KÖZIGAZGATÁSI ÉS INFOKOMMUNIKÁCIÓS JOGI PHD TANULMÁNYOK

PHD STUDIES IN ADMINISTRATIVE AND ICT LAW

2024/III.

V. évfolyam - Volume 5

KÖZIGAZGATÁSI ÉS INFOKOMMUNIKÁCIÓS JOGI PHD TANULMÁNYOK

PHD STUDIES IN ADMINISTRATIVE AND ICT LAW

2024. évi III. SZÁM
V. ÉVFOLYAM

HU – (e)ISSN: 2732-0731

Kiadó: Tudatosan a Környezetünkért Egyesület
Felelős kiadó: Dr. Hohmann Balázs, egyesületi elnök.

Cím: Tudatosan a Környezetünkért Egyesület
7630 Pécs, Deák Ferenc u. 126.
tudatosanpecs@gmail.com

ELŐSZÓ

Az intenzív jogalkotási munkát követően szinte ízzik az elkészült szabályanyag értelmezését tartalmazó, hatásait elemző szakmai diskurzus két szabályozási területen: a platformszabályozás területén, az életünk új sok részét átszövő adatokra vonatkozó szabályok és stratégiai elképzelések körében.

Jelen folyóiratszám is ennek jegyében készült el: szerzőink elmerülnek a digitalizáció és az adatgazdaság témaköreiben, s aktívan vizsgálják a platformszabályozás három markáns elemének, a digitális szolgáltatásokról, a digitális piacokról és a mesterséges intelligenciáról szóló rendeletek összhangját.

A Kiadó nevében ezúton is köszönöm Szerzőink igyekezetét, a Szerkesztőbizottság tagjainak és a lektoroknak a felkérések elfogadását és áldozatos munkájukat. Külön köszönet illeti a Dél-dunántúli Regionális Könyvtár és Tudásközpont munkatársait, akik oly sok tekintetben nyújtanak segítséget folyóiratunk megjelentetéséhez.

Jó szakmai „merítkezést" kívánok minden Olvasónak!

Dr. Hohmann Balázs
főszerkesztő

FOREWORD

Following an intense period of legislative activity, professional discourse is now fervently engaged in interpreting and analyzing the effects of the resulting regulatory framework in two key areas: platform regulation, and the rules and strategic visions concerning data—an increasingly pervasive element in our daily lives.

This issue of the journal has been prepared in this spirit. Our authors delve into topics related to digitalization and the data economy, critically examining the coherence among the three prominent pillars of platform regulation: the regulations on digital services, digital markets, and artificial intelligence.

On behalf of the Publisher, I would like to express my sincere gratitude to our Authors for their dedication, and to the members of the Editorial Board and the reviewers for accepting our invitations and for their committed work. Special thanks are due to the staff of the South Transdanubian Regional Library and Knowledge Centre, whose support is invaluable in ensuring the successful publication of our journal.

I wish all readers a good professional "immersion"!

Dr. Balázs Hohmann
Editor-in-Chief

KÖZIGAZGATÁSI ÉS INFOKOMMUNIKÁCIÓS JOGI PHD TANULMÁNYOK
PHD STUDIES IN ADMINISTRATIVE AND ICT LAW

2024. évi III. SZÁM
V. ÉVFOLYAM

TARTALOM

Kun László: Megjegyzések a digitalizáció jelenségéhez és néhány nemzetközi gyakorlat az adatgazdálkodás területén.....5-14. o.

Török Tamás Sándor: Az adatvédelmi tisztviselő pozíciója és szerepe a mesterséges intelligenciáról szóló rendelet kockázati rendszerében.....15-32. o.

Joó Patrik Zsolt: Korkép az online óriásplatformok és keresőprogramok problematikájáról.....33-43. o.

MEGJEGYZÉSEK A DIGITALIZÁCIÓ JELENSÉGÉHEZ ÉS NÉHÁNY NEMZETKÖZI GYAKORLAT AZ ADATGAZDÁLKODÁS TERÜLETÉN

Kun László
Nemzetközi projekt koordinátor, Bay Zoltán Alkalmazott Kutatási Közhasznú Nonprofit Kft.
A szerző elérhetősége: laszlo.kun@gmail.com

DOI: 10.47272/KIKPhD.2024.3.1

ÖSSZEFOGLALÓ
A digitalizáció és a digitális eszközök használata immár több évtizedes, mélységében és kiterjedésében egyre nagyobb területet átfogó, globális folyamat, indokolt hosszabb távú elemzések végrehajtása, a különböző gyakorlatok, ezen belül az Európán kívüli megoldások áttekintése. A digitális eszközök használatának elterjedése újfajta mechanizmusok, módszerek kialakulását is jelenti, ilyen például a gyűjtött és tárolt adatok, információk kezelése - a digitális eszközök működésének egyik alapvető eleme és feltétele lett a digitális adatok megfelelő és használata, az adatvagyon hasznosítása. A cikk ezzel a két témakörrel kíván foglalkozni. Az egyik témakör a digitalizáció jelenségéhez, folyamatához tett néhány általános megjegyzés, egyes globális gyakorlatok rövid áttekintése, valamint az adatgazdálkodás néhány területének bemutatása.

