. De nem csupán a virtuális közegben való viselkedésre hathatnak ki az avatár jellemzői, hanem az offline életben is képes alakítani a személyiséget.

Azok a játékosok, akik részt vettek a „Papers, Please” nevű, disztópikus körülmények között játszódó bevándorlási hivatali szimulációs játékban, azok később a bevándorló háttérű személyekkel kevésbé segítőkész módon bántak.⁸ Pozitív példa is hozható ugyanakkor, így például a szuperhőst játszó felhasználók mintha az offline világba visszalépve segítőkészebbé váltak volna. De akár terápiás távlatokat is nyit az avatárokkal való összefonódás, gondolni lehet itt fóbiák kezelésére vagy személyes képességek, lehetőségek javítására.⁹

Úgy tűnik tehát, hogy az emberi méltóság védelmének kérdései a technológia használata kapcsán különös élességgel vetődnek fel: nem önmagában az új technológia, hanem annak használata, nem megfelelő alkalmazása vagy éppen az ismeretek hiánya, a védekezési mechanizmusok kiiktatása vet fel fontos kérdéseket.

Az alábbi jogi elemzésben az érintetti jogokról, adatvédelmi alapelvekről és ezek európai, illetve globális összefüggéseiről lesz szó. Mindezek háttérben azonban ott állnak a most megfogalmazott kérdések, amelyek foglalkoztatják a szerzőt, és valószínűleg a kedves olvasót is.

A metaverzum technológiai oldala

2023-ban a metaverzum még csak egyes elemeiben rajzolódik ki. Nem egy már jelenleg is létező, hanem jövőbeni technológiáról beszélünk, de ahhoz már elég információ áll rendelkezésre, hogy a körvonalait felmérhessük: miként fog felépülni, milyen funkciókat fog kínálni. Online és offline közösségek összekapcsolódását kell elképzelnünk, ahol a felhasználók akár szakmai, akár személyes megfontolások alapján építhetnek ki közösségeket, szórakozhatnak, kereskedhetnek virtuális

⁶ Próteusz görög tengeristenség, aki a mitológia szerint jóstehetséggel rendelkezett, de mivel százféle alakot tudott öltetni, mindig kicsúszott azok kezéből, akik jóslásra akarták kényszeríteni. Online forrás: Próteusz. *Arcanum*. Érdekes megfigyelni, hogy a legújabb technológia jellemzőinek leírásakor is antik gyökerekhez nyúl vissza a tudomány.

⁷ Kim Szolin et al.: “I Am the Character, the Character Is Me”: A Thematic Analysis of the User-Avatar Relationship in Videogames. *Computers in Human Behaviour*, 143. (2023), 3.

⁸ Szolin et al. (2023): i. m. 3.

⁹ Proteus effect. *Tech Target*.

és valóságos javakkal, szolgáltatásokkal.¹⁰ Nagy technológiai vállalatok, mint a Facebook (Meta), a Microsoft, a Tencent vagy az NVIDIA is bejelentette, hogy foglalkozik a metaverzum kiépítésével.¹¹

A metaverzum előképének tekinthető élményekkel találkozhattak már bizonyos online játékok, így a Second Life vagy a Call of Duty használói, amelyek nagy részletességgel adják vissza a való élet körülményeit, és több játékos együttműködésén, kapcsolatán alapulnak.¹²

A metaverzum kiépítésének első fázisa az úgynevezett digitális ikrek (*digital twins*) létrehozása. Ebben a fázisban a fizikai világot leképezik egy virtuális világgá, tehát gyakorlatilag elkészül az eredeti másolata. A két világ, az eredeti és a másolat ekkor még teljesen párhuzamosan létezik egymás mellett. Másolat készül nem csupán a tárgyról, a fizikai valóságról, hanem az emberek is megjeleníthetők az új közegben. A science fiction művészet hagyományaihoz híven ezeket a virtuális lényeket avatároknak nevezik. Az avatár a hinduizmus kifejezése, olyan istenségeket jelöl, akik a földön emberi vagy állati formában küzdenek a gonosz ellen.¹³

A második fázisban a metaverzum már saját belső tartalmakat hoz létre – a használók, például az avatárok közreműködésével természetesen. A metaverzum alapját jelentő digitális közeg ekkor már nem csupán leképezése a való világnak, hanem annál több, illetve attól eltérő. Az új világ elkezd saját életét építeni, belső tartalmat (*native content*) hoz létre.

A harmadik, záró fázisban a két valóság egymással már teljesen összesimul, létrejön egy szürreális világ. A metaverzum végérvényesen magába zárja az eredeti világot, de már nem függ attól, önfenntartóvá válik.¹⁴ Nem ikrek már olyan értelemben, hogy a két világ nem tökéletesen azonos, még ha az összefüggések elkerülhetetlenek is, és a felhasználók értelemszerűen a való világból jelentkeznek be, és oda „lépnek vissza”.

A metaverzum felvonultat számos már ismert technológiát, amelyek hozzájárulnak majd a megfelelő működéshez, így például a mesterséges intelligencia, az Internet of Things, a biometrikus azonosítás,¹⁵ a Bluetooth vagy

¹⁰ Az európai adatvédelmi biztos TechSonar elemzése a metaverzumból: European Data Protection Supervisor: Metaverse.

¹¹ Disha Sinha: Top 10 Companies Working on Metaverse and Its Development in 2022. *Analytics Inside*, 2022. február 19. A szerző áttekintése szerint a tíz vállalat a következő: Meta, NVIDIA, Epic Games, Microsoft, Apple, Decentraland, Roblox Corporation, Unity Software, Snapchat, Amazon.

¹² Online: Second life; Call Of Duty.

¹³ Online forrás: Avatar. *Britannica*.

¹⁴ Yuntao Wang et al.: *A Survey on Metaverse: Fundamentals, Security, and Privacy*. 2022. 1–2.

¹⁵ A biometrikus azonosítók használata az elmúlt évtizedekben bővült. A bővülés mind a lehetséges azonosítási módok, mind a felhasználás volumenében megmutatkozik. Az egyelőre nem jósolható meg, hogy a biometrikus azonosítás kiszorítja-e majd a hagyományos azonosítási módokat, mindenestre a metaverzumban várhatóan jelentős szerepe lesz a biztonságosabb, de privacy szempontból érzékenyebb azonosítási módoknak. Vö. Szabó Endre Győző – Bojnár Katinka – Buzás Péter:

a blokklánc-technológiának is szerepe lesz az új virtuális világ fenntartásában.¹⁶ A belépési pontot egy virtuális valóságot közvetíteni képes szemüveg jelenti majd, így például a Microsoft Hololens¹⁷ vagy az Oculus.¹⁸ Az élmény teljességét szolgálják majd más, például a kezet megjelenítő és funkcióját biztosító eszközök vagy más szenzorok, kamerák, egyéb kellékek is. Mindezek azt eredményezik, hogy a felhasználó képes teljesen elmerülni a virtuális világban, teljes valójával annak részévé válik, érzékei és figyelme az offline világot gyakorlatilag teljesen kizárja. A szem és arc mozgását aprólékosan követő technológia a szemkontaktus lehetőségét ígéri, és valós idejű, a másik arcát, gesztusait közvetíteni képes közeget. Az emberi kommunikáció minél élethűbb közvetítése tehát alapvető kérdés a fejlesztések során.

A metaverzum adatvédelmi szempontú elemzése

Az alábbiakban a személyes adatok kezelésére és védelmére vonatkozó szabályok, illetve fogalommeghatározások segítségével elemezzük azokat a jogkérdéseket, amelyek bizonyosan meghatározói lesznek a metaverzum körüli adatvédelmi jogi problémáknak. A kérdések kiválasztásában a szerző hatósági tapasztalatai is szerepet játszottak. Számos olyan kérdés felvethető lenne, amelyek a már létező technológiai környezetben is releváns kérdések. Ezeket most figyelmen kívül hagyjuk, és a metaverzum újszerűségével járó problémákra koncentrálunk.

Személyes adatok az avatárok adatai?

A metaverzum kiépítésének első fázisában úgynevezett digitális ikrektől szóltunk feljebb. A koncepció kiindulópontja szerint mindennek és mindenkinek, aki részt kíván venni, meglesz a digitális leképezése az új közegben. Az emberek avatárok útján jelennek meg, ami azzal jár, hogy a hús-vér ember felhasználókhöz nem feltétlenül megszólalásig hasonló lények fogják képviselni őket az online világban. Ahogyan a virtuális játékokban, úgy a metaverzumban is elképzelhető, hogy az avatárok tulajdonságai alakíthatók lesznek. Ettől a lehetőségtől függetlenül a legfontosabb,

Új globális technológiák kihívásai a magyar jogban. In Tóth András (szerk.): *Technológia jog*. Budapest, Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, 2016. 70–71.

¹⁶ A blockchain-technológia például a digitális ikrek védelmére szolgálhat. A blokklánc garanciaként szolgál arra, hogy a felhasználó a virtuális közegben nem egy megtévesztés áldozata, hanem amit lát, vagy akivel éppen kommunikál, az valóban az, aki, aminek tűnik. A sok felhasználó által használt felületen a bizalom megteremtése kulcskérdés, és ebben a blokklánc-technológia hatékony lehet. Vö. Ana Reyna et al.: On Blockchain and Its Integration with IoT. Challenges and Opportunities. *Future Generation Computer Systems*, 88. (2018), 173–190.

¹⁷ Online: Microsoft HoloLens.

¹⁸ Online: Oculus.

hogyan az avatár felismerhető lesz, még ha például a felhasználó „idealizált énjét” is fogja megjeleníteni.¹⁹

A szó technológiai értelmében az avatároknak is lesznek „adatai”, de ez valóban műszaki jellegű kérdés. A kérdés jogi oldala arra mutat rá, hogy függetlenül az avatárok és a felhasználók közötti hasonlóságtól, függetlenül a felhasználó által létrehozott avatárok számától, az adatok mindig köthetők lesznek egy természetes személyhez, akinek az adatvédelemhez való joga nem enyészik el.²⁰ Ennek megfelelően az avatárokhöz kötődő adatok személyes adatnak minősülnek a GDPR szerint.²¹

A személyes adatok elkísérik a metaverzumba is a felhasználókat, ennek megfelelően pedig az adatok védelmének igénye is elválaszthatatlan része marad a jogi követelményrendszernek. A metaverzum létrehozásán fáradozó piaci szereplők tisztában vannak ezzel az elvárással, illetve elvárásrendszerrel, ezért az új virtuális világ jellemzői között kiemelt helyen említik a privacy, illetve az adatok védelmét.²²

A természetes személy felhasználót képviselő avatár vagy avatárok (mert minden bizonnyal többet is létre lehet majd hozni) önálló életet élnek a virtuális közegben. Az avatárhoz kapcsolódó adatok végső soron a mögötte álló adatalany személyes adatainak tekintendők. Jogi értelemben nem tehetünk különbséget „valós” és „nem valós” adatok között, nem játszik szerepet az, hogy az avatár a természetes személy felhasználó életétől teljesen eltérő küllemmel és egyéb jellemzőkkel, magatartásmintákkal stb. jelenik meg a metaverzumban.

Adatvédelmi jogi szempontból csupán az a meghatározó, hogy ki a felhasználó, ki az adatalany, akit az érintetti jogok megilletnek. A virtuális személyiséggel összevetve ugyan „elszemélytelenedhet” az avatár, de az adatok jogi értelemben mindaddig személyesek maradnak, amíg a valós személlyel a kapcsolat kimutatható, akár közvetve, akár közvetlenül azonosítható marad. Az azonosíthatóság nem csupán a biztonságos üzemeltetés érdekében fontos, hanem az üzleti megfontolások

¹⁹ Szolin et al. (2023): i. m. 2., 10. Az interjúalanyok arról számoltak be, hogy a játékbéli avatárjuk tulajdonképpen egy kicsit az idealizált énjük is.

²⁰ A személyes adat jellegét megállapíthatjuk a tartalom elemzésével (ha az adat az érintettre vonatkoztatható), a célra tekintettel (az adat kezelésének célja, hogy az érintettet vagy az ő helyzetét befolyásolják), vagy az eredményre tekintettel (az adatkezelés hatással van az érintett érdekeire). Vö. Péterfalvi Attila – Révész Balázs – Buzás Péter (szerk.): *Magyarázat a GDPR-ről*. Budapest, Wolters Kluwer Hungaria, 2018. 67–68.

²¹ A GDPR 4. cikk 1. pontjában rögzített „személyes adat” definíciónak az a kitétele, amely szerint a személy közvetlen vagy közvetett módon azonosítható, kétséget kizáróan érvényesül. Elképzelhető, hogy bizonyos személyek, illetve bizonyos adatok csak szűk adatkezelői kör számára lesznek hozzáférhetők, ez azonban nem változtat azon, hogy az érintett legalább közvetett módon azonosítható marad, és ezért rá a védelmi szabályok alkalmazandók.

²² A Meta által közzétett, Mark Zuckerberg szereplésével készült prezentáció is az elsődleges értékek között említi a biztonságot, az interoperabilitást, a nyitottságot és a privacyt. Online: *The Metaverse and How We'll Build It Together – Connect 2021. YouTube.*

is ebbe az irányba mutatnak. Legyen szó profilozásról, célzott reklámozásról, vagy bármilyen más üzleti értékről, a felhasználó környezetében keletkező adatok megőrzik személyes jellegüket.

Az adatvédelmi felelősség kérdései: adatkezelő és felhasználó – és akik közöttük vannak

A metaverzum „benépesítése” olyan vonzerőt igényel, amely meggyőzi a leendő felhasználókat arról, hogy valóban érdemes abban elmerülni és időt tölteni, valamint pénzt költeni a metaverzumban. Az élmény magával ragadó voltán túl a szolgáltatások megteremtésében, működtetésében részt vevő szereplők érdekalapon fognak dönteni arról, hogy belépjenek-e az új piacra. A közös érdek sok esetben közös adatkezelést fog eredményezni adatvédelmi jogi szempontból. Ez már a hagyományos piaci körülmények között is így volt, a metaverzum tehát a jelenlegi fogalomrendszerünkkel várhatóan nagy biztonsággal leírható lesz.

A szolgáltatói oldalon adatkezelőket fogunk tudni azonosítani, míg a felhasználó, ha szerepe nem terjed túl a hétköznapi használaton, a metaverzumban sem minősül sem adatkezelőnek, sem adatfeldolgozónak.²³ Ami bizonyosan megjósolható, hogy lesznek olyan felhasználók, akik egy másik szereplővel megvalósuló együttműködésük révén, így tipikusan reklámozás, profilozás céljából közös adatkezelői felelősséget fognak viselni.²⁴

A közös felelősség kérdéseit az Európai Unió Bírósága több döntésében is elemezte, és kimondta, hogy az egyszerű felhasználó nem válik a Facebookkal együtt felelőssé a személyes adatok kezeléséért, azonban a rajongói oldal (*fan page*) adminisztrátora nem egyszerű felhasználó. Ami a különbségtételt indokolja, az a Wirtschaftsakademie-ügyben született ítélet szerint az, hogy a rajongói oldal létrehozója lehetővé teszi a Facebook számára, hogy az oldal látogatóinak számítógépén cookie-kat helyezzen el. Az adminisztrátornak beállításokat kell eszközölnie az oldalon, ami befolyásolja a személyes adatok kezelését. Összességében tehát az adminisztrátor részt vesz a személyes adatok kezelése céljának és módjának meghatározásában, tehát ő is adatkezelőnek tekintendő.²⁵

Ha az elemzés nem is lehet teljes, minden részletre kiterjedő egyelőre, de a jelenlegi ismereteinkkel azt már előre tudjuk jelezni, hogy az egyes szereplők

²³ Az Európai Unió általános adatvédelmi rendelete, a GDPR (18) preambulumbekzdése szerint személyes vagy otthoni tevékenységnek minősül többek között a közösségi hálózatokon történő kapcsolattartás és az online tevékenységek. Az „átlagos” felhasználó tehát adatvédelmi felelősséget nem visel általánosságban, és ezt a privilegiált helyzetét a metaverzumban is meg fogja őrizni.

²⁴ A C-210/16. sz. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein kontra Wirtschaftsakademie Schleswig-Holstein ügyben hozott előzetes döntés 35–41. pontjai szerint. Hasonló adatvédelmi jogi elemzést végez el az EUB a Planet 49 (C-673/17), a Fashion ID (C-40/17) és a Jehova Tanúi (C-25/17) ügyekben hozott döntéseiben.

²⁵ A Wirtschaftsakademie ügyben született ítélet (39) pontja.

az adatvédelmi jogi minőségüket a metaverzumban is meg fogják őrizni, ahogyan azt a hagyományos piaci körülmények között megszerezték.

Az Európai Unió Bírósága a védelem megerősítése érdekében az adatkezelői felelősség minél szélesebb körű alkalmazását fontosnak tartotta a közös adatkezelői felelősséget elemző döntéseiben.²⁶ Ez a megközelítés a jogalkalmazás minden területén figyelembe veendő. Bár a metaverzum kínálhat majd újszerű üzleti modelleket, a jogértelmezésben az a tendencia, hogy az adatkezelői felelősséget minél szélesebb körben kell megállapítani, az új virtuális környezetben is irányadó marad. Feltételezhető az is, hogy a metaverzum az összetettebb adatkezelések révén több lehetőséget kínál majd az olyan kooperációkra, amelyek esetében a fent elemzett ítéletek alapján a közös adatkezelői felelősség megállapítható lesz.

*Önkéntelenség, teljes beolvadás, az ösztönös védelmi mechanizmusok
kikapcsolása – a kockázatok megbecsülésére tett kísérlet*

A metaverzum mögött álló mesterséges intelligencia személyre szabott szolgáltatásokat képes létrehozni. Az MI-algoritmusok gazdag és személyes élményvilágot fognak teremteni, termékek, szolgáltatások, információk ajánlásával.²⁷ A technológia tehát készen áll a metaverzum élményekkel való feltöltésére, és ezzel a képességével az adatvédelmi elemzés során is számolni kell.

Mi teszi kockázatosabbá magánszféra-védelmi szempontból a metaverzumot a korábbi technológiai megoldásoknál? A teljes belemerülés, belefeledkezés jelenségét kell itt elsősorban megemlíteni. Akkor, amikor a felhasználó „fél lábbal” kívül áll a virtuális világon, másik felével pedig az online környezetben van, csak egyfajta korlátozott virtuális élményről beszélhetünk. A felhasználó például kezében tartja a telefont, hallja a külvilágból származó hangokat, érzékeivel alapvetően nem a virtuális világ része, hanem az offline-é.

A metaverzum elképzelt világába érkezve a felhasználó teljes valójával a virtuális világba lép be, ott gyakorlatilag feloldódik az őt fogadó környezetben. Bár a felhasználónak értelemszerűen lesz lehetősége alakítani saját környezetét (ennek részletei majd a tényleges megvalósulás időszakában tisztázódnak), és ő maga irányíthatja majd a navigálás menetét, mégis folyamatosan ki lesz téve előre nem látható élményeknek, választási lehetőségeknek.

Könnyen elképzelhető olyan helyzet, amikor érzékeny döntési helyzetbe kerül, akár világnézeti, akár például politikai jellegű választás elé áll az avatárja révén a gyanútlan felhasználó. Az adott ország kultúrájától, szokásaitól, aktuális közéleti eseményeitől függően egészen apró gesztusok, hétköznapiak tűnő preferenciák

²⁶ Szabó Endre Győző: *A védelmi lépcső elmélete*. Budapest, Ludovika Egyetemi Kiadó, 2022. 79–80.

²⁷ Wang et al. (2022): i. m. 7.

is politikai, világnézeti állásfoglalásként foghatók fel, vagy más véleményre engedhetnek következtetni. Ezeket az adatokat aztán sokféleképpen lehet elemezni, felhasználni.²⁸

Nem szabad elfelejteni, hogy az online viselkedés mindig jól monitorozható, visszakereshető, ezért a metaverzum a maga steril formájában a magánszféra el-lentéteként írható le. A világháló előtti kitárulkozás és a folyamatos megfigyeltség lehetősége egy nemkívánatos kombináció: tökéletes ellentpontja annak az állapotnak, amelyet magánszféra-védelmi szempontból ideálisnak tartunk, nevezetesen a más által nem zavart létezés, amelyben az ember úgy viselkedhet, ahogyan neki jólesik, és a személyiség úgy bontakozhat ki, ahogyan azt egészségesnek tekintjük.

Az említett választási kényszerhelyzet, mint a megnyilvánulás elkerülhetetlen példája értelemszerűen csak egy a sok lehetséges és elképzelhető szituáció közül. Az online közegben kialakult gyakorlatokat és súlyos visszaéléseket figyelembe véve naivitás lenne azt állítani, hogy ilyen helyzetek nem adódhatnak, illetve adott esetben ezek megteremtése mögött ne állhatna tudatosság. Az ilyen helyzetek megteremtésében az eredetire megszólalásig hasonlító úgynevezett *deep fake* másolatok is szerepet játszhatnak, illetve a manipuláció egyéb formái, mint a sürgetés, pszichológiai nyomás, félelemérzet keltése. Ezzel a kockázattal tisztában kell lenni, és a felhasználónak egészséges bizalmatlansággal kell majd bejárnia a metaverzum helyszíneit.

Készülni is lehet a kockázatokra, ebben a technológiai megoldások is a felhasználó segítségére lehetnek. Az avatárt át lehet vinni egy olyan környezetbe, amely a metaverzum egy adott szegmensének másolatából készül, ahol a felhasználó magára maradhat, és nem lehet lehallgatni. Vagy például láthatatlanná lehet tenni az avatárt mások számára, és ennek révén előzhető meg a visszaélések.²⁹ Az egy másik kérdés, hogy amennyiben az avatárok egymás számára láthatatlanná tehetők, és ezt a felhasználók tömegével meg is fogják tenni, akkor a metaverzum mennyiben jeleníti majd meg azt a közeget, amelyet a fejlesztők megálmodtak.

Az érzelmi reakciók feltérképezése

A felhasználó érzékeny területeket érintő véleményéhez hasonlóan az érzelmi reakciók elemzése szinte korlátlan távlatokat nyit a különböző preferenciák

²⁸ Az osztrák adatvédelmi hatóság 2019 októberében az osztrák postára vetett ki 18 millió eurós összegű bírságot. Az osztrák hatóság úgy ítélte meg, hogy a posta birtokába kerülő, a lakosok politikai hovatartozására is következtetni engedő információk nem használhatók a „politikai affinitás” megismerésére, továbbá az ilyen információk értékesítése nem áll összhangban az adatvédelmi szabályozással. Bár a határozatot az osztrák közigazgatási bíróság formai okokból hatályon kívül helyezte, a bíróság is megerősítette az adatkezelés jogellenes voltát. Online: BVwG–W258 2227269-1/14E.

²⁹ Wang et al. (2022): i. m. 40.

megfigyelésére. Itt is emlékeztetni kell arra, hogy a metaverzum azt az élményt ígéri, hogy tulajdonképpen teljes beleolvadást hoz magával, és egy valóságosnak tűnő, másodlagos világot teremt. Ebben a felhasználó egy ponton túl már nem képes „viselkedni”, hanem önmagát adja, minden tekintetben önkéntelenül cselekszik. A családtagok, barátok jelenléte, a magával ragadó felhasználói környezet ebben az aspektusban teljesen védtelenné teszi az avatar mögött húzódó tényleges felhasználót az esetleges megfigyeléssel, profilozással szemben.

A metaverzum futurisztikus világában a felhasználó szociális helyzetek résztvevője lehet majd, akár ismerősökkel, akár ismeretlenekkel találkozva. A felhasználó ezekben a helyzetekben valószínűleg hasonlóan fog viselkedni, mint az offline közegben. Ezt a megállapítást azzal is alátámaszthatjuk, hogy a felhasználók nagy része a közösségi kapcsolataik kibontakoztatásának lehetőségét látják majd a metaverzumban, ezért nem fognak majd „kettős életet” élni. A kisebbség ettől eltérő magatartása nem változtatja meg az elemzésünk alapjait.

Ezt az okfejtést támasztja alá az a tilburgi elemzés, amely a Second Life-felhasználók viselkedését vizsgálta. Igaz, hogy a felhasználók önbevallására alapozott a kutatás, és itt torzíthatnak az adatok,³⁰ de a kutatás következtetésként azt vonja le, hogy amennyiben a virtuális világban valóságos társadalmi interakciók zajlanak le, akkor ez lehetőséget ad a valós társadalmi kapcsolatok feltérképezésére, elemzésére is.

Az érzelmi reakciók, illetve általában az érzések megjelenítése az online közegben mindenképpen egy fontos határ átlépését jelenti. Az adatvédelmi hatóságok is jelentőséget tulajdonítanak ennek, különösen, ha az érintett számára nem észlelhető módon történik, akár a bűnüldözés területén,³¹ vagy üzleti típusú felhasználás esetén.³²

³⁰ Ronald Leenes: Privacy in the Metaverse. Regulating a Complex Social Construct in a Virtual World. In Simone Fischer-Hübner – Penny Duquenoy – Albin Zuccato – Leonardo Martucci (szerk.): *The Future of Identity in the Information Society*. Boston, MA, Springer, 2008. 100–101.

³¹ Az Európai Adatvédelmi Testület 5/2022. számú, az arcfelismerő technológia használatáról a bűnüldözés területén címet viselő iránymutatása több olyan, a magánszférába súlyosan beavatkozó felhasználási módot említ, amelyekre tilalmat javasol. Az egyik ilyen az olyan arcfelismerő technológia, amely a természetes személyek érzelmeire nézve képes következtetéseket levonni. Online: Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement. 5.

³² A Nemzeti Adatvédelmi és Információszabadság Hatóság NAIH-85-3/2022 számú határozatában egy bank felelősségét állapította meg telefonos ügyfélszolgálati munkatársakkal folytatott, rögzített beszélgetések elemzése kapcsán. A határozat szerint „[a]z Ügyfél az elemzés eredményét felhasználva állapítja meg, hogy melyik elégedetlen ügyfelet szükséges visszahívni, ezzel kapcsolatban többek között automatikusan elemzi mind a telefonáló érintett, mind az ügyfélszolgálati munkavállaló érzelmi állapotát és a beszélgetés egyéb jellemzőit”. Az ügyben a hatóság mind ez idáig legmagasabbnak számító, 250 millió forintos bírságot szabott ki, ezzel is aláhúzza a jogsértés súlyát és az adatkezelés tolakodó jellegét.

A fogyasztó által generált adatok kiszámíthatatlansága tehát megbecsülhetlenné teszi a lehetséges kockázatokat is. A kockázatalapú megközelítést alkalmazó adatvédelmi szabályozással kapcsolatban itt a metaverzum egy jelentős és további vizsgálatot, garanciákat követelő jellemzőjére kell rámutatnunk.

Az egészséges mértékű internethasználat és a magánszféra összefüggéséről

Az internet használatával összefüggésben nem csupán azokról a kockázatokról tudunk, amelyek a felhasználóra leselkednek, hanem önmagában a túlzott mértékű, túl hosszú használatot is megemlítjük a metaverzum elemzése kapcsán. A metaverzum természeténél fogva magában hordozza azt a lehetőséget, hogy a felhasználói élmény fokozása révén az interneten töltött idő meg fog növekedni. Minél jobban összeolvad a magánszféra és a virtuális közeg, annál valószínűbbnek tűnik, hogy ez ténylegesen bekövetkezhet. A magánszféra határait és meghatározó élményeit befolyásoló közeg kapcsán felmerül a kérdés, hogy a viselkedési minták változásával nő-e a kockázata az úgynevezett viselkedési addikcióknak.

Ahogy Bányai Fanni és szerzőtársai fogalmaznak, „[f]üggő magatartásról akkor beszélhetünk, ha a viselkedés uralni kezdi az egyén életét, károsítja annak és környezetének testi-lelki állapotát”.³³ A pszichológusszakma arra mutat rá, hogy függőséget nem csupán például valamilyen kémiai jelenség okozhat, hanem zavarhoz vezethet bizonyos magatartások túlzásba vitele, és a normális magatartás már nem okoz megelégedettséget, az egyén élete kibillen korábbi egyensúlyából. Nem azt állítom, hogy a metaverzum vegytiszta megvalósulása esetén automatikusan adódik a felhasználók széles tömegét érintő, fent leírt kockázat. Azt a következtetést ugyanakkor megalapozottan vonhatjuk le, hogy a felhasználók kisebbségét érintő úgynevezett problémás internethasználat³⁴ egy új dimenzióval fog kiegészülni.

A természetes közegben megélhető és megelégedést nyújtó magánszféra ebben a kontextusban nem csupán védelmet élvező és védendő közegként írható le, hanem úgy is, mint a magatartási addikció ellen ható, a normális magatartást megjelenítő, végső soron az egyént és az ő társas kapcsolatait védő környezet. Használhatnánk a „buborék” kifejezést, akár figyelmeztetésként is, hogy a túlzott internethasználat ellenében a magánszféra jelentőségét hangsúlyozzuk. Ez ugyanis az a közeg, amelyben a személyes adataink elsődlegesen keletkeznek.

Az elemzésünk arra mutat rá, hogy helyes az a törekvés, ha magánszféránk minél kisebb részét jelenítjük meg az online világban, és az ott töltött idő is korlátozás alá

³³ Bányai Fanni et al.: A problémás videojáték-használat újabb elméleti és gyakorlati megközelítései. *Információs Társadalom*, 18. (2018), 1. 93–106.

³⁴ A problémás internethasználat (Problematic Use of the Internet, PUI) számos jelenséget foglal magában, így játékkal, szerencsejátékkal, online zaklatással kapcsolatos problémákat. Vö. Learning to Deal with Problematic Usage of the Internet. *COST – European Cooperation in Science and Technology*.

esik. Az online és offline világ összefonódásából előálló metaverzumban minden bizonnyal még nehezebb lesz ezt megvalósítani. Az sem idegen gondolat a közösség szintjén, ha a virtuális közegben is elérhetőek bizonyos információk, adott esetben támogatás azok számára, akik a függőségből keresnek kiutat. Ezen a ponton viszont már olyan mélyen járunk a való és virtuális világ összefonódásában, hogy messze eltértünk a szűk értelemben vett adatvédelmi elemzéstől. Mégsem haszontalan elkalandozás ez, hiszen jól illusztrálja az új technológiával kapcsolatos kérdések sokaságát és megválaszolatlanságát.

Fizikai távolság

Képzavarnak tűnhet a metaverzumból szóló tanulmányban fizikai távolságról írni. A felvetés azonban semmiképpen sem indokolatlan, mert az avatárok mögött hús-vér emberek állnak, akik a magánszféra iránti igényüket megőrzik a virtuális világban is. Ott sem tolerálják a bizonyos határt átlépő közelséget. Nem sokkal a létrejötte után a virtuális valóságra épülő közösségimédia-platfommon, a Horizon Worlds felületén történt szexuális zaklatásról számolt be az egyik női felhasználó.³⁵ Úgy tűnik, hogy a virtuális világ sem óv meg azoktól a jelenségektől, amelyekről az offline világban is szabadulnánk.

Továbbá azért sem indokolatlan a fizikai közelség témájáról szólni, mert a metaverzum egyfajta leképeződése a valóságos világnak, és a magánszférára, a mások által meg nem zavart térre ott is szükség van. Nem őrizhető meg a virtuális világ sem élhetőnek, élvezhetőnek, ha nem áll rendelkezésre olyan eszköz, amely a személyes tér kikényszerítését szolgálja.³⁶ A magánszféra klasszikus szabályai az online térben is helyet követelnek maguknak. A Meta úgy reagált a felhasználói igényekre, hogy minden avatárt egy két láb sugarú (körülbelül 60 cm) virtuális kör vesz körül, ami végső soron azt eredményezi, hogy a felhasználók nem kerülhetnek négy lábnál közelebb egymáshoz.³⁷ Ilyen módon próbálják elkerülni a kellemetlen vagy tolatkodó élményeket, és az egészséges fizikai távolságra szorítani azokat, akik ezt zaklató módon át szeretnék lépni.

A fizikai távolság kapcsán nem újdonság, amiről itt értekezünk. Az intim, a személyes, a társadalmi és a nyilvános kapcsolatokhoz tartozó egészséges távolság meghatározása a pszichológia tudományának művelőit már régóta foglalkoztatta.

³⁵ Tanya Basu: The Metaverse Has a Groping Problem Already. *MIT Technology Review*, 2021. december 16.

³⁶ Lásd ebben a tekintetben a privacy jogának alapjait megfogalmazó szerzőpáros tanulmányát: Louis D. Brandeis – Samuel D. Warren: The Right to Privacy. *Harvard Law Review*, 4. (1890), 5. 193–220.

³⁷ Kyle Orland: Meta Established 4-Foot 'Personal Boundary' to Deter VR Groping. *Ars Technica*, 2022. július 2.

G. Stanley Hallnak tulajdonítják ezt a felosztást, amely pontosan meg is határozta ezeket a határokat.³⁸ Hall is körülbelül 50 centiméteres távolságot jelölt meg az intim kör határaként.

Adatbiztonsági kockázatok és megfontolások

A metaverzumot ebben a tanulmányban új technológiaként írjuk le. Amint láttuk, sok tekintetben nem teljesen új, hanem a már létező technológiák újszerű kombinációjaként is leírható. Ennek megfelelően számos adatbiztonsági kockázat nem teljesen ismeretlen, így a felhasználó azonosításához kapcsolódó kockázatok, az identitáslopás, a megtévesztő megszemélyesítéssel járó visszaélések, az avatar azonosításához kötődő visszaélések olyan jelenségek, amelyek a metaverzum nélkül is felmerülnek.

Közelebb a felhasználóhoz

A metaverzum olyan mértékű adatgyűjtést és adatkezelést vetít előre, amely minden korábbi felhasználói környezet adatigényét felülmúlja. Kézenfekvőnek tűnik a felhőszolgáltatások igénybevétele, amelyek rugalmas háttérrel biztosítanak az új virtuális világ fenntartásához. A hatalmas mennyiségű és adott esetben érzékeny információ felhőben való tárolásának jelentős kockázatai vannak. Az adatok felhasználói eszközökön való tárolása mind biztonsági, mind magánszféra-védelmi megfontolásokból helyesebb választás lenne.³⁹ Így például a szem mozgására vagy a testmozgásra vonatkozó adatok nem a felhőben, hanem a felhasználó eszközén lennének elérhetők. Ilyen módon elejét lehetne venni az incidensekből fakadó problémáknak, továbbá az adatokkal való egyéb visszaéléseknek.

Jogtalan hozzáférés az adatokhoz

Bár az adattakarékosság elvét az adatkezelőre vonatkozó kötelezettséggént tartjuk számon, a felhasználó szempontjából is van jelentősége.⁴⁰ A felhasználó úgy tudja a lehetséges kockázatokat csökkenteni, ha valóban a szükségesre szorítja

³⁸ Wang et al. (2022): i. m. 18. Négy fizikai távolságot azonosított: a nyilvános térben 3,5–7,5 métert, a társasági térben 125–350 centimétert, a személyes körben 50–125 centimétert, míg az intim terület határát 50 centiméteres távolságban.

³⁹ Az úgynevezett *edge computing* gyakorlatilag a felhasználóhoz lehető legközelebbi adatfeldolgozást jelenti, amelynek adatbiztonsági mellett üzleti előnyei is kiaknázzhatók.

⁴⁰ A GDPR 5. cikk (1) bekezdés c) pontja szerint a kezelt személyes adatoknak az adatkezelés céljai szempontjából megfelelőeknek és relevánsnak kell lenniük, és a szükségesre kell korlátozódniuk.

az internethasználatot, valamint az annak során feltárt információkat. Ez a megállapítás nem új, de az új technológia vizsgálatakor mégis új jelentőséggel bővül a tartalma.

A virtuális világban nem mindent és mindenkit képes észlelni a felhasználó. Előfordulhat, hogy egy álcázott formában megjelenő felhasználó (avatár) megfigyeli a felhasználó magatartását vagy egy csoport magatartását. Az is lehetséges, hogy a való életről megfélelmett felhasználó fizikai közelségében lévő másik személy képes a beszélgetést, kommunikációt kihallgatni. Az első esetben megoldást nyújthat, ha több avatárt készít a felhasználó, és a rosszindulatú kémkedőkkel szemben megtévesztő stratégiát alkalmaz.⁴¹ Ami a fizikai életben való biztonságot illeti, ott arra kell figyelmeztetni, hogy a teljes belemerülést kínáló metaverzum használatának helyét jól meg kell tervezni, és az illetékteleneket fizikailag is ki kell zárni onnan.

Összegzés

A metaverzum egy sok tekintetben futurisztikus és lenyűgöző virtuális világot kínál, amelyben a felhasználó újszerű módon lesz képes feloldódni a digitális környezetben. A fenti elemzésben arra jutottunk, hogy az új technológia csak részben vet fel újszerű adatvédelmi kérdéseket. A magánszférát érintő szempontokon túl néhány olyan kérdést is elemeztünk röviden, amelyek csupán illusztrációi a metaverzumot, valamint általában az internethasználatot érintő társadalmi kérdések sokaságának.

A metaverzum előképei már léteznek, a virtuális valóságban zajló játékok tapasztalatai sok mindent előrevetítenek abból, ami a metaverzumot a jövőben jellemezni fogja. Az új virtuális közeg semmiképpen sem lesz jogon kívüli terület, ott sok más követelmény mellett az adatvédelmi szabályozás is érvényesítendő lesz. A metaverzum a magánszférát sok szempontból érinteni fogja. Az avatárokhöz kapcsolódó adatokat személyes adatnak kell tekinteni, amelyek védelme érdekében intézkedéseket kell majd tenni. Különös jelentősége lesz a *privacy by design* elvnek a rendszer tervezése során.

Az adatkezelők várhatóan sok esetben osztozni fognak az adatkezelői felelőségen más adatkezelőkkel, és a közös adatkezelői minőség minden bizonnyal számos üzleti modellben érvényesülni fog. Az adatalanyok önkéntelenül is sok személyes adatot fognak feltárni magukról a metaverzumban. Az ilyen adatok kezelését a lehető legszűkebbre kell visszaszorítani, így a különleges adatkategóriába tartozó adatokét, vagy például a felhasználók érzelmi reakcióit leíró adatokat.

Ahhoz, hogy a metaverzumban a magánszféra megőrizhető legyen, a tervezés során védelmi funkciókat kell beépíteni. Ilyen a fizikai távolságot szimuláló funkció,

⁴¹ Lik-Hang Lee et al.: *All One Needs to Know about Metaverse: A Complete Survey on Technological Singularity, Virtual Ecosystem, and Research Agenda*. (2021).

de sok más intézkedést kell elérhetővé tenni, például a mások figyelmé előli elvonulásra lehetőséget adó megoldásokat.

A klasszikus adatbiztonsági problémák a metaverzumban is jelen lesznek. A hozzáféréskontroll érzékeny kérdéseket vet fel, hiszen a biometrikus azonosítók adott esetben magasabb biztonságot képviselhetnek, míg a kezelésük önmagában is magas kockázatúnak tekintendő. Az idő mutatja majd meg, hogy a felhasználók e tekintetben milyen megoldásokat részesítenek előnyben.

A tanulmány fontos kérdéseket vetett fel, és mutatott be néhányat vázlatosan. Más következtetést nem tudunk levonni, mint hogy a metaverzum jogi és magánszféra-védelmi kérdései terén számos további kutatásra lesz szükség a társadalmi hatások pontos feltérképezéséhez.

Felhasznált irodalom

- Bányai Fanni – Zsila Ágnes – Demetrovics Zsolt – Király Orsolya: A problémás videojáték-használat újabb elméleti és gyakorlati megközelítései. *Információs Társadalom*, 18. (2018), 1. 93–106. Online: <https://doi.org/10.22503/infars.XVIII.2018.1.6>
- Basu, Tanya: The Metaverse Has a Groping Problem Already. *MIT Technology Review*, 2021. december 16. Online: www.technologyreview.com/2021/12/16/1042516/the-metaverse-has-a-groping-problem/
- Brandeis, Louis D. – Samuel D. Warren: The Right to Privacy. *Harvard Law Review*, 4. (1890), 5. 193–220. Online: <https://doi.org/10.2307/1321160>
- Lanier, Jaron: *You Are Not a Gadget*. London, Penguin Books, 2011.
- Leenes, Ronald: Privacy in the Metaverse. Regulating a Complex Social Construct in a Virtual World. In Simone Fischer-Hübner – Penny Duquenoy – Albin Zuccato – Leonardo Martucci (szerk.): *The Future of Identity in the Information Society*. Boston, MA, Springer, 2008. 95–112. Online: https://doi.org/10.1007/978-0-387-79026-8_7
- Lee, Lik-Hang – Tristan Braud – Pengyuan Zhou – Lin Wang – Dianlei Xu – Zijun Lin – Abhishek Kumar – Carlos Bermejo – Pan Hui: *All One Needs to Know about Metaverse: A Complete Survey on Technological Singularity, Virtual Ecosystem, and Research Agenda*. 2021. Online: <http://doi.org/10.13140/RG.2.2.11200.05124/8>
- Orland, Kyle: Meta Established 4-foot ‘Personal Boundary’ to Deter VR Groping. *Ars Technica*, 2022. július 2. Online: <https://arstechnica.com/gaming/2022/02/meta-establishes-four-foot-personal-boundary-to-deter-vr-groping/>
- Péterfalvi Attila – Révész Balázs – Buzás Péter (szerk.): *Magyarázat a GDPR-ról*. Budapest, Wolters Kluwer Hungary, 2018.
- Reyna, Ana – Cristian Martín – Jaime Chen – Enrique Soler – Manuel Díaz: On Blockchain and its Integration with IoT. Challenges and Opportunities. *Future Generation Computer Systems*, 88. (2018). 173–190. Online: <https://doi.org/10.1016/j.future.2018.05.046>
- Sinha, Disha: Top 10 Companies Working on Metaverse and Its Development in 2022. *Analytics Inside*, 2022. február 19. Online: www.analyticsinsight.net/top-10-companies-working-on-metaverse-and-its-developments-in-2022/
- Szabó Endre Győző: *A védelmi lépcső elmélete*. Budapest, Ludovika Egyetemi Kiadó, 2022.

- Szabó Endre Győző – Bojnár Katinka – Buzás Péter: Új globális technológiák kihívásai a magyar jogban. In Tóth András (szerk.): *Technológia jog*. Budapest, Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, 2016. 51–97.
- Szolin, Kim – Darija J. Kuss – Filip M. Nuyens – Mark D. Griffiths: “I Am the Character, the Character Is Me”: A Thematic Analysis of the User-Avatar Relationship in Videogames. *Computers in Human Behaviour*, 143. (2023). Online: <http://dx.doi.org/10.1016/j.chb.2023.107694>
- Westin, Alan F. (szerk.): *Information Technology in a Democracy*. Cambridge, MA, Harvard University Press, 1971.
- Wang, Yuntao – Zhou Su – Ning Zhang – Rui Xing – Dongxiao Liu – Tom H. Luan – Xuemin Shen: *A Survey on Metaverse: Fundamentals, Security, and Privacy*. 2022. Online: <https://doi.org/10.48550/arXiv.2203.02662>

Intézményi dokumentumok

- European Data Protection Supervisor: *Tech Sonar 2022–23 report*. Online: https://edps.europa.eu/system/files/2022-11/22-11-10_techsonar_report_22_23_en.pdf
- European Data Protection Supervisor: *Metaverse*. Online: https://edps.europa.eu/press-publications/publications/techsonar/metaverse_en

Online források

- GDPR Hub. Online: https://gdprhub.eu/index.php?title=BVwG_-_W258_2227269-1/14E
- Snow Crash Summary and Study Guide. *SuperSummary*. Online: www.supersummary.com/snow-crash/summary/
- Neal Stephenson on the Future of the Metaverse. *YouTube*. Online: www.youtube.com/watch?app=desktop&v=60u9L5-YO9Q
- Próteusz. *Arcanum*. Online: www.arcanum.com/hu/online-kiadvanyok/Lexikonok-ki-kicsoda-az-antik-mitoszokban-F869D/p-F8BBC/proteusz-F8C7E/
- Proteus effect. *Tech Target*. Online: www.techtarget.com/whatis/definition/Proteus-effect#:~:text=The%20Proteus%20effect%20is%20the,accordance%20with%20their%20digital%20representatives
- Metaverse. *European Data Protection Supervisor*. Online: https://edps.europa.eu/press-publications/publications/techsonar/metaverse_en
- Avatar. *Britannica*. Online: www.britannica.com/topic/avatar-Hinduism
- The Metaverse and How We'll Build It Together – Connect 2021. *YouTube*. Online: www.youtube.com/watch?v=Uvufun6xer8
- Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement. Online: https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf
- Learning to Deal with Problematic Usage of the Internet. *COST – European Cooperation in Science and Technology*. Online: www.cost.eu/publication/learning-to-deal-with-problematic-usage-of-the-internet/

Vákát

IV. rész

Műveletek a kibertérben



Vákát

Sorbán Kinga

Hacktivizmus a demokráciában – bűncselekmény vagy politikai véleménynyilvánítás?



A hacktivizmus a „hackelés” és az „aktivizmus” szavak összevonásából keletkezett neologizmus, amelynek társadalmi megítélése napjainkban igen szélsőséges skálán mozog. Az elmúlt időszakról kifejezetten elmondható, hogy össztársadalmi szinten növekedett a hackerek támogatottsága, amihez több esemény együttese járult hozzá, köztük a radikális információszabadság iránti igény és az orosz–ukrán háború kibertérben megvalósuló cselekményei. Tanulmányom arra kíván választ adni, hogy a jogtudomány szempontjából nézve mi a hacktivizmus: a politikai véleménynyilvánítás egyik formája vagy elítélendő, pönalizálandó cselekmény? Ennek érdekében igyekszem csoportosítani azokat a magatartásokat, amelyek e körbe tartozhatnak, kitérve az online aktivizmus szerepére a politikai véleményformálásban és a kiberterrorizmus szerepére.

Bevezetés

Az internet lehetőségek garmadáját kínálja az emberek számára, hogy kifejezhessék véleményüket. A véleménynyilvánítás az online térben többnyire teljesen ártalmatlan, vannak azonban olyan megnyilvánulások, amelyek nemcsak a közösség morális alapon nyugvó ellenszenvét, hanem akár büntetőjogi szankciót vonhatnak maguk után. Ha a büntetőjog által szankcionált véleménynyilvánításokra gondolunk, akkor többnyire olyan deliktumok sejlenek fel előttünk, mint a gyűlöletbeszéd vagy a becsületsértés. Van azonban az online véleménynyilvánításnak egy olyan formája, amellyel idáig keveset foglalkozott a jogtudomány, az orosz–ukrán háború nyomán azonban – ahogy sok egyéb magatartás – előtérbe került. Ez a magatartás a *hacktivizmus*, amely a „hackelés” és az „aktivizmus” szavak összevonásából keletkezett neologizmus. Sokak szerint ez az első olyan háború, amelynek az egyik jelentős frontja a virtuális térben húzódik, nap mint nap hallunk híreket meghackelt orosz kémműholdakról,¹ vagy olyan oroszországi éttermekről, amelyek Google Maps-profilján az értékelők ukrán városokról készült fényképekkel igyekeznek felhívni a lakosok figyelmét az Ukrajnában zajló eseményekre.² Noha mindkét esetben a hacktivizmus kifejezést használjuk, érezzük, hogy egy másik állam tulajdonában

¹ Az Anonymous azt állítja, meghackelték az orosz kémműholdakat. *HVG.hu*, 2022. március 3.

² Takács Petra: A Google Mapsen több ezer „értékeléssel” figyelmeztetik az orosz népet. *Liner.hu*, 2022. március 4.

lévő katonai műhold feltörése nem ugyanolyan súlyú magatartás, mint fényképeket közzétenni egy étterem internetes profilján.

Tanulmányom arra kíván választ adni, hogy a jogtudomány szempontjából nézve mi a hacktivizmus: a politikai véleménynyilvánítás egyik formája vagy elítélendő, pönalizálandó cselekmény? Ennek érdekében igyekszem csoportosítani azokat a magatartásokat, amelyek e körbe tartozhatnak, illetve kitérek az online aktivizmus szerepére a politikai véleményformálásban.