KULCSSZAVAK
Digitalizáció, adatvagyon, adatgazdálkodás, nemzetközi gyakorlatok, nemzeti szabályozás

I. Bevezetés
Az általános digitalizációs folyamatok részeként az adatok, a különböző szervezetek tulajdonában lévő adatvagyon kezelésének fontossága jelentősen megnőtt az elmúlt néhány évtizedben. Ahogyan a médiában, a sajtóhírekben is gyakran elhangzott már, az adat az „új arany", az „új olaj" vagy az „új valuta".[1] Valószínűleg az ilyen szófordulatokat a médiában használók nem így értelmezik, de a párhuzam abból a szempontból mindenképpen helyes, hogy a kőolaj és az adat esetében is komoly szakértelemre, költséges beruházásokra és biztonságos szállító infrastruktúrára van szükség ahhoz, hogy a „nyersanyag" használható legyen. Hasonlóan a „régi" (a kőolaj) és az „új" olaj (az adat) hasonlathoz, ahhoz, hogy megfelelően értékelhető legyen a digitalizáció, az adatgazdálkodás és a közigazgatás, a közszféra kapcsolata, bevezetésként néhány szempontot indokoltnak tartok áttekinteni.

[1] Angwin, Julia: The web's new gold mine: Your secrets. *Wall Street Journal 30*(07), 2010.
Pataki Gábor – Szőke Gergely László: *Az online személyiségprofilok jelentősége*. In: Polyák Gábor (Szerk.): *Algoritmusok, keresők, közösségi oldalak és a jog – A forgalomirányító szolgáltatások szabályozása.* Budapest, HVG ORAC, 2020. 74-80. o.

I.1. A digitalizáció nem új jelenség és a jövőben is velünk marad

A digitalizáció általános elterjedése és ezzel összefüggésben az adatok feldolgozása, használata több évtizedes múltra tekint vissza, amibe beleértendő a közigazgatás, az állami működés támogatása is.[2] Sőt, a közigazgatás, a közszolgáltatások az egyik első olyan terület volt, ahol elterjedt az adatok kezelésének, feldolgozásának támogatása különböző informatikai eszközökkel.[3] Magyarországon már az 1970-es években is használtak különböző számítógépeket információ feldolgozására, tárolásra, nyilvántartásra,[4] bár Magyarország a „szocialista tábor" tagjaként korlátozottan érhette el a vezető informatikai megoldásokat az ún. COCOM-lista korlátozásai alapján. Szintén megemlíthető példaként, hogy az internet alapú működési modell egyik úttörőjét, a Google-t 1998-ban, közel 30 éve alapították, azóta meghatározó fejlesztője és befektetője a digitális világnak.[5] A nagy visszhangot kapó ChatGPT fejlesztőjét, az OpenAI-t 2015-ben alapították, ezután évek munkája és jelentős mennyiségű forrás volt szükséges ahhoz, hogy 2022. végén általánosan elérhetővé tegyék a mesterséges intelligencia alapú alkalmazásukat.

A digitalizáció helyzetének értékelésénél szintén szükséges figyelembe venni azt a jellemzőt is, hogy a digitalizáció hatásainak, eszközeinek nagyobb része „nem látható". A digitalizáció elemzésénél sok esetben kizárólag az „ember-gép interfészek" figyelembe vétele történik (pl. személyi számítógépek, mobiltelefonok, különböző más személyes használatra alkalmas eszközök), de legalább ilyen lényeges, hogy a „háttérben" hatalmas, az egész világot behálózó, digitális jelekkel működő infrastruktúrák jöttek létre, amelyek állapota, működése nagy mértékben meghatározza az általunk ismert világ működését.[6] Különösen igaz ez az adatgazdálkodás, adathasznosítás területére, ahol jellemző az emberi beavatkozás nélkül működő, automatizált gép-gép kapcsolat. A háttér-infrastruktúráknak, digitális hálózatoknak a működési problémái, esetleges megszűnésük akár teljes szektorok leállását, megszűnését okozhatják, így összességében kritikus fontosságú alapvető eszközökről beszélhetünk. A digitalizáció az elmúlt évtizedekben ennek megfelelően nem kizárólag a felhasználói szokásokat alakította át, hanem létrehozott egy teljesen új, globális szintű együttműködésre alkalmas infrastruktúrát, amely

[2] Schallmo, Daniel R. A. – Williams, Christopher A.: *Digital Transformation Now! Guiding the Successful Digitalization of Your Business Model*. Cham, Springer, 2018. 3-8. o. https://doi.org/10.1007/978-3-319-72844-5_3

[3] Hohmann Balázs: *A digitalizáció személyességi, átláthatósági követelményei a helyi, területi közigazgatási szervek működésére.* In: Csefkó Ferenc (Szerk.): *Szemelvények a helyi és területi közigazgatás aktuális kérdéseiről.* Pécs, Jövő Közigazgatásáért Alapítvány, 2022. 207-210. o.