A hacktivizmus társadalmi megítélése és megjelenési formái

A hacktivizmus társadalmi megítélését nem annyira az e csoportba tartozó magatartások szabályozottsága befolyásolja, hanem inkább az állami intézményrendszerbe és a jogrendszerbe vetett állampolgári bizalom.³ Giovanni A. Travaglino egyik tanulmányában kifejti, hogy azok az egyének, akik igazságtalannak tartják a rendszer működését, ám politikailag kevésbé hatékonyak, a dühüket gyakran úgy fejezik ki, hogy olyan személyeket vagy szervezeteket támogatnak, akiknek a magatartása megzavarja a rendszert.⁴ Szemben a politikailag hatékony csoportok szereplőivel, akik közvetlenül és a fizikai térben nyilvánulnak meg – a szerző ilyennek tartja az Arab Tavasz vagy az Occupy Wall Street résztvevőit –, a politikailag nem hatékony egyének alternatív módját választják az ellenállásnak, például az olyan hackercsoportok, mint az Anonymous támogatását.⁵

Az elmúlt időszakról kifejezetten elmondható, hogy össztársadalmi szinten növekedett a hackerek támogatottsága, amihez több esemény együttese járult hozzá. Jessica L. Beyer a hacktivizmus erősödő támogatottsága egyik okaként a radikális információszabadság iránti igényt nevesíti.⁶ Az olyan platformok, mint a kiszivároztatott, gyakran érzékeny állami információkat közzétevő WikiLeaks, éppen azért váltak népszerűvé, mert az állami működés hagyományosan átláthatatlan, az információszabadság hagyományos értelmezésében elzárt területeire engedtek betekintést.

A hackerek támogatottsága növekedésének kedvezett az Oroszország és Ukrajna között kitört háború is, amihez nagyban hozzájárult Ukrajna háborús kommunikációja. Az ukrán digitális fejlesztési miniszter már a háború elején bejelentette, hogy önkéntes kiberhadsereget toboroznak, amelynek bárki a részese lehet, akár

³ Leanna Ireland: We Are All (Not) Anonymous: Individual- and Country-Level Correlates of Support for and Opposition to Hacktivism. *New Media & Society*, (2022). 1.

⁴ Giovanni A Travaglino: Support for Anonymous as Vicarious Dissent: Testing the Social Banditry Framework. *Group Processes & Intergroup Relations*, 22. (2019), 2. 163–181.

⁵ Travaglino (2019): i. m.

⁶ Jessica L. Beyer: The Emergence of a Freedom of Information Movement: Anonymous, WikiLeaks, the Pirate Party, and Iceland. *Journal of Computer-Mediated Communication*, 19. (2014), 2. 141–154.

hackerként, akár olyan „civilként”, akinek a számítógépét a DDoS-támadásokban botként felhasználhatják.⁷ A kezdeményezéshez sokan csatlakoztak, mivel úgy érezték, hogy ezzel is tudnak tenni valamit Ukrajna megsegítése érdekében.

A közvéleménnyel szemben biztonsági szakértők kimondottan óva intenek a hackercsoportok támogatásától, érveik között gyakran elhangzik, hogy a legtöbb ország büntetni rendeli a hacktivisták eszköztárába tartozó tevékenységeket.

Mivel a hacktivizmus kifejezést főleg a köznyelvben használjuk, vagyis nem egy egzakt jogtudományi fogalom, jogi megítélése nagyon sokféle lehet. Az alábbiakban a hacktivizmus legjellemzőbb megjelenési formáit csoportosítom, elsősorban három fogalom elhatárolásával. A hacktivizmustól el kell választanunk az ahhoz nagyon hasonló, de megítélésükben sokszor erőteljesen különböző egyéb cselekményeket, az online aktivizmust, vagy más néven kiberaktivizmust, valamint a kiberterrorizmust. Az elhatárolás, mint látjuk, nem mindig mentes a nehézségektől, hiszen sokszor ezek a tevékenységek összeérnek, nem lehet élesen megkülönböztetni őket egymástól.

A kiberaktivizmus

2015. február 19-én az Európai Gazdasági és Szociális Bizottság (EGSZB) úgy határozott, hogy saját kezdeményezésű véleményt dolgoz ki a kiberaktivistákról és civil társadalmi szervezetekről. A kiberaktivizmust a dokumentum az aktivizmus egyik formájaként definiálja, mégpedig olyan formájaként, amely „ösztönzi a politikai, környezeti, társadalmi, állampolgári, kulturális stb. ügyek militáns felvállalását, és ehhez nincs szüksége meghatározott ideológiákban, hierarchiákban vagy programokban megtestesülő előzményekre, és amely olyan technológiai eszközöket használ, amelyek lehetővé teszik az információ gyors terjedését és a részvétel »járványszerű« bővülését”.⁸ A kiberaktivizmus, vagy más néven online aktivizmus kizárólag jogszerű, a véleménynyilvánítás normális rendjébe illeszkedő cselekményeket takar, amelyek az új technológiákat kommunikációs csatornaként alkalmazva törekszenek a közvélemény befolyásolására. A fentebb hivatkozott EGSZB-vélemény az online aktivizmus eszközei között elsősorban nem destruktív internetes eszközöket sorol fel, úgymint:

- információkeresés;
- információt és dokumentumokat kínáló webhelyek építése;
- elektronikus kiadványok közreadása;

⁷ Matt Burgess: Ukraine’s Volunteer ‘IT Army’ Is Hacking in Uncharted Territory. *Wired*, 2022. február 27.

⁸ Európai Gazdasági és Szociális Bizottság: Az Európai Gazdasági és Szociális Bizottság véleménye – Kiberaktivisták és civil társadalmi szervezetek (saját kezdeményezésű vélemény). C 13/116 (2016. január 15.). 1.1.

- virtuális közösségek létesítése;
- vitafórumok létrehozása;
- közösségi akciók tervezése, hirdetése, cselekvések összehangolása.⁹

A kiberterrorizmus

A kiberterrorizmus fogalmának meghatározásakor az egyik nehézség, amellyel szembe kell néznünk, hogy mind a „kibertér”, mint a „terrorizmus” fogalmának többféle meghatározása létezik. Jelen tanulmányban a kiberterrorizmuson azokat az információs rendszerek és hálózatok felhasználásával elkövetett erőszakos cselekményeket értem, amelyek valamely állam ellen irányulnak, és halálhoz, sérüléshez, vagyontárgy súlyos károsodásához vagy a társadalmi rend megzavarásához vezetnek. Tipikusan ilyennek minősülnek a kritikus infrastruktúrák, például erőművek elleni támadások. Dornfeld László a kiberbűnözés egyik fajtájaként tekint a kiberterrorizmusra, ugyanakkor elválasztja azt a kiberhadviseléstől.¹⁰ Kifejti, hogy a kiberhadviselés hadtudományi fogalom, végrehajtói államok, kiberterrorizmust ellenben bármilyen államtól független szervezet elkövethet.¹¹

A hacktivizmus

A hacktivizmus valahol a kiberaktivizmus és a kiberterrorizmus között helyezkedik el. A hacktivisták alapvető jellemzője, hogy a hackerek eszköztárát használják annak érdekében, hogy valamilyen társadalmi, politikai célt érjenek el. Gyakori motivációjuk az internetes szólás- és információszabadság biztosítása, valamint az internetes polgári engedetlenség. A hacktivisták csoportok kommunikációit és kiáltványait megfigyelve látható, hogy a szerveződések üzeneteinek egyik kulcspontja a moralitás és az igazság keresése. Fehér Katalin rámutat, hogy ez a morál a jogi szabályozással gyakran szembemenő, olyan univerzális morál, amely globálisan is érvényesíthető.¹² Ennek az univerzális morálfelfogásnak köszönhető, hogy az egyes hacktivisták csoportok működése nem korlátozódik egy-egy országon belülre, az igazságtalanság és a „hatalmasoknak” visszavágás narratíváján keresztül könnyedén megszólíthatók azok a támogatók is, akik az egyes konkrét ügyekben viszonylag kevésbé érdekeltek,

⁹ Európai Gazdasági és Szociális Bizottság (2016): i. m. 3.4.

¹⁰ Dornfeld László: Kiberterrorizmus – a jövő terrorizmusa? In Mezei Kitti (szerk.): *A bűnügyi tudományok és az informatika*. Pécs–Budapest, Pécsi Tudományegyetem Állam- és Jogtudományi Kar – MTA Társadalomtudományi Kutatóközpont, 2019. 18.

¹¹ Dorothy E. Denning: Activism, Hacktivism, and Cyberterrorism: The Internet As a Tool for Influencing Foreign Policy. In John Arquilla – David Ronfeldt (szerk.): *Networks and Netwars. The Future of Terror, Crime, and Militancy*. Santa Monica, RAND Corporation, 2001. 239–288.

¹² Fehér Katalin: *Digitalizáció és új média*. Budapest, Akadémiai Kiadó, 2017.

ám hajlandóak szolidaritást vállalni akár más országok polgáraival is. A kiberaktivizmustól elsősorban az különbözteti meg, hogy míg az előbbi legális eszközökre épít a figyelemfelhívás érdekében, a hacktivisták által alkalmazott megoldások a legtöbb jogrendszerben jogsértőnek, de legalábbis jogilag aggályosnak minősülnek. A hacktivizmus körébe tartozó magatartások ugyanakkor jellemzően nem eredményeznek súlyos kárt, vagyis a kiberterrorizmus súlyosságát nem érik el. Illig szerint a hacktivizmus művelői kifejezetten elkötelezettek az erőszakmentesség mellett,¹³ tevékenységükben tehát sokkal inkább a figyelemfelhívás dominál, köszönhetően annak, hogy akcióik általában nagy médiafigyelmet kapnak. Denning úgy látja, hogy a hacktivizmus leggyakoribb megjelenési formái az alábbiak:

- virtuális tüntetések (*virtual sit-in*);
- weboldalak megrongálása (*defacing*);
- weboldalak tükrözése (*website mirroring*);
- érzékeny, jogosulatlanul megszerzett információk nyilvánosságra hozatala (*doxing*);
- DDoS támadások;
- spamek.

Virtuális tüntetések esetében több ezer hacktivistát látogat meg egy weboldalt, olyan forgalmat generálva, amelyet nem tud kezelni a rendszer, és összeomlik. Legelőször 1995-ben került rá sor, amikor a magát Strano Networknek nevező csoport úgy demonstrált a francia kormányzat nukleáris politikája ellen, hogy támogatóikat arra kérték, hogy egy meghatározott egyórás időtartamban keressenek fel francia kormányzati weboldalakat.¹⁴

A weboldalak megrongálása (*defacing*) során az oldal valamely sérülékenységet kihasználva a hacktivisták hozzáférnek annak forráskódjához, és különböző változtatásokat eszközölnek az eredeti portálon. Weboldalrongálásra hazai példa is van, az Anonymous hackercsoport magyarországi csoportja 2012-ben átírta az Alkotmánybíróság honlapján az Alaptörvény szövegét.¹⁵ A weboldalak tükrözése szintén az eredeti oldal valamely sérülékenységeinek kihasználásával történik, ahelyett azonban, hogy az oldalt megváltoztatnák, a domaint átirányítják egy másik címre, amely gyakran az eredeti oldal módosított változata.

A *doxing* motivációja jellemzően az, hogy a hacktivisták az állami működés átláthatatlan rétegeibe engedjenek bepillantást. A kiszivárogtatott információk érinthetnek egy-egy társadalmilag érzékeny témakört vagy konkrét személyeket, de célja lehet általánosságban a minősített adatok körébe tartozó információk közzététele is.

¹³ Andrew T. Illig: Computer Age Protesting: Why Hacktivism is a Viable Option for Modern Social Activists. *Dickinson Law Review*, 119. (2015), 4. 1035–1036.

¹⁴ Denning (2001): i. m. 264.

¹⁵ Az Anonymous átírta az alaptörvényt. *Index*, 2012. március 4.

Hiába az a célja ezeknek a magatartásoknak, hogy közérdekű ügyekkel kapcsolatos véleményt fejezzenek ki, radikális módszereik olyan érdekeket sértenek, amelyek miatt a demokratikus társadalmakban korlátozás alá vonhatók. Az Emberi jogok európai egyezményének 10. cikke a szólásszabadság legitim korlátai között említi a nemzetbiztonságot, a közbiztonságot, a bűnüldözési érdeket, valamint az egyének jogainak sérelmét; egy-egy információs rendszerbe való jogszerűtlen belépés és az abban végrehajtott adatmanipuláció, még ha csak figyelemfelkeltésre irányul is, egészen biztosan kockázatot jelent ezek valamelyikére. A hacktizmussal azonosított magatartásokra a magyar büntetőtörvény, a Büntető Törvénykönyvről szóló 2012. évi C. törvény (Btk.) rendelkezései egytől egyig kiterjednek. A következőkben a magyar büntetőjogi rendelkezéseket mutatom be, amelyek az információs rendszer és adatok elleni bűncselekményeket szabályozzák.

Információs rendszer és adatok elleni bűncselekmények a magyar büntetőjogban

A Btk. XLIII. fejezete szól a tiltott adatszerzésről, valamint az információs rendszer elleni bűncselekményekről, így az információs rendszer vagy adat megsértéséről, valamint az információs rendszer védelmét biztosító technikai intézkedés kijátszásáról. E rendelkezések 2004 óta képezik a magyar jog részét – Magyarország ekkor ratifikálta az Európa Tanács 2001. november 23-án Budapesten elfogadott, a számítástechnikai bűnözésről szóló egyezményét,¹⁶ aminek alapján kötelezettséget vállalt arra, hogy megalkotja a megfelelő jogszabályokat az egyezményben meghatározott cselekmények kriminalizálása érdekében. A Btk. e szabályainak beiktatásával a magyar jogalkotó az uniós aktusok átültetésére vonatkozó kötelezettségének is eleget tett.

Az Európai Parlament és a Tanács 2013/40/EU irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról lényegében a Cybercrime-egyezménnyel azonos szabályokat fektet le. Az irányelv, sok egyéb európai uniós normához hasonlóan, a *minimumharmonizáció* elvét követi, vagyis a tagállamok annak szabályainál részletesebb, illetve szigorúbb szabályokat szabadon megállapíthatnak.

Az információs rendszer vagy adat megsértése tényállásáról a Btk. 423. §-a rendelkezik. Az e szakasz által kriminalizált elkövetési magatartások köznyelvi elnevezése általában sokkal beszédesebb – ezek a bekezdések szabályozzák a hackelést, a kártékony szoftverek, például vírusok terjesztését, a botnetworkok kiépítését és a túlterheléses támadásokat.

¹⁶ Az egyezményt Magyarországon az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről szóló 2004. évi LXXIX. törvény hirdette ki.

423. § (1) Aki információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve vagy azt megsértve bent marad, vétség miatt két évig terjedő szabadságvesztéssel büntetendő.

(2) Aki

- a) az információs rendszer működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza, vagy
 - b) információs rendszerben lévő adatot jogosulatlanul vagy jogosultsága kereteit megsértve megváltoztat, töröl vagy hozzáférhetetlenné tesz,
- büntett miatt három évig terjedő szabadságvesztéssel büntetendő.

(3) A büntetés büntett miatt egy évtől öt évig terjedő szabadságvesztés, ha a (2) bekezdésben meghatározott bűncselekmény jelentős számú információs rendszert érint.

(4) A büntetés két évtől nyolc évig terjedő szabadságvesztés, ha a bűncselekményt közérdekű üzem ellen követik el.

(5) E § alkalmazásában adat: információs rendszerben tárolt, kezelt, feldolgozott vagy továbbított tények, információk vagy fogalmak minden olyan formában való megjelenése, amely információs rendszer általi feldolgozásra alkalmas, ideértve azon programot is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja.

A Btk. 423. §-a által szabályozott tényállás valójában háromféle elkövetési magatartással is megvalósítható, ezek:

- az információs rendszerbe történő jogosulatlan belépés [(1) bekezdés];
- a rendszer működésének akadályozása [(2) bekezdés a) pontja]; valamint
- az információs rendszerben tárolt adatokkal végzett jogosulatlan műveletek [(2) bekezdés b) pontja].

E bekezdés szövegén látszik, hogy a technológiasemlegesség jegyében fogalmazták meg, így az alkalmazott technológiától és az elkövetés módszerétől függetlenül büntetendő minden olyan magatartás, amely a meghatározott eredményre vezet.

A 9/2012. számú büntető elvi döntés szerint „a védett jogi tárgy a számítástechnikai rendszerek működéséhez, a bennük tárolt, feldolgozott, továbbított adatok megbízhatóságához, valamint titokban maradásához fűződő érdek, és nem magának a számítógépnek vagy gépeknek a mechanikus védelme, erre ugyanis a rongálás törvényi tényállása nyújt büntetőjogi védelmet”. A védett jogi tárgy jogosulatlan belépés és az információs rendszer működésének akadályozása esetén az elektronikus adatfeldolgozó és adatátviteli rendszer integritása, biztonsága, míg az adatokkal való visszaélés esetében az adatok által megtestesített érték, érdek. A bűncselekmény elkövetési tárgya az információs rendszer, amelynek fogalmát a Btk. 459. szakasz (1) bekezdésének 15. pontja pontosan meghatározza. Eszerint „információs rendszer:

az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezés, vagy az egymással kapcsolatban lévő ilyen berendezések összessége”.

„Az információs rendszer fogalma nemcsak az egyes berendezésekre terjed ki, hanem felöleli az azok összekapcsolása révén létrejött hálózatot, valamint az adattovábbítást, a kapcsolatfelvételt biztosító műszaki berendezéseket is. A berendezések közötti kapcsolat nem jelent feltétlenül fizikai összekapcsoltságot. Az információs rendszerek közötti összeköttetés létrejöhet elektronikus vagy optikai jeleket továbbító kábelek, vagy vezetékek útján, valamint rádióhullámok, infravörös, illetőleg rövidhullámok segítségével, vagy műholdas sugárzás igénybevételével is.”¹⁷

Jogosulatlan belépés, bent maradás és a belépési jogosultság túllépése vagy kijátszása

Az I. alapeset, amely az (1) bekezdésben jelenik meg, a valamely hálózatba vagy számítógépbe történő jogosulatlan belépés, illetve jogosulatlan bent maradás. Nagy Zoltán András részletesen foglalkozik azzal, hogy mikor jogellenes a hálózatba való belépés vagy bent maradás.¹⁸

Ha a számítógépbe az elkövető nem jogosult belépni, és a számítógép olyan biztonsági mechanizmusokkal védett, amelyek csak meghatározott személyek számára engedélyeznek belépést, valamint ezek a mechanizmusok aktiválva is vannak az elkövetés idején, a belépés vagy bent maradás jogellenes. Jogosultság nélkül lép be a felhasználó abban az esetben is, ha nem a számára engedélyezett belépési ponton lép be (például a munkahelye helyett az otthonában), a számítógép vagy hálózat biztonsági rendszere megoldásait kihasználva lép be, illetőleg más felhasználó nevével, jelszavával lép be. A magatartás csak abban az esetben tényállásszerű, ha arra az információs rendszer védelmét szolgáló intézkedések megsértésével, kijátszásával kerül sor. A jogszabály nem követeli meg, hogy a védelmet megvalósító biztonsági intézkedések műszaki-technikai jellegűek legyenek, azok elvileg lehetnek testi, személyi jellegűek is, ez esetben, ha az elkövető az előbbi adatokat erőszak vagy fenyegetés alkalmazásával szerzi meg, más bűncselekmény (kényszerítés, zsarolás) is megvalósulhat. A belépéshez szükséges adatok megszerzésének egyik elterjedt módszere, ahogyan arra Mezei Kitti is rámutat, a pszichológiai manipuláció, az úgynevezett *social engineering*.¹⁹

¹⁷ Görgényi Ilona et al.: *Magyar büntetőjog különös rész.* Budapest, Wolters Kluwer, 2020. XLIII. fejezet. Tiltott adatszérés és az információs rendszer elleni bűncselekmények.

¹⁸ Nagy Zoltán András: A számítógépes bűnözés története. In Dobák Imre – Hautzinger Zoltán (szerk.): *Szakmaiság, szerénység, szorgalom. Ünnepi kötet a 65 éves Boda József tiszteletére.* Budapest, Dialóg Campus Kiadó, 2018. 473–474.

¹⁹ Mezei Kitti: A jogosulatlan belépés, avagy a hacking szabályozása a büntetőjogban. *Rendőrségi Tanulmányok*, 3. (2020), 2. 32.

A jogosulatlan belépést valósítja meg a hackerek tevékenysége is, akik informatikai ismeretek, módszerek segítségével lépnek be különféle rendszerekbe. Az összes ilyen módszert nyilvánvalóan célszerűtlen lenne felsorolni, az információs rendszerek sokfélesége és összetettsége miatt pedig vélhetően lehetetlen volna mindenre teljes körű listát állítani, ezért az alábbiakban csak néhány fontosabb módszert emelünk ki. Népszerű módszerek a puffertúlterhelés (*buffer overflow*) vagy a „nyers erő” (*brute force*) módszer. Előbbi „alapját programozási hiányosságok képezik, konkrétan a bevitt adatokat tároló pufferek mérete nem megfelelően meghatározott. Ha nincs rendesen kezelve az adatbevitel, a támadó túlírhatja a puffert, és a program adatterületén továbbírva a program visszatérési értékét egy tetszőleges helyre irányíthatja. Jellemzően olyanra, mely részére rendszergazdai jogosultságaival való élest tesz lehetővé, amennyiben a támadott program is ilyen jogokkal futott.”²⁰ A *brute force* módszer működésének lényege, hogy a rejtjelező rendszer ismeretében az összes lehetséges kulcsot kipróbálva határozza meg az alkalmazott jelszót, adatot. Mezei Kitti említést tesz az alap felhasználói műveletekkel, illetve a rendszergazdáéhoz hasonló jogosultságokkal rendelkező „*root level access*” vagy „*god level access*” hozzáférésekről is.²¹ Az információs rendszer feletti irányítás megszerzése gyakran úgy történik, hogy az elkövető rosszindulatú szoftvert juttat a célzott számítógépes rendszerbe, ezek azonban már olyan módszerek, amelyek a számítógép működését is akadályozzák, így a következő alapesetnek megfelelően ítélandók meg. A jogosulatlan belépés után végzett további műveletek esetében általánosságban elmondható, hogy ezek már a következő bekezdés valamelyik fordulatát valósítják meg.

Kritikája lehet a jogosulatlan belépést szabályozó szakasznak, hogy gyakorlatilag egy olyan cselekedetet rendel büntetni, amelynek társadalomra veszélyessége sok esetben igen csekélynek mondható. Főképp a fiatalok körében figyelhető meg az a tendencia, hogy azért törnek be rendszerekbe, hogy megmutassák, ők képesek rá, vagyis vannak annyira képzettek technikailag, hogy ki tudják játszani a rendszert védő mechanizmusokat mindenféle ártó szándék nélkül.

Itt kell szólni azokról az esetekről is, amikor a rendszerbe való belépés nem károkozásra irányul, de még csak nem is öncélú fitogtatása az informatikai ismereteknek, hanem valójában segítségnyújtási céllal történik. Az úgynevezett etikus hacking olyan tevékenység, amelynek során a hacker azért tör be bizonyos rendszerekbe, hogy azok sebezhető pontjait feltárja, az információkat pedig megossza a rendszer üzemeltetőjével a hibák kijavítása és a komolyabb, rosszindulatú támadások megelőzése végett. Az etikus hackerek gyakran egy-egy cég alkalmazottjaiként működnek, ez esetben a büntetőjogi felelősségük értelemszerűen fel sem merül, más esetekben azonban kívülállóként avatkoznak be a rendszer

²⁰ Varga Balázs: Informatikai bűncselekmények. *Jogi Fórum*, 2003. december 19. 36.

²¹ Mezei Kitti (2020): i. m. 24.

működésébe, ezt Szathmáry Zoltán kéréstlen sérülékenységvizsgálatnak nevezi.²² Noha e cselekmény önmagában véve tényállásszerűnek minősül, a társadalomra veszélyesség gyakorta hiányzik, sőt a sérülékenységek feltárása inkább a társadalom hasznára válik, amennyiben komolyabb károsodástól óvja meg az érintett cégeket és azok ügyfeleit. Mivel vékony a határmezsgye a bűncselekmény és a jó szándékú, de kéréstlen sérülékenységvizsgálat között, a jelenség semmiképpen nem maradhat szabályozási anomáliaként, a jelenlegi Btk.-beli szabályozás azonban túl szigorú, és nem feltétlenül szolgál társadalmi érdeket. A rosszindulatú hackerek számára szolgálhat a kódex e passzusa elrettentésül, azonban a fiatal informatikusok jövőjének derékba törése már nyilvánvalóan túlmutat a jogalkotó eredeti szándékán. Meglátásom szerint a probléma kezelhető jogalkotás révén, valamint a joggyakorlat finomhangolásával is a már létező jogszabályi kereteken belül. A bírói gyakorlat azzal tudná elősegíteni a helyzet megoldását, ha a bűncselekmény tárgyi oldali elemeinek megvalósulásán túl nagy hangsúlyt helyezne a motívumra és a célzatra, továbbá ha azonos elbánásban részesítené az azonos töről fakadó cselekményeket. Figyelemre méltó Ambrus István meglátása is, aki a panaszokról és a közérdekű bejelentésekről szóló 2013. évi CLXV. törvényre hivatkozva közérdekű bejelentésként kategorizálja az egyes, kéréstlen sérülékenységvizsgálattal összefüggő magatartásokat.²³ Álláspontja szerint az etikus hackerek bejelentése a feltárt problémáról a társadalom érdekét szolgáló, jogellenességet kizáró közérdekű bejelentésnek minősülhet. E minősítésnek azonban meg kell felelnie azoknak a feltételeknek, amelyek kimunkálása jelenleg is a joggyakorlatra vár, így például a hackerrel szembeni követelmény, hogy dokumentálja a cselekménye egyes lépéseit, haladéktalanul jelezze a feltárt sérülékenységet, és tevékenysége ne irányuljon haszonszerzésre.