[4] Álló Géza – Molnár Szilárd: *A „hiteles helyektől" az elektronikus közigazgatásig. Mérföldkövek a hazai közigazgatás automatizálásának és a kormányzati számítástechnika kialakulásának történetében.* Szeged, Primaware Kiadó, 2014. 89. o.

[5] Google: *From the garage to the Googleplex*. https://about.google/our-story/ (2024.12.31.)

[6] Du, Zhuo-Ya – Qian Wang: Digital infrastructure and innovation: Digital divide or digital dividend?. *Journal of Innovation & Knowledge 9*(3), 2024. 100542. https://doi.org/10.1016/j.jik.2024.100542

megváltoztatta a különböző szférákban működő szervezetek mindennapi gyakorlatait is.

A fentieket figyelembe véve ma már indokolt a digitalizációról olyan módon gondolkodni, amely évtizedek óta hatást gyakorol a társadalom különböző szereplőinek viselkedésére, működésére és amely jelenlegi tudásunk és most még nem ismert, a jelenlegi viszonyokat gyökeresen megváltoztató jelenség nélkül folyamatosan jelen lesz a környezetünkben a jövőben. Ez a háttér-infrastruktúra ugyanolyan folyamatos fejlesztést és a változásokhoz alkalmazkodást igényel,[7] mint például az épületek vagy a járművek, ahol folyamatosan jelennek meg új, fejlettebb, költség - és erőforráshatékonyabb megoldások, amelyek folyamatos fejlesztési lehetőséget és ezzel egyidejűleg ilyen szükségletet is jelentenek.

I.2. A közszféra információ alapú működése, mint általános jellemző

A közszféra működésének mindig is alapeleme volt az információk, adatok gyűjtése és felhasználása.[8] Ha nagyon távoli történelmi példákat szeretnénk keresni, már a legkorábbi írásos emlékek nagy része a különböző központi közszolgáltatások megvalósításának részeként értelmezhető (például az ókori emlékek jelentős része is a különböző uralkodói funkciók megvalósításával kapcsolatos). De hogy időben és jellemzőkben is közelebbi példákat említsek, Magyarországon 1871-től működik hivatalos központi statisztikai hivatal.[9] A közigazgatás, az államszervezet működése, működtetése emiatt különösen alkalmas a digitalizáció bevezetésére, az információ – és adat alapú fejlesztések eredményeinek használatára.

A digitalizáció és az adatok jellege lehetőséget ad gyakorlati, technológiai azonosságaik vagy hasonlóságuk miatt a legfejlettebb informatikai, folyamatszervezési gyakorlatok, alkalmazások bevezetésére a közigazgatásban a közszolgáltatásokban is (ahogyan erre számtalan példát látunk világszerte). Ahogyan a legtöbb területen, ebben is kiemelt jelentőségű a megfelelő szemlélet alkalmazása, ebből a szempontból lényeges az előző pontban írott megjegyzés is, amely szerint a digitalizáció immár egy hosszabb időtávon létező, és jelenlegi tudásunk szerint a jövőben is zajló folyamat, amely nem időben véges „projektként", hanem gyakorlatilag folyamatos fejlesztési szükségletként jelentkezik.

I.3. A közszféra egységes szemléletű megközelítése

A közszolgáltatások, az állampolgároknak, ügyfeleknek nyújtott különböző állami szolgáltatások elvégzésekor, az ügyek intézésekor a központi közigazgatás és a

[7] Hu, Jin – Zhang, Hong– Irfan, Muhammad:How does digital infrastructure construction affect low-carbon development? A multidimensional interpretation of evidence from China. *Journal of cleaner production 396*, 2023. 136467. https://doi.org/10.1016/j.jclepro.2023.136467

[8] Szőke Gergely László: *Big Data and Algorithms in the Public Sector and Their Impact on the Transparency of Decision-Making*. In: Hansen, Hendrik, et al. (Szerk.): *Central and Eastern European eDem and eGov Days 2018 : Conference proceedings*. Wien, Facultas Verlag, 2018. 301-303. https://doi.org/10.24989/ocg.v331.25

[9] Központi Statisztikai Hivatal: *A statisztikai szolgálat megalakulása*. https://www.ksh.hu/mult_kezdetek (2024.12.31.)

közigazgatás, a közszolgáltatók további csoportjai közötti együttműködésben, a feladatok elvégzésében a digitalizáció szintén jelentős módosulást eredményezett.