A másik lehetőség az etikus hackerek tevékenységével kapcsolatos feszültségek feloldására a szabályozási út, vagyis az etikus hackerek tevékenységének *expressis verbis* dekriminalizálása. Mivel a kibertérben számtalan jogellenes belépés fordul elő, én a szabályozási választ tartom követendőnek, amely a joggyakorlat számára vezérfonalként szolgálva egységesen meghatározhatja a büntetőjogi felelősségre vonás alóli mentesülés szükséges feltételrendszerét is.

Belépési jogosultsága kereteinek túllépésével, illetőleg annak megsértésével marad benn az elkövető, ha van ugyan valamilyen szintű jogosultsága a rendszer használatára, azonban e jogosultságát meghaladó műveleteket folytat, vagy a számára engedélyezett idő lejártával nem lép ki a rendszerből. A bűncselekmény befejezett, amint a tettes az első hozzáférési korlátot átlépte, és számára az adatok vagy az adatfeldolgozó rendszer további lépései nyitva állnak.²⁴ A Kúria az egyik

²² Szathmáry Zoltán: Etikus és nem etikus hacking – a kéréstlen sérülékenységvizsgálat büntetőjogi kérdései. *Magyar Jog*, 67. (2020), 6. 340–346.

²³ Ambrus István: *Digitalizáció és büntetőjog*. Budapest, Wolters Kluwer, 2021. 87.

²⁴ Gelányi Anikó – Csepely-Knorr Tamás: A jogosulatlan wifi használat minősítése, avagy ha nyitva van az ajtó, akkor bemehetek? *Infokommunikáció és Jog*, 6. (2009), 34. 201–207.

ítéletében felhívta a figyelmet arra, hogy ahhoz, hogy a jogosultság keretein való túllépés bűncselekménynek minősüljön, szintén szükséges a rendszer védelmét biztosító technikai intézkedés megsértése vagy kijátszása, önmagában a jogosultság kereteinek túllépése „nem éri el azt a veszélyességi szintet, mint amit az első fordulat megkíván” (BH2017. 392.).

Az információs rendszer működésének akadályozása

Az információs rendszer működésének megzavarása történhet akár hardvereszközök (például különböző jelzavarók), akár szoftvereszközök révén.

Az információs rendszer rendeltetésszerű működésének akadályozására a modern technológia állása szerint különösen alkalmasak a különféle kártékony programok, ezért a 423. §-ban szabályozott cselekmény két legtipikusabb elkövetési magatartása a *malware*-, illetve a botnettámadás. Az 1978. évi Btk.²⁵ *Kommentárja* a számítástechnikai rendszer megsértésének egyik eszközeként a számítógépes vírusokat említi.²⁶ A számítógépes vírus azonban csak egyike azoknak a kártékony programoknak (*malware*), amelyek alkalmasak a számítógép működésének kedvezőtlen befolyásolására. A kártékony programok közös jellemzője, hogy olyan szoftverek, amelyek akadályozzák a számítógép működését, illetve korlátozzák a rendeltetésszerű használatát. A legismertebb *malware*-fajták az alábbiak:²⁷

- Vírus (*virus*): vírusnak nevezzük azokat a szoftvereket, amelyek képesek a felhasználó tudta nélkül egyik számítógépről a másikra, vagy akár ugyanazon a gépen belül több helyre észrevétlenül reprodukálódni. Általában fertőzött program segítségével terjednek. A programvírusok (*file-infector virus*) bináris futtatható (például exe) fájlokba ágyazódnak. Gyakran találhozhatunk mostanában az úgynevezett zsarolóvírusokkal (*ransomware*), amelyek a rendszert megfertőzve állományokat titkosítanak, és csak akkor adják meg a feloldáshoz szükséges kódot, ha a felhasználó egy megadott számlaszámra váltságdíjat utalt. A zsarolóvírusok egyre gyakrabban jelennek meg Magyarországon is, ahol magánszemélyek mellett főként cégek, illetve kritikus infrastruktúrák (például kórházi rendszerek) válnak áldozatul. Adatfájlokban lévő vírusok például a makrovírusok, valamint az érvénytelen fájlformátumot kihasználó vírusok.
- Féreg (*worm*): a féreg olyan önmagában működő szoftver, amely képes önmagát reprodukálva egyik számítógépről a másikra terjedni. Abban

²⁵ 1978. évi IV. törvény a Büntető Törvénykönyvről.

²⁶ Varga Zoltán (szerk.): *Nagykommentár a Büntető törvénykönyvről szóló 1978. évi IV. törvényhez*. Budapest, KJK-Kerszöv, 2004.

²⁷ A csoportosítás és a fogalommagyarázat a https://nki.gov.hu/it-biztonsag/kiadvanyok/szorolapok/felhasznalasaval_keszult.

- különbözik a vírustól, hogy önmagában is működik és életképes, nem kapcsolódik egyéb szoftverekhez. Az önsokszorosításon kívül a féreg számtalan dologra programozható – ezeknek a másodlagos funkcióknak a neve *payload*.
- Trójai faló (*trojan horse*): trójai szoftvereknek nevezzük azokat a kártékony szoftvereket, amelyek magukat általában ártalmatlan vagy segítő célú szoftvernek álcázva települnek fel a számítógépre. Hasonlóan a számítógépes férgekhez, a rendszerbe kerülésüket követően számtalan dologra programozhatók, például a számítógépen található állományok titkosítására, zombiszámítógép létrehozására, személyes adatok összegyűjtésére és elküldésére, a felhasználó webkamerájának használatára, az operációs rendszer távoli használatára stb.
 - *Rootkit*: olyan szoftvereszközök, amelyek elrejtenek egyes folyamatokat vagy adatokat az operációs rendszerben, vagy hozzáférést tesznek lehetővé bizonyos alrendszerekhez vagy programokhoz.
 - Hátsó ajtó (*backdoor*): olyan program, amely a felhasználó tudta nélkül távoli hozzáférést tesz lehetővé. Ezek a programok általában egy előre meghatározott TCP- vagy UDP-portot nyitnak, amelyre az elkövető rácsatlakozhat.
 - Kémprogram (*spyware*): célja a számítógépről információ megszerzése. Lehet webalapú, mint egy káros weboldal, települhet is webről, de megeshet, hogy maga az ártani kívánó fél telepíti fel a gépre (például billentyűleütés-naplózó program [*keylogger*], amely megjegyzi az összes leütött billentyűt).
 - Kéretlen reklám (*adware*): olyan szoftver, amely automatikusan reklámokat jelenít meg.

Az előbbieken felsorolt kártékony programok általában nem egymástól elhatárolhatóan működnek, az előbbi kategóriák a mai környezetben inkább az egyes programfunkciók leírására szolgálnak. Egy-egy kártevő több funkció ellátására is programozható, így valójában a modern *malware*-ek a fentiek valamilyen csomagba szerkesztett változatát jelentik. Kártékony szoftverek egyre gyakrabban jelennek meg Magyarországon is, az Országos Bírósági Hivatal adatbázisában rendelkezésre álló nyilvános információk azonban arra engednek következtetni, hogy ezek terjesztőivel szemben jogerős ítéletek ritkán születnek. Ennek hátterében számos ok állhat, részben az, hogy az elkövetők felett nem Magyarország rendelkezik joghatósággal, az eljárások bonyolultak és elhúzódnak, valamint az is, hogy kevés sértett tesz feljelentést, tartva az üzleti jó hírnevük csorbulásától. A 2017-ben futótűzként elterjedt WannaCry zsarolóvírus miatt az ORFK tájékoztatása szerint csak ketten tettek feljelentést.²⁸

A hacktivisták eszköztárában kiemelt helyen szerepelnek az úgynevezett botnethálózatok, amelyeken keresztül a hackerek összehangolt támadásokat tudnak indítani különböző célpontok ellen. A botnet a *robot* és a *network* szavak

²⁸ ORFK: ketten tettek feljelentést a WannaCry vírus támadása miatt. *HVG*, 2017. június 16.

összekapcsolásából ered, és vírussal fertőzött számítógépek hálózatára utal, amelyeket az elkövető(k) távolról küldött utasítások sorozatán keresztül képes(ek) irányítani, ezáltal tömegesen felhasználni bűncselekmények elkövetéséhez. A botnet kifejezést európai uniós dokumentumban először 2006-ban említik. A spamekről szóló közleményében az Európai Bizottság a kényszerű üzenetek küldésére szolgáló eszközként jellemezte a botnethálózatokat. A 2007 májusában kiadott, a kiberbűncselekmények elleni fellépés általános megközelítéséről szóló közlemény már jóval nagyobb szerepet tulajdonított a botneteknek, és ezeket az infrastruktúrákat tette felelőssé az olyan átfogó, információs rendszerek elleni támadásokért, mint amilyen az észtországi kritikus infrastruktúrák elleni támadás volt 2007-ben.²⁹

Az információs rendszerek elleni támadásokról szóló irányelv kiemelten foglalkozott a botnethálózatok elleni fellépés kérdésével.³⁰ Ez az uniós norma már a célját is abban határozza meg, hogy „[büntetőjogi] szankciókat állapítson meg a botnetek létrehozására, vagyis azon cselekményre vonatkozóan, amellyel célzott informatikai támadások révén jelentős számú számítógép felett veszik át a távvezérelt irányítást oly módon, hogy rosszindulatú számítástechnikai programokkal fertőzik meg őket”.³¹ Az irányelv arról is rendelkezik, hogy az olyan támadások esetében, amelyek célja botnet létrehozása, vagy amelyeket botnet révén hajtanak végre, a tagállamok megállapíthatnak súlyosabb szankciót.³² Ezt a szabályt a Btk. akképp ültette át, hogy az információs rendszer vagy adat megsértése büntettének minősített esete valósul meg, ha a cselekmény jelentős számú információs rendszert érint.³³ A botnet számos funkciót elláthat, Nagy Zoltán és Mezei Kitti a következő botnetfunkciókat különbözteti meg: DDoS-támadások indítása, spamküldés, adathalászat, hálózatfigyelés, billentyűzetfigyelés, internetes reklámokhoz kapcsolódóan klikkelések begyűjtése.³⁴ Újabban a botnethálózatokat gyakran használják kriptovaluták (például bitcoin) bányászására.

²⁹ Hancu [Hanula Zsolt]: Az oroszok visszabombázzák Észtországot az online kőkorszakba. *Index*, 2007. május 31.

³⁰ Az Európai Parlament és a Tanács 2013/40/EU irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról. L 218/8 (2013. augusztus 4.).

³¹ Az Európai Parlament és a Tanács 2013/40/EU irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról. L 218/8 (2013. augusztus 4.). (1) preambulumbekezdés.

³² Az Európai Parlament és a Tanács 2013/40/EU irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról. L 218/8 (2013. augusztus 4.). (13) preambulumbekezdés.

³³ Btk. 423. § (3) bekezdés.

³⁴ Nagy Zoltán András – Mezei Kitti: A zsarolóvírus és a botnet vírus mint napjaink két legveszélyesebb számítógépes vírusa. In Gaál Gyula – Hautzinger Zoltán (szerk.): *Szent Lászlótól a modernkori magyar rendészettudományig*. Pécs, Magyar Hadtudományi Társaság, Határőr Szakosztály, Pécsi Szakcsoport, 2017. 163–168.

A botnethálózatok funkciói közül talán az egyik leghírhedtebb a túlterheléses támadás (*denial of service attack* – *DOS*). A túlterheléses támadások esetében az elkövető azzal akadályozza a rendszer működését, hogy olyan adatmennyiséget zúdít a célrendszerre, amelyet az képtelen kezelni. A túlterheléses támadások manapság leggyakrabban úgynevezett elosztott túlterheléses támadással (*distributed denial of service attack* – *DDoS*) történnek, ami annyit jelent, hogy a megfertőzött zombiszámítógépek a megcélzott szervereknek folyamatosan kéréseket – adatcsomagokat – küldenek, és ha több ezer csomag érkezik egyszerre, a forgalmazás mértékét a támadott rendszer nem bírja el, és ez a rendszer teljes összeomlását eredményezheti. Ugyanakkor az információs rendszer működésének akadályozásához nem feltétel a célrendszer teljes megbénulása, ahogy Nagy és Mezei is kiemelik: a „funkcionális működésképtelenséghez elegendő a nagymértékű lelassulás is, ami a válaszügyi megnövekedett mértékéből adódik”.³⁵ A cselekmény különösen súlyos lehet, hiszen a Btk. szerint a cselekmény minősített esetét követi el, aki a 423. §-ban szabályozott magatartásokat közérdekű üzem ellen követi el. Mivel bizonyos infrastruktúrák megbénításának a háttérben gazdasági érdek, de akár politikai figyelemfelhívás is állhat, a szervezett bűnözői körök ma már gazdasági szolgáltatásként kínálják a DDoS-támadások lefolytatását, illetve az ilyen támadások lefolytatásához használható infrastruktúra bérbeadását. Mezei Kitti tanulmányában kifejti, hogy napjainkban „napi vagy havi díjjal átlagosan 5 \$ és 1000 \$ közötti áron lehet szert tenni hasonló eszközökre”.³⁶

Az elosztott túlterheléses támadások esetében érdemes röviden foglalkozni a tettesség kérdésével. Témánk szempontjából különösen fontos, kit tekinthetünk tettesnek, hiszen a hacktivistákat támogató egyének gyakran maguk telepítik fel a számítógépeikre azokat a programokat, amelyekkel hackercsoportok kezébe adják annak irányítását. A Btk. *Kommentárja* alapján a Btk. 423. § (2) bekezdése szerinti cselekmények elkövetője bárki lehet, azonban azok csak szándékosan valósíthatók meg.³⁷ A botnetek esetében a támadásban zombiként, távoli vezérléssel részt vevő rendszerek tulajdonosainak sokszor nincs arról tudomásuk, hogy a gépük vírusfertőzés áldozata, a támadással érintett információs rendszer tekintetében az akadályozási szándék esetükben tehát egyértelműen kizárható. A szándék általában a mestergép tulajdonosa, a *botherder* oldalán jelenik meg, az ő cselekménye szándékos és egyben célzatos. Az elkövető ebben az esetben nemcsak a túlterheléses támadással célzott információs rendszer működését akadályozza, hanem az összes olyan információs rendszer működését is, amelyet megfertőzött és távoli hozzáféréssel támadásra utasított. A hacktivistákat saját erőforrásaival támogató önkéntesek ellenben

³⁵ Nagy–Mezei (2017): i. m. 164.

³⁶ Mezei Kitti: A DDoS-támadások büntetőjogi szabályozása az Egyesült Államokban, Európában és Magyarországon. *Pro Futuro*, 8. (2018), 1. 70.

³⁷ Karsai Krisztina (szerk.): *Kommentár a Büntető Törvénykönyvről szóló 2012. évi C. törvényhez*. Budapest, Wolters Kluwer, 2017.

maguk is lehetnek tettesek, amennyiben tudatuk átfogta azt, hogy számítógépüket DDoS-támadások elkövetésére használták fel, és ehhez kifejezetten hozzájárultak.

Az információs rendszerben tárolt adatok jogosulatlan megváltoztatása és törlése

A 423. § (2) bekezdésének b) pontjában található az elkövetési magatartások II. köre, amely elektronikus adatok bevitelét, megváltoztatását, törlését és hozzáférhetetlenné tételét rendeli büntetni. Elkövető ebben az esetben bárki lehet, még az is, aki a rendszerbe jogosultan lép be, ám a fent megnevezett műveleteket már jogosulatlanul végzi. A tényállás szövegében a jogosulatlan jelző az eredményre utal, így elkövetheti a bűncselekményt az is, aki egyébként jogosult a rendszerbe belépni, ott az adatokon műveleteket végrehajtani, jogosultsága azonban nem terjed ki a rendszer működésének akadályozására. Adat törlése kapcsán az elkövető tudattartalma lényeges, megvalósul ugyanis a törlés akkor is, ha az adatokat csak különleges szakértelemmel lehet visszaállítani. A törlés megvalósulhat a törlés funkcióval vagy a mágnesszalagok elektromágneses úton való törlésével, hozzáférhetetlenné tételen pedig az adatok elrejtését értjük például egy olyan fájlban, amely jelszóval védett, vagy kódolt, de idetartozik az adathordozó elrejtése is.

A cselekmény az adatok megváltoztatásán túl megvalósítható új, valótlán adatok rögzítésével is. Ezekben az esetekben az adatbevitel más bűncselekményt is megvalósíthat (például sikkasztás), de az is előfordulhat, hogy az elkövető az adatbevitelt vagy -módosítást más jogellenes cselekmény leplezésére használja fel.

A doxing vagy az információ kiszivárogtatása a magyar büntetőjogban

A magyar büntetőjog rendszerében más szabályok vonatkoznak a személyes adatokkal való visszaélésre, valamint a minősített adatokra.

A visszaélés a személyes adatokkal a Btk. 219. §-ában szabályozott deliktum. A Btk. keretjogszabály, amelyet tartalommal a 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.) és a GDPR³⁸ töltenek ki. A bűncselekmény jogi tárgya a személyes adat megismeréséhez és biztonságos kezeléséhez, őrzéséhez való jog. A személyes adat lehet az egyénnel összefüggésbe hozható bármely információ. A GDPR 4. cikk 1. pontja példálózó jelleggel fel is sorolja a legjellemzőbb személyes adatokat, amelyek: „név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai,

³⁸ Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet). L 119/1 (2016. május 4.).

genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó ismeret”.³⁹ A Btk. személyes adattal való visszaélést büntetni rendelő szakaszában általános alanyt használ a törvényhozó, vagyis az elkövető – szemben a magántitok megsértésével – bárki lehet. A törvény négyféle elkövetési magatartást szabályoz. Az első két alapeset szerint megvalósítható a bűncselekmény jogosulatlan vagy céltól eltérő adatkezeléssel. Adatkezelésnek minősül az adatokon végzett bármilyen művelet, vagy a műveletek összessége, például gyűjtése, törlése, megváltoztatása, nyilvánosságra hozatala. Jogosulatlannak minősül az az adatkezelés, amely a GDPR 6. cikk (1), illetve az Infotv. 5. § (1) bekezdéseiben felsorolt jogalapok hiányában történik. Jogosulatlan az adatkezelés például akkor, ha ahhoz az érintett nem járult hozzá, vagy azt nem jogszabály rendelte el. A céltól eltérő adatkezelés akkor is tényállásszerű, ha az adatkezelésre egyébként megfelelő jogalappal került sor, mivel a célhoz kötöttség olyan általános elv, amelynek az adatkezelés teljes folyamatát át kell hatnia. Az 1/2012. Büntető Jogegységi Határozat kimondta, hogy az első fordulatba ütköző bűncselekményt bárki elkövetheti, nem csak az, aki adatkezelőnek minősül. Ezt erősítette meg a BH2012. 87., amikor kimondta, hogy alanyi oldalon nem feltétel az Infotv. szerinti adatkezelői minőség. Éppen ezért személyes adattal visszaélés könnyen megvalósulhat azáltal, hogy a sértettől annak hozzájárulása nélkül osztanak meg valamilyen személyes adatot, az online környezetben igen gyakran képet vagy videófelvételt. Lényeges fordulata ennek a szakasznak, hogy az a) és b) pontban leírt elkövetési magatartások tanúsításával még nem valósul meg bűncselekmény, annak szükséges eleme az is, hogy az elkövetés jogtalan haszonszerzési célból vagy jelentős érdeksérelem okozva valósuljon meg. A jelentős érdeksérelem tehát minden esetben valamilyen negatív eredmény, többnyire a sértett társadalmi megítélésének, megbecsültségének csorbulása. A jelentős érdeksérelem, mint eredmény vonatkozásában a bírósági gyakorlat azt mutatja, hogy bekövetkezőnek megállapítása nem a sértett szubjektív és elfogult álláspontján alapul, hanem bírói mérlegelésen, amelyben fontos szerepet tölt be a sértett egyéni tulajdonságainak, élethelyzetének és a társadalmi felfogásnak a vizsgálata. Az egyén társadalmi megítélésének csorbulása esetében lényeges annak vizsgálata, hogy a nyilvánosságra került információról hogyan vélekedik általában a társadalom, és melyek azok a tényezők, amelyek a közfelfogást negatív irányban befolyásolhatják. Személyes adattal visszaélés kísérlete miatt ítélték el azt a politikust, aki egyes megyei vadásztársaságok által szervezett ingyenes vadászatokról hozott nyilvánosságra információkat (vadászati naplók, trófeabírálati lapok, számlák). A terhelt védekezésében előadta, hogy az ingyenes vadászatok, amelyeken zömében magas rangú politikusok vettek részt, a közvagyonot károsították, ezért államtitkári minőségét kihasználva, de hatáskörét túllépve kért be személyes adatokat is tartalmazó információkat a vadásztársaságoktól, földügyi hatóságoktól. A bíróság szerint ugyanakkor az érintetteknek nem származott jelentős hátránya az információk nyilvánosságra hozatalából, amely

³⁹ GDPR 4. cikk 1. pont.

a köztudatban inkább politikai jellegű lejárataként jelent meg, így a cselekmény kísérleti szakban maradt (28.B.436/2011/56.).

A Btk. 265. §-a rendeli büntetni a minősített adattal való visszaélést. A minősített adatok körét a minősített adat védelméről szóló 2009. évi CLV. törvény (Mavtv.) határozza meg, és idesorolja azokat a szigorúan titkos, titkos, bizalmas, illetve korlátozott terjesztésű nemzeti vagy külföldi minősített adatokat, amelyekről a „minősítő a minősítési eljárás során megállapította, hogy az érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele a minősítéssel védhető közérdekek közül bármelyiket közvetlenül sérti vagy veszélyeztet, és tartalmára tekintettel annak nyilvánosságát és megismerhetőségét a minősítés keretében korlátozza”.⁴⁰ A cselekmény elkövetési magatartásai a minősített adat jogosulatlan megszerzése, felhasználása, jogosulatlan személy részére történő hozzáférhetővé, illetve jogosult személy részére hozzáférhetetlenné tétele. A hacktivisták módszereibe leginkább a második és harmadik elkövetési magatartások, vagyis a minősített adatok jogosulatlan felhasználása és hozzáférhetővé tétele illeszkedik. A bírósági gyakorlat alapján a hozzáférhetővé tételnek fontos feltétele, hogy az csak akkor valósul meg, ha konkrétan áll fenn annak a veszélye, hogy a titok ténylegesen illetéktelen személy számára hozzáférhetővé válik, a titok megismerhetőségének absztrakt veszélye, amit mondjuk a kezelő mulasztása okozott, még nem eredményez tényállásszerűséget.⁴¹

Konklúzió

A növekvő társadalmi támogatottság ellenére hiba lenne úgy tekinteni a hacktivistákra, mint a kibertér Robin Hoodjaira. Szemben az ártalmatlan kiberaktivisták eszköztárával, a hacktivisták eszközei jogsértőek. Akár számítógépes rendszerekbe való jogosulatlan belépésről, akár DDoS-támadások megindításáról, akár minősített adatok kiszivárogtatásáról beszélünk, olyan magatartásokról van szó, amelyeket a magyar büntetőjog pönalizál.

Noha e cselekmények jogsértő jellege nem kérdéses, a hacktivistáknak mégsem kell különösebben tartaniuk a felelősségre vonástól, hiszen a hackercsoportokhoz köthető személyek felderítése nem egyszerű és igencsak erőforrás-igényes feladat. Tipikusan olyan cselekményekről beszélünk, ahol igen magas a látencia, az igazán nagy kárt okozó cselekményeken túli magatartások nem is feltétlenül kerülnek fel a nyomozó hatóságok radarjára. Mivel a hacktivisták csoportok nem feltétlenül kötődnek adott országokhoz, a csoport tagjainak felderítése kiterjedt nemzetközi együttműködést igényel, a kibertér által biztosított anonimitás miatt pedig magas

⁴⁰ 2009. évi CLV. törvény a minősített adat védelméről (Mavtv.) 3. § 1. pont.