A digitális eszközök hálózatokba szervezhetősége lehetővé teszi, hogy a különböző közszolgáltatók, államigazgatási szereplők – központi közigazgatási szervek, önkormányzatok, állami közszolgáltatók, állami tulajdonú cégek stb – minden eddiginél jobban együtt tudjanak működni, egységes működési sztenderdeket, háttérmegoldásokat alkalmazzanak, ezzel egyszerűbbé, átláthatóbbá és gyorsabbá téve a megoldásaikat és ami legalább ilyen fontos, átjárhatóvá téve a különböző rendszereket. Az elmúlt években Magyarországon is sok kezdeményezést, fejlesztést láthattunk ezen a területen (például nemzetközi szinten is jó gyakorlatként említhető a közszféra működésébe egységes szemléletet, feltételrendszert hozó szabályozott elektronikus ügyintézési szolgáltatások, központi elektronikus ügyintézési szolgáltatások, ismert rövidítésük szerint a SZEÜSZ-ök és KEÜSZ-ök rendszerének kidolgozása és bevezetése).[10]

A fenti szempontok áttekintését azért tartottam indokoltnak, mert az ehhez hasonló jellemzők alapján látható, hogy a digitalizáció mind időbeliségében mind pedig társadalmi-gazdasági-technológiai kiterjedésében jelentős. Ez alapján már lehetséges és időszerű is a hosszabb távú, évtizedes tendenciák feltárása, komplex, több társadalmi szektort átfogó elemzések elvégzése. A digitalizáció a társadalmi hálózatok, társadalmi kapcsolatok minden eddiginél jobban láthatóvá és elemezhetővé tette. A digitális megoldások egyik alapja az adatok megfelelő használata és jobb gazdálkodás, a terület fejlesztése, a következő oldalakon elsősorban emiatt szerepel néhány gondolat és gyakorlat bemutatása.

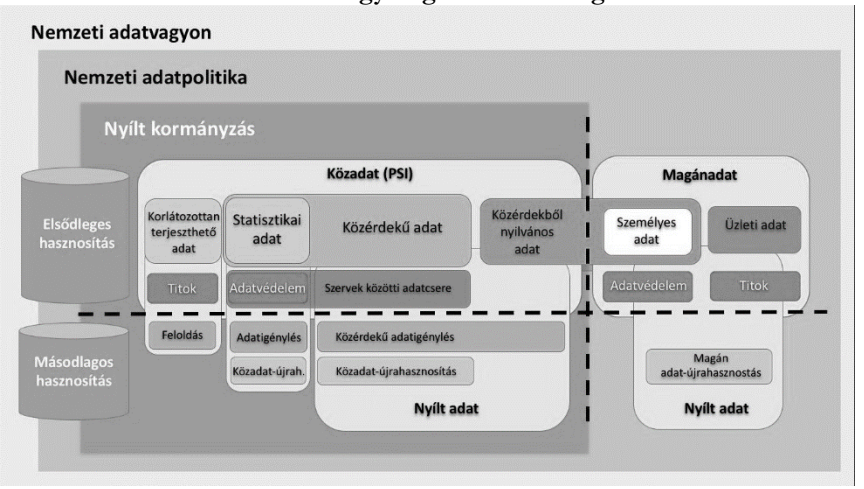
II. Példák az adatgazdálkodás hazai stratégiai keretrendszeréből

A közigazgatás érintettségének megfelelően az adatok, az adatgazdálkodás témája megjelent különböző kormányzati stratégiai dokumentumokban is, mint stratégiai terület. Az alábbiakban két ilyen dokumentumot mutatok be, amelyek elkészítése és elfogadása között évek teltek el, ami keretezi a két dokumentum elfogadása közötti időszakot. Az egyik ilyen, az adatokkal, az adatgazdálkodással mélységében és kiterjedten foglalkozó, egyik első ilyen hazai dokumentum a 2016-ban elfogadott, a Nemzeti Hírközlési és Informatikai Tanács Szakértői Tanácsadó Testülete által készített Fehér könyv a nemzeti adatpolitikáról. A Fehér könyv legfontosabb célja, a közadatok hozzáférésével, gazdálkodásával kapcsolatos elvek megfogalmazása. A Fehér könyv az alábbi ábrát tartalmazza a nemzeti adatvagyon gazdálkodás fogalmi rendszeréről, amely fogalmi alapként ma is alkalmazható.[11]

[10] Cseh-Zelina Gergely – Czékmann, Zsolt: Hungarian regulation of e-government in the light of EU legislation. *Balkan Social Science Review 22*, 2023. 29-49. o. https://doi.org/10.46763/BSSR232222029c

[11] Nemzeti Hírközlési és Informatikai Tanács Szakértői Tanácsadó Testülete*: Fehér könyv a nemzeti adatpolitikáról.* Budapest, NHIT, 2016.