⁴¹ BH2016. 138.

fokú műszaki-technikai ismeretek is szükségesek az eredményes munkához. Noha mind az Interpol, mind az Europol igyekszik összehangolni a nemzeti nyomozó hatóságok munkáját, az Europol által évente közzétett internetes szervezett bűnözésről szóló jelentés még 2021-ben is az egyik kezelendő problémaként azonosította a nemzetközi együttműködés nehézségét.⁴²

Felhasznált irodalom

Ambrus István: *Digitalizáció és büntetőjog*. Budapest, Wolters Kluwer, 2021.

Az Anonymous átírta az alaptörvényt. *Index*, 2012. március 4. Online: https://index.hu/tech/2012/03/04/az_anonymous_atirta_az_alaptorvenyt

Az Anonymous azt állítja, meghackelték az orosz kéműholdakat. *HVG.hu*, 2022. március 3. Online: https://hvg.hu/tudomany/20220305_oroszorszag_kemmuhold_anonymous_hackerek_hacker-tamadas_network_battalion_65_roszkozmosz

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet). L 119/1 (2016. május 4.)

Az Európai Parlament és a Tanács 2013/40/EU irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról. L 218/8 (2013. augusztus 4.)

Beyer, Jessica L.: The Emergence of a Freedom of Information Movement: Anonymous, WikiLeaks, the Pirate Party, and Iceland. *Journal of Computer-Mediated Communication*, 19. (2014), 2. 141–154. Online: <https://doi.org/10.1111/jcc4.12050>

Burgess, Matt: Ukraine's Volunteer 'IT Army' Is Hacking in Uncharted Territory. *Wired*, 2022. február 27. Online: www.wired.com/story/ukraine-it-army-russia-war-cyberattacks-ddos/

Denning, Dorothy E.: Activism, Hacktivism, and Cyberterrorism: The Internet As a Tool for Influencing Foreign Policy. In John Arquilla – David Ronfeldt (szerk.): *Networks and Netwars. The Future of Terror, Crime, and Militancy*. Santa Monica, RAND Corporation, 2001. 239–288. Online: <https://doi.org/10.7249/MR1382>

Dornfeld László: Kiberterrorizmus – a jövő terrorizmusa? In Mezei Kitti (szerk.): *A bűnügyi tudományok és az informatika*. Pécs–Budapest, Pécsi Tudományegyetem Állam- és Jogtudományi Kar – MTA Társadalomtudományi Kutatóközpont, 2019. 46–63.

Európai Gazdasági és Szociális Bizottság: Az Európai Gazdasági és Szociális Bizottság véleménye – Kiberaktivisták és civil társadalmi szervezetek (saját kezdeményezésű vélemény). C 13/116 (2016. január 15.). Online: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv%3AOJ.C_.2016.013.01.0116.01.HUN&toc=OJ%3AC%3A2016%3A013%3ATOC

Europol: *Internet Organised Crime Threat Assessment (IOCTA) 2021*. Luxembourg, Publications Office of the European Union, 2021. Online: www.europol.europa.eu/publications-events/main-reports/iocta-report

⁴² Europol: *Internet Organised Crime Threat Assessment (IOCTA) 2021*. Luxembourg, Publications Office of the European Union, 2021. 40.

- Fehér Katalin: *Digitalizáció és új média*. Budapest, Akadémiai Kiadó, 2017. Online: <https://doi.org/10.1556/9789630597432>
- Gelányi Anikó – Csepely-Knorr Tamás: A jogosulatlan wifi használat minősítése, avagy ha nyitva van az ajtó, akkor bemehetnek? *Infokommunikáció és Jog*, 6. (2009), 34. 201–207. Online: https://infojog.hu/wp-content/uploads/pdf/200934_GelanyiAniko_CsepelyKnorrTamas.pdf
- Görgényi Ilona – Gula József – Horváth Tibor – Jacsó Judit – Lévay Miklós – Sántha Ferenc – Váradi Erika: *Magyar büntetőjog különös rész*. Budapest, Wolters Kluwer, 2020.
- Hancu [Hanula Zsolt]: Az oroszok visszabombázzák Észtországot az online kőkorszakba. *Index*, 2007. május 31. Online: <https://index.hu/tech/net/eszt290507/>
- Illig, Andrew T.: Computer Age Protesting: Why Hactivism is a Viable Option for Modern Social Activists. *Dickinson Law Review*, 119. (2015), 4. 1033–1057. Online: <https://ideas.dickinsonlaw.psu.edu/cgi/viewcontent.cgi?article=4107&context=dlra>
- Ireland, Leanna: We are all (not) Anonymous: Individual- and Country-Level Correlates of Support for and Opposition to Hactivism. *New Media & Society*, (2022). Online: <https://doi.org/10.1177/14614448221122252>
- Karsai Krisztina (szerk.): *Kommentár a Büntető Törvénykönyvről szóló 2012. évi C. törvényhez*. Budapest, Wolters Kluwer, 2017.
- Mezei Kitti: A DDoS-támadások büntetőjogi szabályozása az Egyesült Államokban, Európában és Magyarországon. *Pro Futuro*, 8. (2018), 1. 66–83. Online: <https://doi.org/10.26521/Profuturo/2018/1/4674>
- Mezei Kitti: A jogosulatlan belépés, avagy a hacking szabályozása a büntetőjogban. *Rendőrségi Tanulmányok*, 3. (2020), 2. 23–43.
- Nagy Zoltán András – Mezei Kitti: A zsarolóvírus és a botnet vírus mint napjaink két legveszélyesebb számítógépes vírusa. In Gaál Gyula – Hautzinger Zoltán (szerk.): *Szent Lászlótól a modernkori magyar rendészettudományig*. Pécs, Magyar Hadtudományi Társaság, Határőr Szakosztály, Pécsi Szakcsoport, 2017. 163–168.
- Nagy Zoltán András: A számítógépes bűnözés története. In Dobák Imre – Hautzinger Zoltán (szerk.): *Szakmaiság, szerénység, szorgalom. Ünnepi kötet a 65 éves Boda József tiszteletére*. Budapest, Dialóg Campus Kiadó, 2018. 471–480.
- ORFK: ketten tettek feljelentést a WannaCry vírus támadása miatt. *HVG*, 2017. június 16. Online: https://hvg.hu/tudomany/20170616_wannacry_zsarolovirus_orfk_magyar_feljelentések
- Szathmáry Zoltán: Etikus és nem etikus hacking – a kényszerű sérülékenységvizsgálat büntetőjogi kérdései. *Magyar Jog*, 67. (2020), 6. 340–346.
- Takács Petra: A Google Maps-en több ezer „értékeléssel” figyelmeztetik az orosz népet. *Liner.hu*, 2022. március 4. Online: <https://liner.hu/google-maps-orosz-ukran-haboru-2/>
- Travaglino, Giovanni A.: Support for Anonymous as Vicarious Dissent: Testing the Social Banditry Framework. *Group Processes & Intergroup Relations*, 22. (2019), 2. 163–181. Online: <https://doi.org/10.1177/1368430217722037>
- Varga Balázs: Informatikai bűncselekmények. *Jogi Fórum*, 2003. december 19. Online: www.jogi-forum.hu/publikaciok/127
- Varga Zoltán (szerk.): *Nagykommentár a Büntető törvénykönyvről szóló 1978. évi IV. törvényhez*. Budapest, KJK-Kerszöv, 2004.

Vákát

Bányász Péter

Lélektani műveletek az ukrán–orosz háborúban



A 2022 februárjában kitört háború alapjaiban változtatta meg világunkat. A közvéleményt, illetve a szakértők nagy részét is váratlanul érte az orosz agresszió, amely azonban átírta a várakozásokat. Oroszország az elmúlt évtizedekben fejlett katonai világhatalom képét mutatta magáról. Ez a kép azonban a háború kezdetén fokozatosan foszlott szét, mind a konvencionális, mind a kibertámadói képességeket illetően. A tanulmány a konfliktus kezdeti időszakát vizsgálja, alapvetően a lélektani műveletek aspektusából, amelyek vélemezhetően jelentősen hozzájárultak az események alakulásához. Nem csupán a harcoló felek moráljában, hanem a nemzetközi közvélemény befolyásolásával alakítják napjainkban is a háború eseményeit.

Bevezetés

Az Oroszország által 2022. február 24-én indított katonai művelet meglepte a szélesen értelmezett közvéleményt, illetve a szakértők nagy részét, annak ellenére, hogy a háború kezdete előtt Ukrajna és a NATO, valamint Oroszország is nagyszabású információs műveleteket folytatott. Az Egyesült Államok és szövetségesei, köztük Ukrajna, rendszeresen azzal vádolták Oroszországot, hogy katonai támadásra készül Ukrajna ellen. Eközben Oroszország folyamatosan változó, gyakran abszurdabbnál abszurdabb narratívát alkalmazva vádolta – és mai napig vádolja – Ukrajnát, megpróbálva magát áldozatnak beállítani, amivel igazolni vélte a katonai agressziót. Ilyen visszatérő vád többek között, hogy az orosz kisebbség ellen szisztematikus népiirtást folytattak a náci ukránok, Ukrajna nukleáris fegyvereket rejteget, amivel el akarja pusztítani Oroszországot, vagy éppen ukrán biológiai laborokban fejlesztették ki amerikai támogatással az új típusú koronavírus, amivel új világrend kiépítését tűzték célul. Az információs műveletek részét képező lélektani műveletek a háború kezdete után minden oldalon jelentősen felerősödtek.

E tanulmány a Nemzeti Közszolgálati Egyetem Eötvös József Kutatóközpont Információs Társadalom Kutatóintézete által 2022. május 25-én szervezett *Új technológiák hatása a demokráciára* címet viselő konferencián tartott előadás írásos változata. Ahogy a konferencián, úgy az írott verzióban is bizonyos megköteket szükséges alkalmazni. Háború esetén az igazság hallgat, mindenki hazudik, ami a háború természetes velejárója. Ezt azt jelenti, hogy a részt vevő felek érdekeik minél hatékonyabb képviselése, elérése érdekében úgynevezett lélektani műveleteket alkalmaznak, amelyek esetében, finoman szólva is, ritkán fejtik ki az igazság minden

szeletét. Éppen ezért rendkívül komoly információs zajt generál minden résztvevő, amiből elképesztően nehéz a valóságot objektíven leszűrni. Kutatóként viszonylagos szerencse, hogy ellentétben a sajtó munkatársaival, bennünket nem befolyásol a hírverseny, és nem kell azon aggódnunk, hogy mielőbb számoljunk be egy bekövetkezett eseményről, ami jó esetben ellenőrizetlen forrásból származik. Az újságírók egy része meggyőződésből terjeszt hazugságokat, hitet téve valamelyik oldal narratívája mellett, szovjet terminológia szerint „hasznos idiótaként”, míg jelentősebb részük a hírverseny logikája alapján a mielőbbi publikálás okán továbbít propagandát, mert nincs fizikailag jelen egy másik országban zajló hadművelleti területen, így másod-, harmad-, sokadik forrásból számol be az eseményekről. Mindezt nehezíti, hogy a művelti biztonság érdekében a hadviselő felek hírkorlátozást vezetnek be, hogy az ellenség ne értesülhessen a csapatmozgásokról, miközben párhuzamosan hamis híreket terjeszt, hogy megtéve valós szándékairól, támadási irányairól.

E tanulmány írásának idején bizonyos szempontból tisztábban látjuk az elmúlt nyolc hónap eseményeit, azonban így is sokszor lepel fedi a különböző műveleteket, tevékenységeket. Fentiekből fakadóan e tanulmány – ahogy az előadás május végén – a háború kezdeti időszakát vizsgálja.

A lélektani műveletek napjainkban is zajlanak, mégpedig rendkívül intenzíven. A tél közeledtével, az erőviszonyok átrendeződésével a frontok megmerevedni látszanak. A kritikus infrastruktúrák, ezen belül is az energiaellátás célzott és hatékony támadásával vélelmezhetően jövő év tavaszáig megmerevednek a frontok. A változás bekövetkeztére, legyen szó békekötésről, állások feladásáról, politikai döntések fognak határozni. Ezek befolyásolása pedig mind az ukrán, mind az orosz félnek kiemelt érdeke.

A lélektani műveletek fejlődése

A lélektani műveletek célja a kiválasztott célcsoport befolyásolása a kognitív dimenzió keresztül annak érdekében, hogy a művelet céljának megfelelően cselekedjenek. A célcsoport nemcsak az ellenség, hanem a szövetségesek vagy akár a saját lakosság is lehet. A politikai kampányok célja például a saját szavazók befolyásolása, hogy mozgósítsák őket, az ellenfél szavazóit rávenni, hogy otthon maradjanak, a bizonytalankodókat pedig, hogy a céljaiknak megfelelően szavazzanak.

A technológia fejlődésével egyre több eszközt használtak a kiválasztott célcsoportok befolyásolására, a tömegmédia elterjedése pedig paradigmaváltáshoz vezetett. A totalitárius rezsimek a propagandát a tömegmédián keresztül terjesztették előszeretettel. Ez az egyik oka annak, hogy a NATO kerüli a propaganda kifejezés használatát az információs műveleteiben, mivel a náci és szovjet ideológiai és politikai konnotációi miatt negatív felhangra tett szert. Következésképpen a NATO a „célzott információközlés” terminológiát használja a propaganda helyett.

A közösségi média megjelenése és elterjedése egy másik fontos mérföldkő volt a lélektani műveletekben. A közösségi média életünk számos aspektusát alakította át, és használatának kezdeti pozitívumai gyorsan ellentmondásokba torkolltak. Egy sor tanulmány mutatta ki, hogy súlyos depressziót okoz a fiatalok körében,⁴³ jelentősen növeli a szorongást.⁴⁴ Napjainkra a közösségi média komoly fegyverré vált az egyének és a társadalmak befolyásolásában. Mindezt több tényezőre vezethetjük vissza:

- a közösségi oldalak több tízezer szempont alapján gyűjtenek adatokat a felhasználóikról. Hogy csak egy példával illusztráljuk ennek jelentőségét, rögzítik az elküldött és a begépett, de elküldés előtt törölt üzeneteket.⁴⁵ Az egyénekre vonatkozó információk mellett a nyílt forrású információgyűjtés a trendelemzés szempontjából is releváns, ahol valós időben vizsgálhatók az egyes folyamatokra adott reakciók. Ennél is fontosabb, hogy elegendő adat birtokában a jövőbeli események nagymértékben megjósolhatók. Kertész János magyar hálózatkutató és szerzőtársai például egy tanulmányban kimutatták, hogy egy film Wikipedia-oldalának trendelemzése 85%-os pontossággal képes megjósolni, hogy a film bemutatásának első hétvégéjén milyen lesz a jegybevétel.⁴⁶ A technológia fejlődésével, a nagymértékű adatgyűjtés eredményeképpen a közösségi oldalak algoritmusai a mesterséges intelligenciával és a gépi tanulóval kombinálva vélhetően hetekre előre meg tudják jósolni, hogy a felhasználók mikor és mit fognak tenni;
- a 2013-as Snowden-ügy megmutatta, hogy a közösségi oldalak a nemzetbiztonsági szolgálatok szinte teljes körű megfigyelésének eszközévé váltak.⁴⁷ Az antidemokratikus államok esetében ez az állam polgárai ellenőrzésének és elnyomásának alapvető eszköze;
- a közösségi oldalak algoritmusai úgynevezett véleménybuborékokat hoztak létre, amelyeket a post-truth jelensége felerősített.

⁴³ Renae A. Merrill – Chunhua Cao – Brian A. Primack: Associations between Social Media Use, Personality Structure, and Development of Depression. *Journal of Affective Disorders Reports*, 10. (2022), 100385.

⁴⁴ Claire A. Wolniewicz et al.: Problematic Smartphone Use and Relations with Negative Affect, Fear of Missing out, and Fear of Negative and Positive Evaluation. *Psychiatry Research*, 262. (2018), 618–623.

⁴⁵ Manya Sleeper et al.: The Post that Wasn't: Exploring Self-Censorship on Facebook. In CSCW '13: *Proceedings of the 2013 Conference on Computer Supported Cooperative Work*. New York, NY, Association for Computing Machinery, 2013. 793–802.

⁴⁶ Márton Mestyán – Taha Yasseri – János Kertész: Early Prediction of Movie Box Office Success Based on Wikipedia Activity Big Data. *PLOS ONE*, 8. (2013), 8.

⁴⁷ Péter Bányász: Spies Act as a Spy: The Edward Snowden Case. In *Manažment–teória, výučba a prax 2014*. Liptovský Mikuláš, Akadémia ozbrojených síl generála Milana Rastislava Štefánika, 2014. 194–201.

Mit is értünk ez utóbbi fogalmak alatt? A plurális hírfogyasztási szokások hiányában a felhasználói viselkedéshez igazodó automatizált szelekciós folyamat egy úgynevezett buborékszűrő kialakulásához vezethet; vagyis a felhasználó csak azokat a tartalmakat fogja megtalálni a hírfolyamában, amelyeket rendszeresen fogyaszt, míg az ellentmondó tartalmakkal nem vagy alig találkozik; bármennyire is elterjedtek azok egyébként más felhasználók esetében.⁴⁸ Kijelenthető ez alapján, hogy a véleménybuborék azt a benyomást kelti a felhasználóban, hogy az ő leszűkített valóságperspektívája objektív, és magában foglalja a valóságot úgy, ahogy van. A gond, hogy ez párhuzamos valóságok kialakulásához vezetett.

Ehhez szorosan kapcsolódó fogalom a közelmúltban elterjedt post-truth jelenség, amely lényegében hozzájárul az álhírek politikai döntéshozatalra gyakorolt hatásához.⁴⁹ A post-truth kifejezés olyan állapotra utal, amikor a közvéleményt érzelmek és személyes meggyőződésekben gyökerező hiedelmek vezérik ahelyett, hogy tényeken, az objektivitáson alapulnának. Ebben az állapotban az objektivitás fokozatosan elveszíti jelentőségét a valóságérzékelésben, miközben helyébe számos párhuzamos szubjektív valóságérzékelés lép. Ez a folyamat nemcsak az álhírek felszívódásához járul hozzá, hanem a főáramú hírek érvényességét megkérdőjelező alternatív információk terjesztésével szándékosan keltett zűrzavarhoz is. Ez utóbbi tevékenységet zajkeltésnek nevezik, amelynek célja a demokrácia intézményeibe vetett közbizalom aláásása, és ezáltal a demokratikus intézmények legitimitásának megkérdőjelezése. A zajkeltést általában az illiberális, tekintélyelvű államok nemzetbiztonsági szervei alkalmazzák, különösen az Európai Unió tagállamai ellen, mivel az EU széttagoltsága megakadályozza a tagállamokat abban, hogy globális politikai szereplőként egységesen lépjenek fel, ami nagyobb teret enged a zajkeltő államok politikai ambícióinak. A demokratikus intézményrendszer mellett ezek a kampányok egyre gyakrabban a tudomány hitelességének megkérdőjelezését is célul tűzték, ami a Covid-19 első hullámától erősödött fel igazán.

Az álhírek terjedésének vizsgálatakor kutatók megállapították, hogy az álhírek, különösen a hamis politikai hírek gyorsabban terjedtek, szélesebb közönséghez jutottak el, és minden megfigyelt információs kategóriában mélyebben terjedtek, egyes esetekben jelentősen túlhaladva a valódi hírek terjedését. Azt is érdemes megjegyezni, hogy az emberek gyorsabban terjesztették az álhíreket, mint a botnetek.⁵⁰

⁴⁸ Dominic Spohr: Fake News and Ideological Polarization: Filter Bubbles and Selective Exposure on Social Media. *Business Information Review*, 34. (2017), 3. 150–160.

⁴⁹ Stephan Lewandowsky – Ullrich K. H. Ecker – John Cook: Beyond Misinformation: Understanding and Coping with the “Post-Truth” Era. *Journal of Applied Research in Memory and Cognition*, 6. (2017), 4. 353–369.

⁵⁰ Soroush Vosoughi – Mostafa ‘Neo’ Mohsenvand – Deb Roy: Rumor Gauge: Predicting the Veracity of Rumors on Twitter. *ACM Transactions on Knowledge Discovery from Data*, 11. (2017), 4. 1–36.

Az ukrán–orosz háború tanulságai

A háború kezdeti időszakában Oroszország nem tudta elérni feltételezett céljait, a légi és információs fölény megszerzését, ami a konfliktus elhúzódásához vezetett – e tanulmány írásakor még nem világos, hogy mikor ér véget a fegyveres konfliktus,⁵¹ de a folyamatban lévő szankciók a jelek és adatok szerint vélelmezhetően jelentős válságba sodorják Oroszországot.⁵² A szankciók hatása az európai országok számára is jelentős kihívásokat jelent, különösen az energiaellátás tekintetében.⁵³ A háború hatásai többek között a világgazdaság lassulására és a globális ellátási láncok változásaira is felhívták a figyelmet.⁵⁴

Feltehetően Oroszország a 2014-es agresszióját követőekhez hasonló marginális reakciókra számított az Egyesült Államok és az Európai Unió részéről, de geopolitikai szempontból olyan időpontot választott a háborúra, amikor a különböző NATO- és EU-tagállamok kormányai – belpolitikai fejleményeikre tekintettel – abban voltak érdekelték, hogy szigorú egységet mutassanak az orosz agresszióval szemben, és jelentősen támogassák Ukrajnát. Csak néhány példa:

- Franciaországban a háború idején elnökválasztás volt, és Macron elnököt a kampányban erős vezetőként, a Merkel utáni időszakban pedig olyan vízióval bíró politikusként mutatták be, aki az Európai Unió erős integrációjának jövőjét fogja meghatározni;
- az Egyesült Államokban 2022. november 8-án félidős választások lesznek, és a Biden-kormánynak erős, hozzáértő vezetést kell mutatnia a Covid-19 okozta gazdasági válság és a 2021 augusztusában katasztrofálisan sikerült afganisztáni kivonulás után;
- bár Lengyelországnak történelmileg komoly ellenérzései vannak Oroszországgal szemben, az erős fellépéssel igyekezett az Európai Bizottsággal kapcsolatos, jogállamiság ügyében zajló konfliktusát mérsékelni;
- az Egyesült Királyságban Boris Johnson miniszterelnök folyamatos politikai kritikáknak volt kitéve, amiért a Covid-19-záratok alatt bulizott. Az előadás, illetve a tanulmány írása közötti időszakban Johnson lemondott a tisztségről, akit Liz Truss követett a miniszterelnöki székben, mindössze 44 nap múlva bekövetkező lemondásáig;

⁵¹ Moran Yarchi: The Image War as a Significant Fighting Arena – Evidence from the Ukrainian Battle over Perceptions during the 2022 Russian Invasion. *Studies in Conflict & Terrorism*, 2022. április 26. 1–13.

⁵² Elliot Smith: Russia Faces ‘Economic Oblivion’ Despite Claims of Short-term Resilience, Economists Say. *CNBC*, 2022. augusztus 2.

⁵³ Haris Doukas – Alexandros Nikas: Europe’s Energy Crisis — Climate Community Must Speak Up. *Nature*, 608. (2022), 7923. 472–472.

⁵⁴ Sergio Mariotti: A Warning from the Russian–Ukrainian War: Avoiding a Future That Rhymes with the Past. *Journal of Industrial and Business Economics*, 2022. július 4.

- Törökország súlyos recesszió felé tart, de Erdogan elnök jól felismerte a fekete-tengeri erőviszonyok átrendeződését, ami Törökországot, és így őt magát is, még inkább megkerülhetetlen szereplővé teszi, hiszen a szíriai menekültek mellett hamarosan a világ gabonaellátásának és Európa gázellátásának biztosításában is kulcsszereplővé válik.

A háború elhúzódása meglepte a legtöbb szakértőt, hiszen általános volt az egyetértés Oroszország jelentős katonai képességeiről. A konvencionális hadviselési képességei mellett talán csak Oroszország kiberképességei voltak – mai tudásunk szerint – jelentősen túlbecsülve. Az elmúlt évtizedek során a Kremlhez köthető, államilag támogatott hackereket gyanúsítottak meg egy sor paradigmaváltó kibertámadás elkövetésével, amelyek alakították, irányították és keretbe foglalták a NATO kiberbiztonsággal kapcsolatos stratégiai gondolkodását.