1. ábra A nemzeti adatvagyon gazdálkodás fogalmi rendszere



Forrás: NHIT: Fehér könyv a nemzeti adatpolitikáról. Budapest, NHIT, 2016. 12. o.

Az egyik legújabb, legfrissebb, a digitalizációval foglalkozó stratégia a „Digitális Évtized 2030 Nemzeti Stratégiai Ütemterv" címet viseli. Az Ütemtervet a Stratégiai és Családügyi Kabinet 2023. december 4-én fogadta el, ezután került benyújtásra az Európai Bizottság részére. Az Ütemterv elkészítésének előzménye, hogy a Digitális évtized 2030 szakpolitikai program létrehozásáról szóló (EU) 2022/2481 határozat értelmében az Európai Unió tagállamainak el kell készíteniük a célok elérését biztosító tévő intézkedési tervet. A stratégia az adatok területével viszonylag sokat foglalkozik, a digitalizáció és az informatikai fejlesztések alapelemének tekinti ezeket. Külön beavatkozási csomagként a nagy adathalmazok (Big Data) témája jelenik meg a következő két intézkedés végrehajtásával:

- KKV-k digitalizálása ezen belül:
  Támogatási konstrukciók kidolgozása és megvalósítása a magyarországi KKV-k számára (most már látható, hogy ezek közül több 2024. végén elérhető Európai Uniós társfinanszírozású pályázatként a Digitális Megújulás Operatív Program Plusz keretében[12])
- Mesterséges intelligencia és big data megoldások felhasználásának javítása közpolitikai és disszeminációs eszközökkel a vállalkozások körében, ezen belül:

[12] Pályázati Portál https://www.palyazat.gov.hu/programok/szechenyi-terv-plusz/dimop-plusz (2024.12.31.)

Mesterséges Intelligencia Koalíció működtetése, Mesterséges Intelligencia Stratégia felülvizsgálata, megújítása, a kormányzati technológiai ügynökség (Neumann János Nonprofit Kft.) és platform működtetése, országos mesterséges intelligencia adaptációs roadshow vállalkozásoknak, alapvető ismeretek terjesztése, tanulógyár mintaprojektek kidolgozása, támogatása, szakmai rendezvények, kiállítások lebonyolítása.

A közszféra adatgazdálkodásának fejlesztése a kormányzati digitális szolgáltatásokon belül jelenik meg, például az „evidencia-alapú kormányzati döntéshozatalt, valamint a közszféra adatvagyonának és információinak kiaknázását szolgáló fejlesztések" intézkedés formájában.

III. Az Európai Unió határain túli adatkezelési, nyílt adat gyakorlatok, módszerek

Magyarország földrajzi elhelyezkedéséből, történelméből, Európai Uniós tagsága és sok más ok miatt az Európai Unió adatgazdasággal, adatgazdálkodással kapcsolatos intézkedéseit követi, alkalmazza, ezek az intézkedések jól ismertek, jelentős irodalom és elemzés foglalkozik ezekkel.[13] Azonban az internetes gazdaság, az adatgazdaság területén jelenleg nem az Európai Unió jelenti a legnagyobb gazdasági erővel, kutatás-fejlesztéssel stb. rendelkező régiót. Az internet gazdaság meghatározó cégeinek többsége az Egyesült Államokban működik, illetve történelmileg – a fentiekben is említett évtizedes folyamatok eredményeként - is kijelenthető, hogy az informatikai, digitalizációs fejlesztések meghatározó része az Egyesült Államokhoz köthető vagy jelenleg is ott zajlik. A technológiai fejlődés részeként az eredetileg is kizárólag informatikai, digitális területen működő vállalkozások mellett sok jelentős méretű cég is belépett a high-tech iparágakba (ilyen például az Amazon cégcsoport részeként az Amazon Web Services).

A digitális technológia területén a másik nagy jelentőségű, Európán kívüli térség a Távol-Kelet. Az elmúlt években Kína szerepe erősödött meg. Kínával kapcsolatosan folyamatosan vetődnek fel a különböző adatbiztonsági, adathasználati kritikák, kifogások, ugyanakkor Kína az elmúlt években ezeken a területeken nagy számú intézkedést vezetett be, amelyek több szempontból is foglalkoznak az adatok kezelésével, használatával, az adatbiztonsággal.

A két nagy fontosságú állam adatgazdálkodással kapcsolatos összehasonlítására alkalmasak lehetnek a különböző, globális méretben is használt mutatószámok alapján elért eredmények. Az egyik ilyen mutatószám a World Wide Web Alapítvány által összeállított és használt Open Data Barometer.[14] A jelenleg elérhető adatok szerint az utolsó mérésre 2017. szeptembere és 2018. márciusa között került sor, vagyis az adatok viszonylag réginek minősíthetőek, de a két ország közötti különbségek láthatóak ebben is. Az Open Data Barometer a különböző

[13] Ld. pl. Angyal Zoltán: Úton a digitális egységes piac felé. *Miskolci Jogi Szemle* 15(3), 2020. 5-7.o.

[14] World Wide Web Foundation: *The Open Data Barometer.* https://opendatabarometer.org/?_year=2017&indicator=ODB (2024.12.31.)

szempontokat a maximálisan elérhető 100-hoz viszonyítja, így a különböző országok értékei inkább az egymáshoz viszonyítás miatt érdekesek. Az Open Data Barometer nem méri meg minden ország teljesítményét, a 30 országot tartalmazó listán az Egyesült Államok 9. helyezést ért el 64 értékkel, míg Kína ugyanitt 24. helyen szerepel 31 értékkel, minden szempontban jelentősen elmaradva az USA-tól.

2. ábra Az Open Data Barometer „műszerfala" az USA esetében

IMPLEMENTATION

DATASET SCORED															
United States of America	95	25	95	60	85	5	100	95	95	90	75	90	75	80	75
Does the data exist?	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Is it available online from government in any form?	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Is the dataset provided in machine-readable and reusable formats?	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Is the machine-readable and reusable data available as a whole?	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Is the dataset available free of charge?	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Is the data openly licensed?	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Is the dataset up to date?	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Is the dataset being kept regularly updated?	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Was it easy to find information about this dataset?	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Are data identifiers provided for key elements in the dataset?	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

IMPACT

COUNTRY	POLITICAL	SOCIAL	ECONOMIC
United States of America	20.00	30.00	60.00

Forrás: World Wide Web Foundation: *The Open Data Barometer* https://opendatabarometer.org/country-detail/?_year=2017&indicator=ODB&detail=USA (2024.12.31.)

A nyílt adatokkal történő gazdálkodás mérése és országonkénti összehasonlítása mellett létezik olyan mutatószám is, amely általában a statisztikai rendszerek, az adatok rendelkezésre állását méri,[15] ez a Világbank Statistical Performance Indicators (SPI) elnevezésű rendszere. Az SPI nem klasszikus értelemben vett sorrendet tartalmaz, hanem összesen öt csoportra, kvintilisre osztja az országokat teljesítmény szerint. Az USA ebben a mutatószámban 92,8 értéket kapott, amellyel a legfelső kvintilisbe tartozik, míg Kína 59,6 értékkel a második kvintilisbe tartozik. A különbség nagy mértéke azt jelenti, hogy az SPI szerint Kína a statisztikai adatszolgáltatás gyakorlatilag minden területén jelentősen elmarad az USA teljesítményétől.

Összességében mindkét ország kiemelt fejlesztési területként tekint a közadatok használatára, az adatvagyonnal gazdálkodásra. Az adatvagyon-gazdálkodás nélkülözhetetlen része olyan stratégiai céloknak, mint például a

[15] Hohmann Balázs: Interpretation the Concept of Transparency in the Strategic and Legislative Documents of Major Intergovernmental Organizations. *Közigazgatási és Infokommunikációs Jogi Phd Tanulmányok* 2(1), 2021. 48-68. o. https://doi.org/10.47272/KIKPhD.2021.1.4

mesterséges-intelligencia fejlesztése, a kiberbiztonság vagy az állami szuverenitás, ez is oka a kiemelt jelentőségűként kezelésnek és a fejlesztéseknek. A kiemelt jelentőség miatt érdemes áttekinteni, hogy ez a két, a digitalizáció területén központi szerepet játszó ország milyen intézkedéseket, gyakorlatokat vezetett be az adatgazdaság, az adatokkal gazdálkodás területén. Az alábbi kitekintés röviden bemutat néhány fontos elemet, jogszabályt, nyílt adat platformot erről a területről.

III.1. Az Amerikai Egyesült Államok gyakorlatai

Az Amerikai Egyesült Államok a digitális gazdaságban vezető szerepet játszik, a mindenki által jól ismert, milliárdos felhasználói számokkal rendelkező, a sok esetben ma már alapvetőnek tekintett szolgáltatásokat (például ingyenes e-mail, kommunikáció, digitális térkép) nyújtó vállalkozások nagy részének székhelye az USA-ban van, legtöbb esetben alapításuk is itt történt.