Ez alatt nem csupán az Észtország kormányzati, pénzügyi és médiaszolgáltatásokhoz kapcsolódó kritikus infrastruktúrái ellen 2007-ben elkövetett elosztott szolgáltatásmegtagadásos (DDoS) támadásokat kell érteni,⁵⁵ hanem a 2016-os brit Brexit-népszavazásba⁵⁶ és a szintén ez évben zajló amerikai elnökválasztásba történő beavatkozást is. Ezeket az eseményeket követően a nyugati közvélemény mindig Oroszországot gyanította a nagyszabású kibertámadások mögött, és Oroszország – akár érintett volt, akár nem – intenzív információs műveleteivel erősítette az orosz hackerek mindenhatóságától való félelmet.⁵⁷ Az amerikai Belbiztonsági Hivatal és az FBI közös jelentése, amely a 2016-os amerikai elnökválasztásba való beavatkozást vizsgálta, egyértelműen Oroszországot attribúálta elkövetőként.⁵⁸

A szofisztikált kibertámadások jelentős károkat okozhatnak, mivel a támadás nemcsak a fizikai, hanem a kognitív dimenzióban is zajlik. A már említett 2007-es Észtország elleni kibertámadást követően több szerző is foglalkozott az ilyen komplex kibertámadások forgatókönyveinek felvázolásának lehetőségével. Magyarországon például 2010-ben *Digitális Mohács* címen elemezték kutatók e kérdéskört,⁵⁹ amit aztán 2017-ben kiegészítették a 2016-os amerikai elnökválasztás tapasztalatainak feldolgozásával.⁶⁰ A tanulmány alapjául szolgáló ukrán–orosz konfliktus

⁵⁵ Michael Lesk: The New Front Line: Estonia under Cyberassault. *IEEE Security & Privacy*, 5. (2007), 4. 76–79; John Arquilla: Twenty Years of Cyberwar. *Journal of Military Ethics*, 12. (2013), 1. 80–87.

⁵⁶ Daniel Treisman (szerk.): *The New Autocracy. Information, Politics, and Policy in Putin's Russia*. Los Angeles, Brookings Institution Press, 2018.

⁵⁷ Alexander Lanoszka: Disinformation in International Politics. *European Journal of International Security*, 4. (2019), 2. 227–248.

⁵⁸ Kovács László – Krasznay Csaba: „Mert övök a hatalom”: Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során. *Nemzet és Biztonság*, 10. (2017b), 3. 3–15.

⁵⁹ Kovács László – Krasznay Csaba: Digitális Mohács. *Nemzet és Biztonság*, 3. (2010), 1. 44–56.

⁶⁰ Kovács László – Krasznay Csaba: Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint. *Nemzet és Biztonság*, 10. (2017a), 1. 3–16.

paradigmaváltó eseményei inspirálták a szerzőket egy újabb kiegészítésre, a *Digitális Mohács 3.0*-ra, amely e sorok írásakor készül. Mint később látni fogjuk, a kibertámadások és a lélektani műveletek a kognitív dimenzióban hatással vannak egymásra, nem csupán kiegészítik egymást.

A közelmúlt háborús időszakának eseményei sok tekintetben arra kényszerítettek bennünket, hogy újragondoljuk a kiberbiztonsággal kapcsolatos felfogásunkat, ismereteinket. A várakozásokkal ellentétben Ukrajna nemcsak a hagyományos hadviselésben, hanem a kiberképességek magas szintjén is meglepett minket. Ez utóbbiban jelentős szerepet játszottak az úgynevezett „kiberönkéntesek”. Ezeket a civileket felháborította az orosz agresszió, amiben jelentős szerepet játszottak a professzionális ukrán lélektani műveletek is.

Más országok állampolgáraiként több százezer civil önkéntes vett/vesz részt az orosz elektronikus információs rendszerek elleni támadásban; sokan közülük az Ukrajna által hivatalosan létrehozott, IT Armynak nevezett formális szervezet tagjaként. Az ukrán hivatalos adatok szerint az IT Army tagjai 250 ezer főt számlálnak, azonban érdemes ezt is szkeptikusan kezelni, ugyanis ez a bejelentés is a lélektani műveletek kontextusában értelmezendő.

Az önkéntesek nemcsak Ukrajnát támogatják, hanem fokozatosan növekvő számban oroszbarát csoportok is megjelentek,⁶¹ akik jellemzően kiberbűnözői csoportokat támogatnak. Oroszország ismereteink szerint évek óta hallgatólagos megállapodás alapján használja az orosz kiberbűnözőket hibrid műveleteiben:

- az orosz hackerek szabadon tevékenykedhetnek, de nem támadhatnak orosz célpontokat, kizárólag csak külföldieket;
- és ha az orosz állami érdekek úgy kívánják, akkor szakértelmükkel hozzá kell járulniuk Oroszország kibertérbeli műveleteihez.

A NATO a 2016-os varsói csúcstalálkozón deklarálta, hogy a kibertér új műveleti területként értelmezendő a stratégiai gondolkodásában.⁶² Az ukrán–orosz háború azonban átírta a papírformát, és számos új típusú kibertéri fenyegetést hozott létre, amelyek következményeit ma még nem tudjuk felmérni. A háború első hónapjaiban Oroszország elektronikus információs rendszerei óriási mennyiségű kibertámadásnak voltak kitéve, és rendkívüli mennyiségű, különböző típusú adat került nyilvánosságra, köztük személyes adatok, pénzügyi adatok, érzékeny és minősített adatok. Emellett nagyszámú kritikus információs infrastruktúrát (közlekedési rendszerek, műholdak, nukleáris létesítmények, közművek stb.) is támadás ért.

A háború kezdetét követően az orosz lélektani képességek meg sem közelítették az ukrán műveletek sikerét. Az orosz nemzetbiztonsági szolgálatok korán felismerték a véleménybuborék és a post-truth fontosságát, és sikeresen kampányoltak

⁶¹ E tanulmány írásának idején számuk átbillent az oroszbarát csoportok javára.

⁶² László Kovács: Cyber Security Policy and Strategy in the European Union and Nato. *Land Forces Academy Review*, 23. (2018), 1. 16–24.

a bizalmatlanság megerősítése érdekében. A Covid-19 megerősítette ezt a tendenciát, jelentősen növelve az áltudományos tartalmak terjedését és csökkentve a polgárok bizalmát a tudományban és a demokratikus intézményekben. A különböző abszurd álhírek nem kioltották egymást, hanem új paradigmává olvadtak össze. Egy példa a magyarországi háború első napjaiból:

„Nos láttok mostanában Cremtél csikokat az égen??? Ugye nem!!!!!! Na akkor érted mit bombázott le Putyin?? Az Ukrán biolaborokat ahol ezeket a mérgeket állították elő számunkra na meg ... a repereiket ahonnan felszáltak a mérget permetező gépek!! Akkor Fucs a influenzának meg a Covidnak!!!!!! Putyin bombái értünk robbantak! Ukrajna volt a dep stat hadibázisa!! Minden vegyipermert onnan jött s minden méreg onnan van az élelmiszereinkben!! Na akkor ki ad hálát Putyinnak??? Legyen áldott minden lépése!!” A szöveg kétszer ismétlődő imádkozó hangulatjellel, szív hangulatjellel, orosz zászló hangulatjellel zárul.

Az idézetet szövegűen másoltam be, nem változtattam a helyesírási hibákon. A felhasználó vélemezhetően nem valós személy, hanem a propaganda terjesztésének céljára létrehozott profil, de ettől függetlenül tovább osztva megjelenik olyan felhasználók hírfolyamában, akik hajlamosak a bejegyzésben szereplő narratíva befogadására. Ebben a Facebook-bejegyzésben több összeesküvés-elmélet is megjelenik, mint a mély állam, a Covid mint biológiai fegyver, a chemtrail és a genetikailag módosított élelmiszerek.

Mivel az algoritmus buborékot hoz létre a felhasználók számára, ez a tartalom elsősorban azok között terjed, akik már hisznek ebben a narratívában. A buborék aláássa a buborékon kívüli emberek meggyőzésére irányuló törekvéseket. Véleményem szerint az orosz lélektani műveletek sikertelensége a korábbi orosz eredményekkel magyarázható. Háborúban azonban kulcsfontosságú, hogy másokat is meggyőzzünk arról, hogy támogassák a narratívánkat, és ehhez új közönségeket kell meggyőznünk.

A háború előtt az oroszországi sajtó nyilvánossága nem volt különösebben erős, de a háború kezdete után az orosz kormány szinte teljes egészében felszámolta a független sajtót. Emiatt az ukránoknak különösen kreatívnak kellett lenniük ahhoz, hogy az orosz lakosságot a valódi történések alapján tájékoztassák a háborúról, és ne csak az orosz propaganda és cenzúra által alakított narratívával. A háború kezdetétől fogva létfontosságú volt Ukrajna számára, hogy erősítse a lakosság morálját, ugyanakkor gyengítse az orosz katonák morálját, ami különösen nagy kreativitással történt. Ahogy a tanulmányban korábban már rámutattam, a kibertámadások és a lélektani műveletek befolyásolják egymást. Ezt tökéletesen illusztrálja, hogy a kiberönkéntesek feltörték az orosz fegyveres erők nyilvántartását, és nyilvánosságra hozták az Ukrájában harcoló katonák személyes adatait.

Ennek alapján elkezdtek felhívni az Ukrájában megölt vagy hadifogságba esett katonák családtagjait, hogy tájékoztassák őket a katonák állapotáról. Ezzel egyrészt tájékoztatták az orosz állampolgárokat arról, hogy háború folyik – az orosz narratíva szerint ma is csak különleges katonai műveletek zajlanak. A csapatok állapotáról

való tudósítással csökkent a morál az orosz háterszágban, és a megfelelő kérdésekkel információkat lehetett kicsikarni a csapatmozgásokról. Végül elindítottak egy kampányt, amelynek keretében a fogságba esett orosz katonák egy Google-úrlap kitöltésével tájékoztathatták édesanyjukat arról, hogy hadifogságba estek, és ha édesanyjuk értük jön, akkor kiszabadulnak. Ez egyszerre erősítette az ukrán katonák morálját, megerősítve a felsőbbrendűség érzését, ugyanakkor jelentősen csökkentette az orosz katonák morálját. Elég csak az „anyámasszony katonája” kifejezésre gondolni, hogy mit is jelent mindez. A hadtörténelem példái a keleti front hadifogságát sosem a néppünnepély kategóriájába sorolták, így teljes mértékben érthető, ha valaki az ott átélt borzalmaktól mielőbb szabadulni szeretne, akkor is, ha a morálra egyébként a fenti módon hat.

Mindkét országnak komoly érdeke fűződik a nemzetközi közvélemény befolyásolásához. A háború folytatásával Oroszország megpróbálja csökkenteni az Európai Unió tagjainak egységét, és erősíteni azt a narratívát az európai polgárok körében, hogy a szankciók nem Oroszországnak, csak az EU-nak ártanak. Ennek célja, hogy a közvélemény támogatásának erodálásával megváltoztassa az Ukrajnának nyújtott kormányzati támogatást. Ennek semlegesítése érdekében Ukrajna is keményen dolgozik, hiszen a folyamatos támogatás a túlélés kérdése.

Minden bizonnyal a mesterséges intelligencia lesz az álhírkampányok következő paradigmaváltó entitása. Napjainkban számos olyan videót találunk az interneten, amelyekben közszereplők olyan dolgokat mondanak, amelyeket egyébként nem mondanának. Ez az úgynevezett deepfake jelenség, amikor a mesterséges intelligencia a közszereplők arcát – akár valós időben – a színészek arcára montírozza, miközben e személyek hangján szólnak meg. A gépi tanulás fejlődésével ez a technika a jövőben egyre kifinomultabbá válik. Ez tovább fogja erodálni az igazságba vetett bizalmat. Nem nehéz belátni ennek háborús alkalmazásának lehetőségeit, és hogy milyen mértékben fogja átalakítani a lélektani műveletek kereteit.

A lélektani műveletek egy izgalmas aspektusát jelenti az internetes mémek alkalmazása. A háború kitörésének első heteiben rendkívüli mennyiségben találkozhatunk a háborúra reflektáló mémekkel. A mémek terjedésének már a Covid-19 idején is komoly szerepe volt. A mémek alapvető platformot jelentettek a kormányzati üzenetek (mint például maszkviselés, társadalmi távolságtartás) terjesztéséhez, amelyek a járvány terjedésével párhuzamosan fejlődtek. Amíg a járvány főként Kínára korlátozódott, a mémek általában a korábbi vírusok (például SAARS 2003, H1N1 sertésinfluenza 2009) média által generált tömeghisztériájára összpontosítottak, de a járvány terjedésével az említett fontos nyilvános üzenetek hordozóivá váltak. Elfogadva Shana MacDonald álláspontját a mémek társadalmi jelentőségéről, a mémek komoly veszélyt is jelentenek, ha negatív üzenetek és dezinformáció terjesztésére használják őket.⁶³

⁶³ Shana MacDonald: What Do You (Really) Meme? Pandemic Memes as Social Political Repositories. *Leisure Sciences*, 43. (2020), 1–2. 143–151.

Véleményem szerint a mémek netrográfiai elemzése kulcsfontosságú módszer a társadalmak ellenálló képességének tanulmányozásához, mivel lehetőséget nyújt a társadalom befolyásolására a megfelelő stratégia megválasztásával. Matteo La Torre és szerzőtársai tanulmánya ennek a következtetésnek a fontosságára világít rá az olasz kormány stratégiájának vizsgálatával a Covid-19 első hullámának idején.⁶⁴

A háború első heteiben a mémoldalak (például a 9gag vagy a Reddit) kizárólag az ukrán–orosz háborúval kapcsolatos mémekkel volt tele, amelyek szinte teljes egészében az ukrán narratívát közvetítették, Oroszországot elítélve. Természetesen próbálkozott Oroszország is ezeken a felületeken erősíteni a narratívát, azonban ezek alig érték el nézettséget, ami egyrészt a cenzúrából, másrészt a többi felhasználó lepontozásából következett.

Következtetések

A kibertámadások mellett, mint már említettem, számos lélektani műveletet hajtottak végre a részt vevő felek, értelemszerűen különböző célokkal. Ukrajna, mint a megtámadott fél, különlegesebb helyzetben volt, mivel könnyebben elnyerte a nemzetközi közvélemény támogatását. Ez pedig létfontosságú volt a háború kimenetele szempontjából, hiszen így az Európai Unió és a NATO tagállamai összetartottak, megghiúsítva Oroszország feltételezett várakozásait. Ez nemcsak a szankciók elfogadásában nyilvánult meg, hanem jelentős fegyvertámogatásban is, ami e sorok írásakor kiegyenlítette az Ukrajna és Oroszország közötti aszimmetrikus viszonyokat, átbillentve a védekezést az orosz félre.

Az Ukrajna által végzett sikeres lélektani műveletek hatására sok fiatal a világ különböző tájáról érezte úgy, hogy ki kell állnia az orosz agresszió ellen, ami a korábban említett „kiberönkéntesek” megjelenéséhez vezetett. Fiatalok százezrei tettek szert támadó képességekre, megtanulták, hogyan lehet következmények nélkül behatolni védett rendszerekbe, beleértve kritikus infrastruktúrákat. Ez azonban számos kockázatot rejt magában, amelyek közül az egyik legfontosabb szempont a „kiberönkéntesek” „pacifikálása” a háború befejezése után. A kiemelt kérdés az, hogyan lehet biztosítani, hogy ne kiberbűnözőkként folytassák, hanem etikusan használják fel képességeiket.⁶⁵

E sorok írásakor még nem világos, hogy mikor és milyen formában ér véget a háború. Ami biztos, hogy a korábbi világrend felborult, beláthatatlan következményekkel kell foglalkoznunk a közeljövőben. A háború elején alkalmazott

⁶⁴ Matteo La Torre et al.: Calculative Practices, Social Movements and the Rise of Collective Identity: How #istayathome Mobilised a Nation. *Accounting, Auditing & Accountability Journal*, 35. (2021), 9. 1–27.

⁶⁵ Botond Feledy – Csaba Virág: An Assessment of Cyber Volunteer Groups in Interstate Conflicts and Their Impact on Public Policies. *Scientia et Securitas*, 3. (2022), 1. 12–18.

lélektani műveletek nem várt következményekkel jártak, amelyek többek között Finnország és Svédország NATO-aspirációjához vezettek. E két ország vélelméhez NATO-tagsága az elmúlt évtizedek hidegháborús tabuját döntötte meg.

Amit biztosan kijelenthetünk, hogy a jövőbeli konfliktusokban a kiberválság kétségtelenül egyre nagyobb szerepet fog játszani, ami a részt vevő államok polgárait és az egész világra kihatással lesz.

Felhasznált irodalom

- Arquilla, John: Twenty Years of Cyberwar. *Journal of Military Ethics*, 12. (2013), 1. 80–87. Online: <https://doi.org/10.1080/15027570.2013.782632>
- Bányász, Péter: Spies Act as a Spy: The Edward Snowden Case. In *Management-teória, vizsgálata és a gyakorlat* 2014. Liptovský Mikuláš, Akadémia ozbrojených síl generála Milana Rastislava Štefánika, 2014. 194–201. Online: http://real.mtak.hu/94341/1/Spies_act_as_a_spy-_The_Edward_Snowden_c.pdf
- Doukas, Haris – Alexandros Nikas: Europe’s Energy Crisis – Climate Community Must Speak Up. *Nature*, 608. (2022), 7923. 472–472. Online: <https://doi.org/10.1038/d41586-022-02199-5>
- Felty, Botond – Csaba Virág: An Assessment of Cyber Volunteer Groups in Interstate Conflicts and Their Impact on Public Policies. *Scientia et Securitas*, 3. (2022), 1. 12–18. Online: <https://doi.org/10.1556/112.2022.00091>
- Kovács, László: Cyber Security Policy and Strategy in the European Union and NATO. *Land Forces Academy Review*, 23. (2018), 1. 16–24. Online: <https://doi.org/10.2478/raft-2018-0002>
- Kovács László – Krasznay Csaba: Digitális Mohács. *Nemzet és Biztonság*, 3. (2010), 1. 44–56.
- Kovács László – Krasznay Csaba: Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint. *Nemzet és Biztonság*, 10. (2017a), 1. 3–16.
- Kovács László – Krasznay Csaba: „Mert övök a hatalom”: Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során. *Nemzet és Biztonság*, 10. (2017b), 3. 3–15.
- Lanoszka, Alexander: Disinformation in International Politics. *European Journal of International Security*, 4. (2019), 2. 227–248. Online: <https://doi.org/10.1017/eis.2019.6>
- La Torre, Matteo – Patrizia Di Tullio – Paola Tamburro – Maurizio Massaro – Michele Antonio Rea: Calculative Practices, Social Movements and the Rise of Collective Identity: How #istayathome Mobilised a Nation. *Accounting, Auditing & Accountability Journal*, 35. (2021), 9. 1–27. Online: <https://doi.org/10.1108/AAAJ-08-2020-4819>
- Lesk, Michael: The New Front Line: Estonia under Cyberassault. *IEEE Security & Privacy*, 5. (2007), 4. 76–79. Online: <https://doi.org/10.1109/MSP.2007.98>
- Lewandowsky, Stephan – Ullrich K. H. Ecker – John Cook: Beyond Misinformation: Understanding and Coping with the “Post-Truth” Era. *Journal of Applied Research in Memory and Cognition*, 6. (2017), 4. 353–369. Online: <https://doi.org/10.1016/j.jarmac.2017.07.008>
- MacDonald, Shana: What Do You (Really) Meme? Pandemic Memes as Social Political Repositories. *Leisure Sciences*, 43. (2020), 1–2. 143–151. Online: <https://doi.org/10.1080/01490400.2020.1773995>

- Mariotti, Sergio: A Warning from the Russian–Ukrainian War: Avoiding a Future That Rhymes with the Past. *Journal of Industrial and Business Economics*, 2022. július 4. Online: <https://doi.org/10.1007/s40812-022-00219-z>
- Merrill, Renae A. – Chunhua Cao – Brian A. Primack: Associations between Social Media Use, Personality Structure, and Development of Depression. *Journal of Affective Disorders Reports*, 10. (2022), 100385. Online: <https://doi.org/10.1016/j.jadr.2022.100385>
- Mestyán, Márton – Taha Yasseri – János Kertész: Early Prediction of Movie Box Office Success Based on Wikipedia Activity Big Data. *PLOS ONE*, 8. (2013), 8. Online: <https://doi.org/10.1371/journal.pone.0071226>
- Sleeper, Manya – Rebecca Balebako – Sauvik Das – Amber Lynn McConahy – Jason Wiese – Lorrie Faith Cranor: The Post that Wasn't: Exploring Self-Censorship on Facebook. In CSCW '13: *Proceedings of the 2013 Conference on Computer Supported Cooperative Work*. New York, NY, Association for Computing Machinery, 2013. 793–802. Online: <https://doi.org/10.1145/2441776.2441865>
- Smith, Elliot: Russia Faces 'Economic Oblivion' Despite Claims of Short-term Resilience, Economists Say. *CNBC*, 2022. augusztus 2. Online: www.cnbc.com/2022/08/02/russia-faces-economic-oblivion-despite-short-term-resilience.html
- Spohr, Dominic: Fake News and Ideological Polarization: Filter Bubbles and Selective Exposure on Social Media. *Business Information Review*, 34. (2017), 3. 150–160. Online: <https://doi.org/10.1177/0266382117722446>
- Treisman, Daniel (szerk.): *The New Autocracy: Information, Politics, and Policy in Putin's Russia*. Los Angeles, Brookings Institution Press, 2018. Online: www.brookings.edu/book/the-new-autocracy/
- Vosoughi, Soroush – Mostafa 'Neo' Mohsenvand – Deb Roy: Rumor Gauge: Predicting the Veracity of Rumors on Twitter. *ACM Transactions on Knowledge Discovery from Data*, 11. (2017), 4. 1–36. Online: <https://doi.org/10.1145/3070644>
- Wolniewicz, Claire A. – Mojisola F. Tihamiyu – Justin W. Weeks – Jon D. Elhai: Problematic Smartphone Use and Relations with Negative Affect, Fear of Missing out, and Fear of Negative and Positive Evaluation. *Psychiatry Research*, 262. (2018), 618–623. Online: <https://doi.org/10.1016/j.psychres.2017.09.058>
- Yarchi, Moran: The Image War as a Significant Fighting Arena – Evidence from the Ukrainian Battle over Perceptions during the 2022 Russian Invasion. *Studies in Conflict & Terrorism*, 2022. április 26. 1–13. Online: <https://doi.org/10.1080/1057610X.2022.2066525>

Nyáry Gábor

Akindzszik a kibertérben

Virtuális háború kontra digitális felforgatás



A szemünk előtt, a közvetlen szomszédságunkban véres háború dúl, és ez óhatatlanul vonzza a tekintetünket. De ne legyenek kétségeink: veszélyes konfliktusok terepe a földgolyó jó része. Az életünket felismerhetetlenségig megváltoztatja, jó értelemben is, veszélyekkel is a digitalizációnak nevezett drámai átalakulás. Nemcsak a technológia változik, de a minket körülvevő világ is. Tektonikus geopolitikai átrendeződés zajlik körülöttünk. A többpólusú világban az érdekérvényesítés és a szabályoknélküliség a jellemző, amihez jól illeszkedik a kiberhadszínterek átláthatatlan, képlékeny közege. Ami vitathatatlan: szakadatlanul „dörögnek” már a fegyverek ebben az új kiberdimenzióban. Ami viszont még kérdés: ez vajon „kiberháború”, vagy valami más lesz?¹ Szakértők sorra tárják fel a probléma jelentéssrétegeit, és a megértéshez talán közelebb segít minket a kiber-nemzetbiztonsági kutatásokban ma már egyáltalán nem ismeretlen analógiás gondolkodás.² Egy számunkra ismerősen csengő metaforát hívunk ehhez segítségül.

A sarkaiból kifordult világ – bevezető helyett

Hajlamosak vagyunk még mindig úgy fogalmazni, hogy „információs társadalomban” élünk. Pedig az igazság az, hogy a világunk egyre inkább elmozdul egy „digitális társadalom” felé. A kapcsolat persze szerves, hiszen ez utóbbi az információ központi szerepe köré szerveződő közösségből nő ki azáltal, hogy lassan minden tevékenységünk digitális eszközökön alapszik, és az interneten nyugvó, decentralizált hálózatok szervezik életünk működését. Az anyagi javak termelése és fogyasztása, a gazdaság szintén a digitalizáció rohamos terjedésével kap új dimenziót. Sommás megfogalmazással úgy jellemezhető ez a folyamat, mint amelyben az adatok és a hálózatok körbefonják, átítatják a termelési folyamatokat,

¹ Vö. Amit Sharma: Cyber Wars: A Paradigm Shift from Means to Ends. *Strategic Analysis*, 34. (2010), 1. 67–73.