Az USA adatgazdálkodásának szabályozási alapja az ún. nyílt adatkormányzás törvény, hivatalos nevén a 2018. évi törvény a tényalapú kormányzásról.[16] A törvény megfogalmazása szerint a jogszabállyal érintett adatok nyitottak, nyilvánosak, elektronikusak és szükségesek. A törvény értelmében minden szövetségi intézmény köteles publikálni nyílt adatait, sztenderdizált, számítógéppel olvasható formátumban és a metaadatokat a data.gov portálon közzétenni az ott publikált nyílt adat katalógusban.

A törvényben említett data.gov oldal az USA első számú, legfontosabb adatportálja. A portál 2009. május 21-én indult (immár több mint 15 éve), összesen 47 adatkészlettel. A portál indításának előzménye a 2009. januári elnöki rendelkezés volt az átláthatóságról és nyílt kormányzásról. A portál működésében nagy változást jelentett, hogy 2013-ban kötelezővé tették a szövetségi intézmények számára adataik közzétételét. Az elérhető, kereshető adatkészletek száma azóta is folyamatosan nő, mára meghaladta a 300 ezret, az adatok az állami működés minden területéről származnak. A portál az adatokon kívül olyan hasznos információkat tartalmaz, mint például az általuk ismert nyílt adat weboldalak listája, vagy a USA más nyílt adat weboldalainak listája.[17] A közzétett lista azonban nem nevezhető teljes körűnek, például magyar weboldal, adatportál nem szerepel közöttük annak ellenére, hogy legalább a legfontosabbak felsorolhatóak lennének.

III.2. A Kínai Népköztársaság gyakorlatai

A Kínai Népköztáraság sok esetben negatív példaként jelenik meg az adatgazdálkodással, adatvédelemmel kapcsolatos irodalomban és hírekben, azonban a digitális gazdaságban és általában a világgazdaságban betöltött szerepe miatt indokolt áttekinteni az országban használt jellemző megoldásokat, gyakorlatokat.

[16] Viljoen, Salomé: A relational theory of data governance. *The Yale Law Journal 131*(2), 2021. 573-654. o.
[17] Data.gov: *USA Open Government*. https://data.gov/open-gov/ (2024.12.31.)

Hasonlóan az amerikai példákhoz, a különböző nagy kínai digitális platformok, beleértve a kezdetben nem kizárólag vagy nem elsősorban nem digitális szolgáltatásokat nyújtó platformokat, fejlesztőket (pl. internetes webáruházak működtetői, pénzügyi szolgáltatók) az általuk kezelt és működtetett nagy informatikai infrastruktúrákat, nagy adatbázisokat felhasználják különböző digitális megoldások és nyújtására fejlesztésére is.

A kínai digitális gazdaság egyik ilyen meghatározó szereplője az inkább „analóg" áruk piactereként ismert Alibaba csoport. A céget 1999-ben alapították, ezután tevékenységüket folyamatosan kiterjesztették egyre több üzletágra, mára leginkább e-kereskedelmi csoportként jellemzik önmagukat. Az Alibaba jelenleg hét nagyobb tevékenységi körrel foglalkozik, beleértve a digitális szolgáltatásokat is (például felhőszolgáltatások, digitális média és szórakoztatóipar, alkalmazásfejlesztés).[18]

A kínai digitális gazdaság másik nagy szereplője a Tencent csoport, amely az Alibabától eltérően szinte kizárólag internetes és IT megoldásokkal foglalkozik. Az Alibabával közel egy időben, 1998-ban alapították Sencsenben, az egész világra kiterjedő iroda hálózattal rendelkezik, Kelet-Ázsián kívül Észak-Amerikában, Európában (ezen belül Amszterdamban, Londonban, Liverpoolban, Frankfurtban, Münchenben, Berlinben, Varsóban, Isztambulban és Párizsban), a Közel-Keleten és Afrikában is vannak irodái.[19] A Tencenthez tartozik például a Weixin alkalmazások csoportja, amelyek magukban foglalják a Kínában széles körben, kb. 1,3 milliárd felhasználó által használt Weixin, kezdetben üzenetküldő, majd szociális média platformmá fejlesztett alkalmazást és fizetési megoldásokat. A gazdasági méret jellemzésének jó mutatója, hogy a csoport éves forgalma kb. 86 milliárd dollár volt 2023-ban.[20]

Kína a mesterséges intelligencia fejlesztését kitörési pontként kezeli, nyilvánvalóan világvezető szerepre tör ezen a területen. 2017-ben fogadták el a mesterséges intelligencia fejlesztésére vonatkozó stratégiát, amely szerint 2025-re néhány területen világvezető pozícióba kívánnak kerülni és 2030-ra a fejlesztések elsődleges központjává terveznek válni. A stratégia részeként Pekingben kb. 2 milliárd dollár költséggel építenek technológiai parkot, és a kapcsolódó iparágakkal együtt összességében kb. 1300 milliárd dollár méretű mesterséges intelligencia ipart terveznek kialakítani Kínában.[21] A mesterséges intelligencia fejlesztésének alapja a megfelelő mennyiségű és minőségű adat, az általában jellemző indokok – például az adatbiztonság, személyes adatok kezelése – mellett ez az egyik oka, hogy Kínában is