² A témában máig megkerülhetetlen a kiberháborúhoz kapcsolódó mítoszképzés mechanizmusait feltáró tanulmány. Vö. Erik Gatzke: The Myth of Cyberwar. *International Security*, 38. (2013), 2. 41–73.

a kormányzati és személyes fogyasztást, a határokon átvitelő kereskedelmi forgalmat és természetesen a gazdaságot mozgató pénzügyeket is.

A dolgoknak azonban rendszerint megvan a maguk árnyoldala is. A korszerű technológiák mindent átszövő használata megsokszorozza a jólétünket, kényelmünket – de ugyanakkor hallatlanul kiszolgáltatottá is teszi a modern társadalmakat. Ahogy bővül a világban felhalmozódó adattömeg, ahogy terjeszkedik, bővül a digitális gazdaság – egyre növekszik a kiberbiztonsági kockázatok abszolút és relatív mértéke is. A sérülékenységet az ár, amelyet a digitalizáció elképesztő lehetőségeiért fizetnünk kell. A kibertér, életünknek ez az új dimenziója nem csupán a tisztességes vagy békés szándékú szereplőknek ad otthont. Jól képzett, a technológia réseit könyörtelenül kihasználó kiberbűnözők igyekeznek csapdába csalni, megfélemlíteni, kifosztani egyént, vállalatot, államot. De ami még nyugtalanítóbb: az online terek feltáruló világa újfajta harcosok küzdelmének a terepe is. A digitális világban, állítják sokan, már ma is dúl a „háborús szint alatti”, csendes hadakozás. Vagy már „háború”?

Módszertani megközelítések és lehetőségek

A viszonylag hosszú ideje zajló szakmai vitákban való eligazodást egy sajátos módszertani eszköz (valójában inkább látásmód), az analógiákon nyugvó leírás és érvelés segítheti. A történettudomány természetesen régóta használja ezt a kézenfekvő lehetőséget, de ma már a politológia számos részterületének művelői is szívesen nyúlnak ehhez az „eszközhöz”.

Clausewitz a kibertérben

A szomszédban valóságos háborúban csapnak össze az ellentétek, de ugyanakkor a hírek és dezinformációk körül kavargó információs hadviselés is igazi csatatereket idéz. Nem is beszélve a kiberhadszínterekről. A 19. század elejének nagy teoretikusa, a porosz Clausewitz munkássága óta mindent tudni vélünk a háborúról, ám napjaink eseményei mintha fejük tetejére fordítanák ezeket az öröknek gondolt igazságokat is. Szakemberek, a nemzetközi kapcsolatok, a kiberbiztonság kutatói vitatkoznak olyan alapvető kérdéseken, hogy a digitális tereket is elborító támadások, akciók háborúnak tekinthetők-e? Vajon egyáltalán használhatók még ezek a fogalmaink? Ha igen, akkor hogyan?

Analógiás gondolkodás a kiber-nemzetbiztonsági kutatásban

Az analógiás gondolkodás (történeti összehasonlítás) nem ismeretlen a nemzetközi kapcsolatok kutatásában.³ Természetesen maga a politika is szívesen nyúl ehhez a támponthez, és a nemzetbiztonság számos döntését támogatták meg az elmúlt fél évszázadban ilyen elemzési segédeszközzel. Klasszikus példa erre az amerikai Vietnám-politika formálása, amelynél erősen támaszkodtak a korábbi koreai konfliktus számos tanulságára. Az ügy egyben a veszélyekre is figyelmeztet: a helytelenül megválasztott analógiák könnyen vezethetik gondolkodási tévútra az elemzőket. A nemzetközi kapcsolatok területének történetianalógia-slágere mostanában kétségtelenül az úgynevezett Thuküdidész-csapda koncepciója, ami pedig arra mutat rá: a plasztikus történelmihelyzet-hasonlatok sem mindig képesek áttekinthetőbbé, egyértelműbbé tenni az elemzendő mai helyzeteket.

Kevéssé közismert, de a kiber-nemzetbiztonság különösen fontos koncepcionális segédeszközként nyúlt már eddig is az analógiák, történeti múltban gyökerező hasonlatok eszközrendszeréhez. Elég, ha a szakterület leghíresebb metaforájára, a „Cyber Pearl Harbor” kifejezésre gondolunk, amellyel Leon Panetta akkori amerikai hadügyminiszter vetítette előre 2012-ben a kiberháború mindent elpusztító rémképét.⁴ Számunkra különösen fontos (egyben jól mutatja az analógiás történeti gondolkodásban rejlő lokálisprobléma-specifikáló erőt), hogy hazai kutatók is egy szellemes történeti metaforával (a „Digitális Mohács”-konceptió megalkotásával) a magyar közönségnek plasztikus módon vázolták fel a kibertér fenyegetéseinek perspektíváit.⁵

Az analógiás gondolkodás, amely szinte ösztönösen használt fogalomértelmező eszközünk, különösen alkalmas arra, hogy innovatív megoldásokkal segítsen át nehéz problématerületeken. A kibertérben való hadviselés egyszerűnek látszó, de valójában roppantul megosztó értelmezési feladatában mi is egy ilyen történeti

³ Specifikusan a kiberbiztonsággal kapcsolatos alkalmazhatóságot vizsgálja Reasoning by Analogy in Cyberspace. Deadly Balloons and Avoiding Digital Doom. *CFR's Blogs*, 2017. december 18. Alapmunka továbbá David Sulek – Ned Moran: What Analogies Can Tell Us About the Future of Cybersecurity. In Christian Czosseck – Kenneth Geers (szerk.): *The Virtual Battlefield. Perspectives on Cyber Warfare*. Amsterdam, IOS Press, 2009.

⁴ A koncepció gyökereit, majd pályáivét kitűnően összegzi Sean Lawson – Michael Middleton: Cyber Pearl Harbor: Analogy, Fear, and the Framing of Cyber Security Threats in the United States, 1991–2016. *First Monday*, 24. (2019), 3–4. 1–24.

⁵ Vö. Kovács László – Krasznay Csaba: Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint. *Nemzet és Biztonság*, 10. (2017), 1. 3–16.

analógiát hívunk segítségül. A választott analógia bár időben szokatlanul távoli, de kulturális kontextusában nagyon is megfogható, és így a tisztánlátásunkat előmozdító eszköz lehet a jövőben.

Modernitás és a háború új arca

A technológia, amely persze maga is egy társadalmi igény terméke, nyilvánvaló és jól ismert módon képes alakítani az emberi közösségek intézményeit és folyamatait. Talán sehol sem olyan jól dokumentált és széles körben ismert ez a visszahatás, mint a pusztítás eszköztárának és eljárásainak alakulásában. Ez az időtlen kapcsolódás mégis az ipari-tudományos forradalomtól kezdve hozott igazi változásokat. A most zajló IKT-alapú átalakulásnak, és ennek részeként az emberi fegyveres küzdelmek konceptuális transzformációjának is jó okkal kereshetjük az előképét a 19–20. század fordulójának eseményeiben.

Emlék a múltból: a stratégiai pusztítás gondolata gyökeret ver

1940. november 14-én este, a hitleri Németország 3. Légi hadseregének 515 nehéz-bombázója a magasba emelkedett. A gépek a Londontól északnyugatra elterülő Coventry városa felé vették az irányt. Lényegében ellenállás nélkül közelítették meg a mit sem sejtő települést, és pusztító bombazáport zúdítottak a páratlan műemlékekkel is rendelkező, fontos ipari központra. A terv, ma már tudjuk, nem az ipari övezetek elérése volt: a 3000 gyújtóbombával a sűrűn lakott polgári negyedeket vették célba.⁶ A város történelmi negyedei romba dőltek, a halálos áldozatok száma százakra rúgott. A II. világháború elején, az Anglia elleni német légi háború nyitó időszakában történt az eset, amely fordulópontot jelentett a légi hadviselés akkor még újnak számító gyakorlatában.

Tömegipar és a totális háború

A megelőző, 1914 és 1918 között zajló nagy háború időszakában életre hívott repülőcsapatok sokáig csak a megfigyelő, felderítő szerepet mondhatták magukénak. A két világháború közötti időszakban aztán, párhuzamosan a repülőtechnika gyors fejlődésével a világ katonai teoretikusai kutatni, vitatni kezdték a születőben levő új fegyvernem lehetséges alkalmazásait. Talán meglepő, de egy itáliai tábornok, Giulio

⁶ A légi offenzíva átfogó összegzését hozza Tami Davis Biddle: *Rhetoric and Reality in Air Warfare*. Princeton, Princeton University Press, 2002.

Douhet képzeletében fogant meg először a gondolat, hogy a repülő szerkezetek, erős robbanóanyagokat szállítva, az arcvonalak fölötti egyszerű csetepatéknál sokkal drámaibb módon is befolyásolhatnák a hadviselés menetét. Az olasz generális *Az égbolt meghódítása* című meghatározó könyvében a stratégiai bombatámadások elméletét fektette le. Azt vallotta: az új hadszíntér, a levegőég eme új fegyverei, a repülőgépek egymagukban képesek lehetnek eldönteni a jövőben a háborúk kimenetelét. Nem azt állította, hogy az új fegyverek, a távolból felemelkedve és megközelítve a célt, képesek teljesen romba dönteni annak infrastruktúráját. Douhet a tömegbombázások morális eszközként való alkalmazásában hitt: azt állította, hogy a polgári célpontok, mai szavunkkal a kritikus infrastruktúrák elleni tömeges támadások képesek lehetnek arra, hogy megtörjék az ellenség harci kedvét, lelkierejét. Az olasz katonai gondolkodó a totális háború elvét rajzolta fel, ahol mindenki, az egész társadalom harcoló fél, egyben ellenség.⁷

Az új gépezetek és a majdani harcaiknak teret adó „levegőég” persze még újdonságnak számítottak. Valahogy úgy, mint napjainkban a kibertér és benne a különféle támadó szoftverek, a sokat emlegetett kiberfegyverek. Nem voltak még a gyakorlat által kitaposott ösvények, és az elméleti vitákban különböző elképzelések csaptak össze arról, hogyan lenne a legcélszerűbb felhasználni ezeket a modern innovációkat. A kiforratlan alkalmazás, a koncepciók sokfélesége jellemezte az 1939-ben kirobbant második nagy világégés első időszakát. A technológiai kételyek mellett elsősorban morális szempontok korlátozták az új lehetőségek ilyen példátlan pusztítást hozó alkalmazását, amelyet Douhet tábornok javasolt elméletében. A kezdetben szintén a kizárólag katonai jellegű pontcélok bombázására koncentráló brit légügyi vezetők az első háborús hónapok szorongatottságában a polgári célpontok, német városok tömeges pusztítását vetették fel, ám a példátlan lépés sokakat elriasztott ettől a fordulattól. A háború utáni időkben merült fel az elmélet: valójában a brit vezetés különböző hírszerzési forrásokból előre értesült a Coventry elleni közelgő német támadásról, mégsem hozott intézkedéseket a polgári lakosság megóvására. A feltételezés az: egy ilyen tömeges katasztrófával akarták megalapozni a közvéleményben az általuk tervezett stratégiaváltást. A történészi vita máig sem zárult le, egy dolog azonban biztos: Coventry drámája fordulópontot hozott a brit bombázóparancsnokság háborús stratégiájában.⁸ Három és fél évvel később Németország települései romhalmazzá váltak.

⁷ Az 1930-as évek nagy stratégiai közvitáit tekinti át, bemutatva és értékelve a korszak legjelentősebb újítója, Douhet munkásságát Thomas Hippler: *Bombing the People. Guido Douhet and the Foundations of Air Power Strategy, 1884–1939*. Cambridge, Cambridge University Press, 2013.

⁸ Richard Overy: *The Bombers and the Bombed. Allied Air War over Europe, 1940–1945*. New York, Viking, 2015.

Háború a kibertérben – vagy valami más?

Napjaink szakértői és döntéshozói is a konfliktusok jellegét kutatják, a technológia hátán érkező új lehetőségek hadi alkalmazhatóságát latolgatják. Az egyik tábor az összecsapásokat forradalmasító eszköznek látja a kiberarzenált, akár a II. világháborúban városokat eltörlő bombázó armádiákat. Mások a korlátokra figyelmeztetnek, és tagadják a digitális Armageddon rémképét.

A digitalizáció Douhet tábornokai – a héják

A nagy bombázó offenzívákról felvillantott iménti kép, és ezen belül is bizonyára a pesszimistább perspektíva ötlött a kiber-nemzetbiztonság szakembereinek jó része eszébe, amikor 2022 februárjában megindultak az orosz csapatok Ukrajna ellen. Pontosabban: a hosszú ideje prognosztizált, ám mindeddig elmaradt elsőprő kibervégítélet kapcsán. A szakma lényegében az orosz invázió megkezdődése óta azt kérdegetti: hol marad a mindent elsőprő – és a tankoszlopokat, repülőgépeket megelőző, sőt azokat feleslegessé tevő – digitális csapás?⁹ A mindent eldöntő, új hadialkalmazás, azaz a „kiberháború”? A kiberbiztonsági szakma, a katonai vezetések és a politikusok évek óta mondják, hogy a geopolitikai szembenállás legújabb terepe, a kibertér uralására koncentráló Oroszország pusztító csapással avatja majd fel a 21. század új kiberharcmodorát, amint összeütközésbe kerül a Nyugattal. A feltételezés természetesen nem volt alaptalan, hiszen az elmúlt években, de inkább évtizedben jó néhány olyan incidensre került sor a kibervilágban, amelyeket az orosz állam intézményeihez kapcsol a biztonsági szakma. Az Ukrajnával kirobbant véres és elhúzódó konfliktusuk pedig 2014 óta az orosz állami hackerszervezetek egyfajta kísérleti terepévé, laboratóriumává tette a szomszédos országot. Az eddigi időszak egyik legveszélyesebb és globális szinten is roppant károkat okozó kibertámadása és a középpontjában álló hírhedt NotPetya kiberkártévő is az ukrainai polgári infrastruktúrák elleni orosz hackertámadással indult útjára 2017-ben. Szakmai körökben tehát meglehetősen erősen elterjedt az a feltételezés, hogy egy eljövendő fegyveres összetűzésnek is fontos kísérője (talán eldöntője) lesz a számítógépes infrastruktúra, elektronikus igazgatási és kereskedelmi rendszerek elleni koncentrált támadás. Azóta, hogy két amerikai tudós, a RAND kutatói közreadták mérföldkönek számító tanulmányukat, a hadviselés gyökeres átalakulását hirdető digitális stratégiák evangelisták száma egyre növekedett a világban. John Arquilla és David Ronfeld 1993-ban publikált könyve már a címevel meghatározta a közgondolkodást:

⁹ Vö. Ukrainian President Speaks Amid Russian Invasion; Troop, Military Vehicles Enter Ukraine from Belarus; Ukraine Hit by Wave of Cyberattacks as Invasion Begins. Aired 4:30-5a ET. *CNN.com – Transcripts*, 2022. február 24.

Cyberwar Is Coming (A kiberháború eljövetele), hirdette a gyorsan népszerűvé vált munka, amely mély nyomokat hagyott a 21. század stratégiai gondolkodásmódján.¹⁰

Elemzők és ellenzők – a realista galambok

A „kibertér Douhet-jeivel”, a kiberháború elkerülhetetlenségét hirdetőkkal szemben mindig is jelen volt és hallatta szavát egy másik szakmai elképzelés is.¹¹ A kibertérben folyó katonai műveletek lehetséges szerepének túlértékelése ellen felszólaló brit képviselő, a honvédelmi bizottságot vezető Tobias Ellwood velősen így fogalmazta meg ezt a „kiberszkeptikus” álláspontot: „kiberfegyverekkel senki nem foglalhat el egy országot. Tankkal viszont igen.” A kibertér háborús lehetőségeinek korlátozott voltát aztán remekbe szabott tanulmányában járta körbe Thomas Rid, a digitális hadviselés egyik legjobb szakértője.¹² Munkájának a címe (amely később könyv formájában is megjelent) világosan tükrözi álláspontját: *Cyberwar Will Not Take Place*. A mű meggyőző érveléssel állítja: „A kiberháború nem fog beköszönteni!” Elemzését a háború klasszikus értelmezésétől indítva Rid leszögezi: a kiber-műveletek nem képesek olyan értelemben kárt okozni, embert ölni, mint a hagyományos fegyverek. A kibertér akcióinak természetesen van hatása: diszruptív, zaklató, „nyirbáló” jellege tagadhatatlan, ám ez messze nem azonos a klasszikus értelemben vett „háború” eszközeinek és eljárásainak pusztító jellegével. A koncepció ilyen jellegű újragondolói közül külön is érdemes kiemelni két kutató munkásságát: Lennart Maschmeyer és Nadiya Kostyuk elgondolkodtató és gazdag tényanyagra építő tanulmányaikban bizonyítják a kiberhadviselés szubverzív jellegét.¹³ Háborús „fegyvernek” nem alkalmas – de zaklatni, nyugtalanítani, zavart kelteni, felderíteni kiválóan felhasználható.¹⁴ Nem véletlen tehát, vallja a szakemberek egy meglehetősen népes (és érvelését meggyőző empirikus kutatási anyaggal is megtámogató) csoportja, hogy a fegyveres harc kirobbanását nem kísérte egy „mindent elsőprő”, az ellenfelet szinte puskalövés nélkül térdre kényszerítő „kiberháború”: a rettegett kiber-Armageddon nem következett be. A kiber-nemzetbiztonság, konfliktuskutatás kiemelkedő szakembere, az amerikai Brandon Valeriano talán a legfontosabb

¹⁰ John Arquilla – David Ronfeldt: *Cyberwar is coming! Comparative Strategy*, 12. (1993), 2. 141–165.

¹¹ Különösen érdekes, mivel a gyakorló kiberbiztonsági felsővezető szemszögéből láttatja és értékeli az eseményeket, Ciaran Martin: *Cyber Realism in a Time of War. Lawfare Blog*, 2022. március 2.

¹² Thomas Rid: *Cyberwar Will Not Take Place*. Oxford, Oxford University Press, 2013.

¹³ Átfogó és sok szempontból úttörő munka Lennart Maschmeyer: *Slow Burn. Subversion and Escalation in Cyber Conflict and Covert Action*. Toronto, University of Toronto, 2020.

¹⁴ Különösen meggyőzően érvel az ilyen műveletek „nem-háborús” klasszifikációja mellett Nadiya Kostyuk – Yuri M. Zhukov: *Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events? Journal of Conflict Resolution*, 63. (2017), 2. 1–44.

összegzését adta a témának kollégájával, Ryan Maness-szel közösen írt munkájában.¹⁵ A könyv, igazodva a szerző évtizedes kutatási területéhez, az elsők között dolgozza fel empirikus adatokra támaszkodva a kibertér változatos akcióit és támadásait, és a kemény tényekre alapozva utasítja el az új hadügyi forradalmat vizionáló „kiber-Douhetek” szenzacionalistának tekintett álláspontját. A már említett Nadiya Kostyuk szintén több évtized kiberakcióinak empirikus adatait vizsgálva kereste a bizonyítékot arra, hogy az ilyen műveletek a „valódi” (kinetikus) katonai akciót helyettesítők voltak-e (tehát ténylegesen „kiberháborúnak” tekinthető eseménysorok), vagy inkább a fizikai támadásokkal összehangolt, azokat kiegészítő lépések. Kostyuk megállapítása meglepő: sem az egyik, sem a másik alkalmazást nem támasztják alá a tényleges adatok. Inkább jellemző az, hogy a kiberakciókra és a kinetikus fegyveres mozdulatokra egymástól függetlenül került sor.¹⁶ A kiberműveletek tehát, állítja a kutató, jellemzően nem a „háború” állami eszköztárának részét képezik.¹⁷

Eszközök, emberek és integrációk. A hadviselés új paradigmái a kibertérben

Noha a csúcstechnológiájú hagyományos (vagy nukleáris) fegyverzetek árához képest a támadó kiberkapacitások csupán szerény ráfordításokat igényelnek, tévedés volna alábecsülni ennek mértékét. A komoly kibertámadások összetett csapatokat, magas szakértelmű közreműködőket, fejlett eszközöket igényelnek – és mindezt hosszú időn át. A kiberfegyverek háborús alkalmazhatóságát ráadásul számtalan körülmény korlátozza.

Időzíthetőség, kontrollálhatóság, integrálhatóság

Ahogy azt feljebb láttuk, a szakértők egy része határozottan állítja, hogy a rosszindulatú számítógépes programok tényleges háborúra kevésbé alkalmasak. Súlyosan nehezíti a tényleges hadi alkalmazhatóságukat az időzítés kérdése. Bár mindegyik eset egyedi, a szakemberek szerint átlagosan két-három évig is eltarthat egy komoly kibertámadás előkészítése és végrehajtása. Ennek összehangolása (a szokásos gyakorlat szerint adott időpontokban induló és végrehajtandó) hagyományos katonai hadmozdulatokkal gyakorlatilag lehetetlen. A tetemes időigény és a pontos időzítés

¹⁵ Brandon Valeriano – Ryan C. Maness: *Cyber War versus Cyber Realities. Cyber Conflict in the International System*. Oxford, Oxford University Press, 2015.

¹⁶ Vö. Nadiya Kostyuk – Erik Gartzke: Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine. *Texas National Security Review*, 5. (2022), 3. 113–126.

¹⁷ Vö. még Lennart Maschmeyer: A New and Better Quiet Option? Strategies of Subversion and Cyber Conflict. *Journal of Strategic Studies*, 2022. július 27.

korlátai már eleve kétségesse tennék ezeknek az eszközöknek a háborús eszközként való alkalmazását.¹⁸

Hasonlóan komoly problémát jelent a hadi alkalmazás szempontjából az a körülmény, hogy nagyon nehéz előre pontosan meghatározni az akcióval kiváltott hatásokat. Amíg például egy rakétacsapás által előidézett kár viszonylag pontosan felbecsülhető, addig ez a kiberfegyverek alkalmazásakor több szempontból is problémás lehet. Ehhez kapcsolódik az egyik legsúlyosabb alkalmazási nehézség: a rendkívül tökéletlen kontrollálhatóság. Ez annyit jelent, hogy az okozott kár sok esetben nem szűkíthető egyetlen kiválasztott célpontra. A globális konnektivitás révén az ilyen informatikai károkozók könnyen „kiszabadulhatnak”, majd a világhálón tovaterjedve ellenőrizhetetlen pusztítást végezhetnek – akár az akciót indító állam rendszereit is megfertőzve. A korábban említett NotPetya támadás éppen ezzel az utóhatásával okozta a legnagyobb riadalmat szakmai körökben. A nehéz kontrollálhatóság az Ukrajna elleni invázióhoz kapcsolódó kiberműveletekben ismét előbukkant. A fegyveres támadás megindulásával egy időben az ukrainai internetes kommunikáció egy részét biztosító Viasat műholdas rendszere, a KA-SAT ellen (véltetően oroszok által) bevetett számítógépes kártevő is gyorsan „elszabadult”. A rosszindulatú program azután sokfelé okozott károkat.

Eredményesség

A Viasat rendszerei elleni támadás még egy fontos körülményre felhívta a figyelmet. A kiberakcióval megtámadott modemek jelentős része (egyszerű, a cég központjából hálózaton át végzett szoftveres javítással) ismét működőképes volt tehető, és a szolgáltatás alig néhány órnyi kiesés után zavartalanul folytatódott. Az érintett vevődobozok egy számottevő része javíthatatlan károkat szenvedett; azonban ezek kicserélése is csupán néhány napot vett igénybe. Tehát: a hosszas előkészítéssel indított és hatását tekintve nehezen fókuszálható kibernetikus támadás viszonylag olcsón és gyorsan javítható károkat okozott csupán.¹⁹ A tényleges katonai alkalmazhatóság kritériumainak érvényesülését ugyanakkor jól példázza a 2022 őszén indított és az ukrán energetikai rendszer pusztítását, lassítását, rombolását célzó hagyományos támadássorozat. Két nap előkészítés és néhány tucat cirkálórakéta ráfordítása elégséges volt ahhoz, hogy Oroszország hosszú időre működésképtelenné tegye becslések szerint az ukrán energetikai hálózat 30%-át.

¹⁸ Vö. Max Smeets: A Matter of Time: On the Transitory Nature of Cyberweapons. *Journal of Strategic Studies*, 41. (2018), 1–2. 6–32.

¹⁹ Számtalan szerző emeli ki, hogy a kibertérben zajló műveletek stratégiai eredményessége (eredménytelensége) alapvető (mérhető) támpontot adhat az ilyen akciók jellegének megítélésében, a „háború”, vagy valami más dilemmájának tisztázásában. Vö. Richard J. Harknett – Max Smeets: Cyber Campaigns and Strategic Outcomes. *Journal of Strategic Studies*, 45. (2022), 4. 1–34.

Adott célpontok elleni, időzített és legfeljebb kisebb mértékű nemkívánatos következményekkel járó támadásokra tehát összehasonlíthatatlanul alkalmasabbnak látszanak a hagyományos fegyverzetek.

Dilemmák és trilemmák

A kiberharc megvívásához kapcsolódó alapvető paraméterek közötti sajátos összefüggés bemutatására a téma egyik legismertebb kutatója, a zürichi Lennart Maschmeyer szellemes sémát szerkesztett.²⁰ Tézise szerint egy akció stratégiai hasznosságának feltétele az, hogy mérhetően hozzájáruljon az állami célok eléréséhez (vagy az erőegyensúly megváltozásához). Maschmeyer az intenzitást, a végrehajtás gyorsaságát és a kontrollálhatóságot tekinti olyan változóknak, amelyek a kiberművelet operatív eredményessége szempontjából kulcsfontosságúak. Felállítja azt a tételt, hogy egyszerre e három változóból legfeljebb kettő maximalizálható. A végrehajtás gyorsaságát és az akció hatásosságát növelve arányosan csökken annak kontrollálhatósága. Ez annyit jelent, hogy az operatív szempontból használható sebességgel és megfelelő intenzitással végrehajtott kibertámadás nagy eséllyel csúszhat ki az akciót végrehajtó ellenőrzése alól. A nemkívánatos következmények pedig nemcsak csökkentik az akció stratégiai értékét, de egyenesen önveszélyessé is tehetik a műveletet. Egy másik kombinációt figyelembe véve, a végrehajtás sebességét maximalizálva, ám ugyanakkor az ellenőrizhetőség kívánalmát is szem előtt tartva a támadó jó eséllyel lesz kénytelen értékelhető szint alá csökkenteni az akció intenzitását (azaz csupán csekély, vagy semmilyen stratégiai hatást nem lesz képes kiváltani a művelet). Ha pedig a hatásosságot és az ellenőrzés alatt tartást maximalizálná a végrehajtó (elméletileg e két paraméter teljesülése szolgálná a leginkább a stratégiaiilag számottevő eredményességet), úgy az a kivitelezés gyorsaságát csökkentené a használhatóság határa alá.

Célok

A szubverzív elméleten túl más elképzelések is születtek a kiberhadviselés mibenlétére vonatkozóan. Érdekes Benson fogalomrendje: ő a nemzetközi kapcsolatok értelmezési keretrendszerében próbál választ adni a kiberműveletek jellegére vonatkozó kérdésre.²¹ A külpolitika-elmélet legközpontibb fogalmával, az erőegyensúly

²⁰ Lennart Maschmeyer: The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations. *Journal of International Security*, 46. (2021), 2. 51–90.

²¹ Egyben a kiberhadviselés és a nemzetközi kapcsolatok szélesebb kontextusát is bemutatja. David Benson: Not Cyberwar, but Cyberbalance. *Aether. A Journal of Strategic Airpower and Spacepower*, 1. (2022), 2. 81–96.

kérdésével kapcsolja össze a kiberfegyverekkel folytatott műveleteket. Feltételezése az, hogy a kibertérben folyó műveletek célja valójában nem a másik fél megsemmisítése. Sokkal inkább az (adott térségben, adott időben fennálló) erőegyensúly megváltoztatása, eltolása az egyik (vagy több) fél képességeinek megnyírbalása, meggyengítése által. Az elmélet erőssége az, hogy a nemzetközi kapcsolatok rendszerét a maga összetettségében látja és értelmezi, amely szereplők egész sorának bonyolult kapcsolatain alapuló egyensúly formájában működik. Az ilyen koncepció különösen a multipolárisra váló világrenden belüli értelmezésekhez jelenthet hatékony keretet. Benson érvelése az, hogy számos kibertámadás valójában a nemzetközi struktúra egyensúlyrendjének megváltoztatására irányul; célja az egyik (vagy több fél) „hátrányosabb helyzetbe hozása” (*handicapping*).

Janicsárok kontra akindzsik: lehetséges magyarázó analógiák

Mint láttuk, a kibertér hadviselését vizsgáló kutatók egy része kétségbe vonja az ilyen akciók „háború” jellegét. Sőt, elemzéseikben feltételezik, hogy az ilyen eszközcsoport nem is alkalmas hagyományos háborúk megvívására, de még közvetlen támogatására sem. Nagyon is alkalmas eszköznek látszik azonban a zaklató, felforgató tevékenységek céljára. Ezen kutatási érvrendszer összegzésére, értelmezési keretbe helyezésére alkalmasnak gondoljuk a történeti analógiákat segítségül hívó munkamódszert.²² A közelmúltban – a jellegzetes amerikai, atlanti környezet tapasztalataihoz igazodva – különösen érdekes alapvetés született: a kiváló oxfordi kutató, Florian Egloff a 18–19. századi atlanti vizek kalózkodásának jellemzőivel vetette össze (világította meg) a kibertérben folyó műveletek irreguláris jelenségtartalmát.²³

Mi egy, a saját történeti-kulturális környezetünkhöz jobban illeszkedő (ezért számunkra plasztikusabb) történeti analógiát felhasználva, a 16–17. századi magyarországi határvidéki életforma, a végvári harcok ikonikus katonaalakját hívjuk segítségül²⁴ az oszmán török hadszervezet egyik pillére, a könnyű fegyverzetű, sokszor fegyelmezetlen könnyűlovás, az akindzsi személyében, aki mintegy ellentéte a képzett, fegyelmezett, reguláris janicsárnak.²⁵ A janicsár a háborúk központi

²² A hódoltság kori magyarországi hadtörténet egyik klasszikusa Hegyi Klára, aki számos munkában dolgozta fel a problémakört. Például Hegyi Klára: *The Ottoman Military Organization in Hungary. Fortresses, Fortress Garrisons, and Finances*. Belin, Klaus Schwartz Verlag, 2018.

²³ Vö. Florian J. Egloff: *Cybersecurity in the Age of Privateering*. Oxford, Oxford University Press, 2015.

²⁴ A téma bőséges szakirodalmában máig alapmunka Caroline Finkel: *The Administration of Warfare: the Ottoman Military Campaigns in Hungary, 1593–1606*. Wien, VWGÖ, 1988.

²⁵ Ágoston Gábor: *The Last Muslim Conquest. The Ottoman Empire and Its Wars in Europe*. Princeton, Princeton University Press, 2021.

alakja; a „száguldó és égető” akindzsi viszont a hosszú „se nem béke, se nem háború” időszakok, a szürkezóna harcosa.

16–17. századi geopolitikai élet-halál harc és az oszmán hadművészet

A történelmünkben jól ismert 150 évnyi időszak, a hódoltság, a végvári harcok kora tulajdonképpen egy generációkon átívelő „határvidéki világot” teremtett meg a korabeli Magyar Királyság jókora részén.²⁶ Háború (a kor fogalmai és a mi kategóriáink szerint) csupán rövid időszakokra lángolt fel; a hosszú századok idejének zömében „béke” uralkodott itt, vagy pontosabban: „nem háború”. A 100–130 erősségből álló török peremvonallal ugyanennyi magyar vár nézett szembe. Az őrség védelméből gyakran csaptak ki a könnyűlovas akindzsik. Feladatuk hármas volt: állandó felderítéssel segítették a saját oldalukat (hírszerző funkció); időről időre összezsúptak az ellenség kisebb alakulataival (erőlekötő és figyelemelterelő funkció), végül pedig folyamatosan nyugtalanították, zaklatták az ellenfél civiljeit (lélektani hadviselési funkció). Az irreguláris harcmódor mesterei voltak. Nem a háború eszközei voltak (többszörre a szürke „nem háborús” időkben portyáztak), nem az ellenfél legyőzése, hanem annak meggyengítése, elbizonytalanítása volt a küldetésük.

Irregulárisok a kibertérben: a „szürkezóna” hadműveletei

Visszakanyarodva a jelenbe: az Ukrajnában zajló konfliktus egyfajta iskolapéldája annak az újfajta harcmódnak, amely az utóbbi években sokfelé jellemzi a geopolitikai szembenállások új világát.²⁷ Olyan komplex konfliktusrendszereknek vagyunk tanúi, ahol eszközök és alkalmazási módok sokasága keveredik. Hagyományos háború jellegű fegyveres harc; propagandára és dezinformációra építő információs hadviselés; a másik fél informatikai rendszereinek megzavarását, blokkolását célzó kiberakciók; pénzügyi-kereskedelmi korlátozások és szankciók. Sokfajta és különböző intenzitású eszközt és eljárást vetnek be a szemben álló felek, akár egy időben is.²⁸ Ez a hibrid háború, amelyet a hagyományos fegyveres harc fogalmaival sokszor értelmezni is nehéz. A nyugati szakirodalom az úgynevezett „szürkezónás” (*grey*

²⁶ Vö. Ágoston Gábor – Bruce Masters (szerk.): *Encyclopedia of the Ottoman Empire*. New York, Facts on File, 2009. A kitűnő általános összefoglaló a társadalmi-politikai kontextus mellett a hadszervezésre is jó forrás.

²⁷ Sacha-Dominik Bachmann – Hakan Gunneriusson: Hybrid Wars: the 21st-century's New Threats to Global Peace and Security. *Scientia Militaria, South African Journal of Military Studies*, 43. (2015), 1. 77–98. Egyben jó bemutatása a hibrid háború és az úgynevezett szürkezónás műveletek összefüggésének.

²⁸ A hibrid hadviselésen belüli kiberkomponensek kapcsolódási pontjai mellett az utóbbiak „hadjáratformáló” szerepét emeli ki Florian J. Egloff – Lennart Maschmeyer: *Shaping Not Signaling*:

zone) hadviselésről is beszél: arról a posztmodern világunkra jellemző se nem háború, se nem béke állapotról, ahol az ellenfél elbizonytalanítását, meggyengítését, szándékainak és lehetőségeinek kifürkészését célzó akciók vannak túlsúlyban. Erre a célra pedig (az információs hadviseléssel kombinálva) különösen alkalmasnak látszanak a kiberfegyverek. Annál az egyszerű oknál fogva, hogy a digitalizáció által szinte átitatott társadalmaink biztonsága és magabiztossága épül ma már éppen azokra a technológiákra, amelyeket könnyűszerrel vehetnek célba ezek a (halált, fizikai pusztulást nem, de fennakadást, zűrzavart, bizonytalanságot, félelmet okozó) újszerű fegyverek. Tehát a társadalmakat megbénító, térdre kényszerítő, távolról vezérelt „kiberháború” koncepciója talán túlzó rémkép.²⁹ De a kiberfegyverek veszélyessége nagyon is valóságos.

Prolifерáció – a digitális tér „atomfegyverei” helyett a kiberterek „piszkos bombája”?

Ha egyszer majd sikerül az ukrajnai háború fegyveres részét lezárni, az még nem feltétlenül jelenti majd, hogy a szellemet vissza lehet tuszkolni a palackba. Az akciók és a fegyverzetek „társadalmasításával” újabb veszélyforrás is rászabadulhat a társadalmakra: a kiberfegyverzetek proliferációja, elterjedése. A háború sajátos kísérőjelenségeként egy „párhuzamos” kiberhadjárat is kibontakozott a hadműveletek első hetétől kezdve: nehezen beazonosítható magánosok (régóta ismert hackercsoportok, kiberaktivisták, illetve vélhetően egyéni „kiber-revolverhősök”) egész serege kapcsolódott be az online terekben folyó küzdelmekbe. A különféle szervezett és magános hacktivisták mellé felzárkóztak az ukrán állam által szervezett „IT-hadsereg” emberei is. A számok természetesen ellenőrizhetetlenek, ám az ukrán források több százezres kiber-közreműködői „seregéről” beszélnek. Az általuk bejelentett akciók jó részét sem erősítette meg senki. Ugyanakkor ezek a kiberszabadcsapatok ténylegesen ellenőrizhető támadásokat is szép számmal hajtanak végre. Ezek egy része különösebb szakértelmet, szofisztikáltságot (illetve erőforrásokat) nem igénylő, túlterheléses támadás (DDoS), vagy főleg a kezdeti időkben egyszerű webhelyelcsúfítás (*defacing*) volt. Viszonylag hamar megjelentek az adatszivárogtatásos akciók, majd az adattörlések is, a szakemberek véleménye szerint azonban ezek a megmozdulások általában semmiféle komoly fennakadást, kárt vagy sérülést nem okoznak a megtámadott félnek, ez az első napokban döntően az orosz állami és gazdasági szervezetek köréből kikerülő intézményeket jelentette. Időközben aztán a kibertér eme betyárscsapatai

Understanding Cyber Operations as a Means of Espionage, Attack, and Destabilisation. *International Studies Review*, 23. (2021), 3. 997–998.

²⁹ A megállapítás mellett a gyakorló kibervédelmi szakma jeles képviselői is kiálltak, méghozzá az Ukrajna elleni orosz invázió időszakában rögzített esetekre alapozva. Vö. William Turton: *Man-diant Executive Cautions against Russia-Cyberattack Panic*. *Bloomberg*, 2022. február 15.

között megjelentek az Oroszországot támogató és az ukrán állami és gazdasági szervezeteket támadó „alakulatok” is. Az ő esetükben is többnyire igaz: ténykedésük inkább csak felszínes zaklatásnak tekinthető.³⁰

Fegyverek helyett normák: a kibertér deeszkalálásának kísérletei és esélyei

A kibertérben zajló, egyre intenzívebb, egyre nagyobb károkat okozó akciók magas szintre emelték az ilyen incidensek nemzetbiztonsági kockázatát. Ezért aztán erősödnek a törekvések – nemzetállami szinten és a nemzetközi közösségben is – a kibertérben való működés, a támadó kiberakciók szabályozására.

A kibertér, a látszat ellenére, nem valamiféle „technológiai Vadnyugat”. Léteznek normák, jól kigondolt, világos szabályok az itt zajló konfliktusokra, a követendő vagy tiltott magatartásokra. A nyugati szövetség tagjai például közös szabályrendszert dolgoztak ki a kiberháborús helyzetek szabályozására. A Tallini kézikönyvekhez hasonló normarendszereken dolgozik az országok jóval szélesebb körét átfogó ENSZ is.³¹ Az összes ilyen jogi eszköz gyenge pontja viszont az, hogy ezek nem kényszerítő erővel bíró megállapodások.

A digitális terekben elmérgesedő helyzet ugyanakkor valamiféle megegyezés kényszerét is magában hordozza. A geopolitikai rivalizálás szemben álló pólusai ebben a tekintetben is más koncepciót vallanak magukénak. Amíg az oroszok és a kínaiak a támadó szoftverek szabályozására fókuszálnának, az amerikaiak konzekvensen elutasítják az ilyesfajta „kiberfegyverzet-korlátozási megállapodás” gondolatát. Mint mondják, az eredendően kettős rendeltetésű kibereszközök világában ez lehetetlen feladat lenne. Noha van ebben egy adag igazság, nem indokolatlan annak a feltételezése sem, hogy az USA nem szívesen korlátozná magát ezen a kulcsfontosságú harcmezőn. Az amerikai megközelítés, ennek megfelelően, nem a kibertér fegyverzeteinek, hanem inkább a támadható célpontoknak a körét szeretné szabályozni, korlátozni.

Az ezen a téren Biden és Putyin tárgyalásai nyomán 2021-ben megindult lassú egyezkedés a konfrontatív attitűd felülkerekedése, majd az ukrán konfliktus elmérgesedése miatt megtorpant. A kedvezőtlen kilátások ellenére bizakodásra készítenek viszont a háború eddigi eseményei: az, hogy semelyik fél sem vállalkozott arra, hogy pusztító támadást indítson a másik kritikus infrastruktúrái ellen.

³⁰ A kiberfegyverek illegális terjedésével kapcsolatban a nemzetközi rendőri vezetők már megkongatták a vészharangot. Vö. Ryan Browne: Military-Made Cyberweapons Could Soon Become Available on the Dark Web, Interpol Warns. *CNBC*, 2022. május 23.

³¹ A kiberdiplomáciai törekvések számunkra érdekes európai dimenzióját összegzi Molnár Dóra: *Törékeny nagyhatalmítás: a kiberbiztonság. Az európai kibertér brit, német és francia szegmensei*. Budapest, Nemzeti Közszolgálati Egyetem, 2018.

Egyszerűen megfogalmazva: ahogy a fizikai hadszíntéren is óvakodnak attól, hogy háborús oknak tekinthető gesztusokat tegyenek, a kibertérben sem ragadtatják el magukat ilyen végzetes lépésre. A kibertér talán mégsem a háború közege.

Felhasznált irodalom

- Ágoston, Gábor: *The Last Muslim Conquest. The Ottoman Empire and Its Wars in Europe*. Princeton, Princeton University Press, 2021.
- Ágoston, Gábor – Bruce Masters (szerk.): *Encyclopedia of the Ottoman Empire*. New York, Facts on File, 2009.
- Arquilla, John – David Ronfeldt: Cyberwar Is Coming! *Comparative Strategy*, 12. (1993), 2. 141–165.
- Bachmann, Sacha-Dominik – Hakan Gunneriusson: Hybrid Wars: The 21st-century's New Threats to Global Peace and Security. *Scientia Militaria, South African Journal of Military Studies*, 43. (2015), 1. 77–98. Online: <http://dx.doi.org/10.2139/ssrn.2506063>
- Benson, David: Not Cyberwar, but Cyberbalance. *Aether. A Journal of Strategic Airpower and Spacepower*, 1. (2022), 2. 81–96.
- Biddle, Tami Davis: *Rhetoric and Reality in Air Warfare*. Princeton, Princeton University Press, 2002.
- Browne, Ryan: Military-made Cyberweapons Could Soon Become Available on the Dark Web, Interpol Warns. *CNBC*, 2022. május 23. Online: www.cnn.com/2022/05/23/military-cyber-weapons-could-become-available-on-dark-web-interpol.html
- Egloff, Florian J.: *Cybersecurity and the Age of Privateering*. Oxford, University of Oxford, 2015.
- Egloff, Florian J. – Lennart Maschmeyer: Shaping Not Signaling: Understanding Cyber Operations as a Means of Espionage, Attack, and Destabilisation. *International Studies Review*, 23. (2021), 3. 997–998. Online: <https://doi.org/10.1093/isr/viaa086>
- Finkel, Caroline: *The Administration of Warfare: the Ottoman Military Campaigns in Hungary, 1593–1606*. Wien, VWGÖ, 1988.
- Gartzke, Erik: The Myth of Cyberwar. *International Security*, 38. (2013), 2. 41–73.
- Harknett, Richard J. – Max Smeets: Cyber Campaigns and Strategic Outcomes. *Journal of Strategic Studies*, 45. (2022), 4. 1–34. Online: <https://doi.org/10.1080/01402390.2020.1732354>
- Hegyí, Klára: *The Ottoman Military Organization in Hungary. Fortresses, Fortress Garrisons and Finances*. Berlin, Klaus Schwarz Verlag, 2018.
- Hippler, Thomas: *Bombing the People. Guido Douhet and the Foundations of Air Power Strategy, 1884–1939*. Cambridge, Cambridge University Press, 2013.
- Kostyuk, Nadiya – Erik Gartzke: Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine. *Texas National Security Review*, 5. (2022), 3. 113–126. Online: <http://dx.doi.org/10.26153/tsw/42073>
- Kostyuk, Nadiya – Yuri M. Zhukov: Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events? *Journal of Conflict Resolution*, 63. (2017), 2. 1–44. Online: <https://doi.org/10.1177/0022002717737>
- Kovács László – Krasznay Csaba: Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint. *Nemzet és Biztonság*, 10. (2017), 1. 3–16.
- Lawson, Sean – Michael Middleton: Cyber Pearl Harbor: Analogy, Fear, and the Framing of Cyber Security Threats in the United States, 1991–2016. *First Monday*, 24. (2019), 3–4. 1–24.

- Martin, Ciaran: Cyber Realism in a Time of War. *Lawfare Blog*, 2022. március 2. Online: www.lawfareblog.com/cyber-realism-time-war
- Maschmeyer, Lennart: *Slow Burn. Subversion and Escalation in Cyber Conflict and Covert Action*. Toronto, University of Toronto, 2020.
- Maschmeyer, Lennart: The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations. *Journal of International Security*, 46. (2021), 2. 51–90. Online: https://doi.org/10.1162/isec_a_00418
- Maschmeyer, Lenart: A New and Better Quiet Option? Strategies of Subversion and Cyber Conflict. *Journal of Strategic Studies*, 2022. július 27. Online: <https://doi.org/10.1080/01402390.2022.2104253>
- Molnár Dóra: *Törékeny nagyhatalmiség: a kiberbiztonság. Az európai kibertér brit, német és francia szegmensei*. Budapest, Nemzeti Közzolgálati Egyetem, 2018.
- Overy, Richard: *The Bombers and the Bombed. Allied Air War over Europe, 1940–1945*. New York, Viking, 2015.
- Reasoning by Analogy in Cyberspace. Deadly Balloons and Avoiding Digital Doom. *CFR's Blogs*, 2017. december 18. Online: www.cfr.org/blog/reasoning-analogy-cyberspace-deadly-balloons-and-avoiding-digital-doom
- Rid, Thomas: *Cyber War Will Not Take Place*. Oxford, Oxford University Press, 2013.
- Sharma, Amit: Cyber Wars: A Paradigm Shift from Means to Ends. *Strategic Analysis*, 34. (2010), 1. 67–73. Online: <https://doi.org/10.1080/09700160903354450>
- Smeets, Max: A Matter of Time: On the Transitory Nature of Cyberweapons. *Journal of Strategic Studies*, 41. (2018), 1–2. 6–32. Online: <https://doi.org/10.1080/01402390.2017.1288107>
- Sulek, David – Ned Moran: What Analogies Can Tell Us About the Future of Cybersecurity. In Christian Czosseck – Kenneth Geers (szerk.): *The Virtual Battlefield. Perspectives on Cyber Warfare*. Amsterdam, IOS Press, 2009.
- Turton, William: Mandiant Executive Cautions Against Russia-Cyberattack Panic. *Bloomberg*, 2022. február 15. Online: www.bloomberg.com/news/articles/2022-02-15/mandiant-executive-warns-of-cyber-panic-we-need-to-get-a-grip
- Ukrainian President Speaks Amid Russian Invasion; Troop, Military Vehicles Enter Ukraine from Belarus; Ukraine Hit by Wave of Cyberattacks as Invasion Begins. Aired 4:30–5a ET. *CNN.com – Transcripts*, 2022. február 24. Online: <https://transcripts.cnn.com/show/cnr/date/2022-02-24/segment/22>
- Valeriano, Brandon – Ryan C. Maness: *Cyber War versus Cyber Realities. Cyber Conflict in the International System*. Oxford, Oxford University Press, 2015.

„Felforgató technológiák” – jó ideje érezhető, hogy az új technológiák nem csupán lehatárolható részterületeken hozhatnak majd újítást, hanem egész struktúrákat törölhetnek el, vagy írhatnak át úgy, hogy az, ami a korábbi működési mechanizmusok helyén létrejön, radikálisan új kérdéseket vet föl. Valóban így lett, és ennek most már tanúi, résztvevői vagyunk: hasznélvezői és elszenvedői egyszerre.

A Nemzeti Közzolgálati Egyetem Információs Társadalom Kutatóintézetének újabb tanulmánykötete a társadalom digitalizálódásának néhány kiemelt területét vizsgálja. A szerzők ezúttal a legújabb technológiák társadalmi aspektusára fókuszálnak, és azt kutatják, milyen hatásokkal jár az átható digitalizáció társadalmi életünk működési mechanizmusaira, alapelveire, értékeire, szabályozási megoldásaira. Miben hoznak előrelépést, hogyan mozdítják elő például demokratikus céljainkat? Mire kell azonban vigyáznunk, és milyen új megoldásokkal kell biztosítanunk értékeink további érvényesülését egy teljesen megváltozott környezetben? Mit kell esetleg elengednünk eddigi gondolkodásunkból? Hol van szükség új szemléletmódra ahhoz, hogy eddigi társadalmi eredményeinket megtartsuk, továbbfejlesszük?