[18] Alibaba Group: *Our Businesses.* https://www.alibabagroup.com/en-US/about-alibaba-businesses (2024.12.31.)
[19] Tencent Group: *About.* https://www.tencent.com/en-us/ (2024.12.31.)
[20] PR Newswire: *Tencent Announces 2023 Annual and Fourth Quarter Results*. https://www.prnewswire.com/apac/news-releases/tencent-announces-2023-annual-and-fourth-quarter-results-302094552.html (2024.12.31.)
[21] OECD.AI: *Policy Observatory China.* https://oecd.ai/en/dashboards/countries/China (2024.12.31.)

elfogadtak már különböző szabályozásokat az adatgazdálkodás területén. A kínai intézkedések áttekintését bonyolítja, hogy a különböző dokumentumok nagy része kizárólag kínai nyelven érhető el, ez is oka lehet annak, hogy az intézkedések, jogszabályok szakértői elemzése sok esetben nem közvetlenül, hanem különböző más forrásokon keresztül történik. Ugyanakkor néhány alapvető jogszabály tájékoztatásul elérhető a kínai állami weboldalakon is.

Az egyik ilyen általános keretjogszabály a 2021. augusztus 20-án elfogadott és angol nyelven is közzétett „A Kínai Népköztársaság Személyes információk védelmének törvénye" című jogszabály.[22] A törvény leírja a személyes adatok fogalmát, kezelésének, feldolgozásának alapvető elemeit, szabályait, az infrastruktúra kezelésének, telepítésének feltételeit, beleértve az olyan részleteket is, mint például a köztereken elhelyezett képalkotó, személyfelismerő eszközök telepítésének előírásait.[23]

A Kínai Népköztársaság Nemzetgyűlésének honlapján szintén elérhető angol nyelven az adatbiztonságról szóló törvény, amelyet 2021. június 10-én fogadtak el és 2021. szeptember 1-től hatályos.[24] A törvény szorosan kapcsolódik a személyes információkról szóló jogszabályhoz, a Kína területén folytatott adatgyűjtés – és feldolgozás szabályait tartalmazza. Érdekes lehet, hogy a törvény szövege szerint adat minden információ elem, függetlenül attól, hogy elektronikus vagy nem (ez például alapvető eltérés több európai jogszabály gyakorlatától, ami csak digitális formátumot tekint adatnak). Az adatbiztonság alapelveként a törvény az általános biztonsági szempontokhoz illesztést nevezi meg, többek között szerepel benne, hogy az állam támogatja az adatok használatával kapcsolatos fejlesztéseket, az ilyen tevékenységet végző szervezeteket, cégeket, de pénzbírság kiszabásának lehetőségét is tartalmazza.

IV. Összegzés

A digitalizáció, a digitális eszközök használatának elterjedése több évtizedes múltra visszatekintő, egyre gyorsuló ütemű, globális méretű folyamat, amely jelenlegi tudásunk szerint a jövőben is folytatódni fog. A digitális eszközök és megoldások működésének alapja a digitális adatok megfelelő kezelése, használata, enélkül a közigazgatás, a közszolgáltatások működésének megfelelősége sem biztosítható. Figyelembe véve a fenti szempontokat, kiemelten fontos a digitális adatok, a rendelkezésre álló adatvagyon használatának megteremtése és folyamatos, új alkalmazási lehetőségeket is magában foglaló fejlesztése. A hazai és nemzetközi gyakorlatok köre széles a területen (ide értve a közigazgatáson, közszolgáltatásokon kívüli megoldásokat, alkalmazásokat), amelyek alkalmasak lehetnek a hazai jó gyakorlatok megalapozására is.

[22] *Personal Information Protection Law of the People's Republic of China 2021*

[23] Kaszián Ábel Gergő: *A GDPR kínai „unokatestvére" – avagy a kínai adatvédelmi törvény megszületése és várható hatásai. Jogi Fórum* 1/2021. 3-10. o.

[24] *Data Security Law of the People's Republic of China 2021*

AZ ADATVÉDELMI TISZTVISELŐ POZÍCIÓJA ÉS SZEREPE A MESTERSÉGES INTELLIGENCIÁRÓL SZÓLÓ RENDELET KOCKÁZATI RENDSZERÉBEN

dr. Török Tamás Sándor LL.M.
Doktorandusz, Pécsi Tudományegyetem Állam-és Jogtudományi Doktori Iskola
A szerző elérhetősége: tamas.drtorok@gmail.com

DOI: 10.47272/KIKPhD.2024.3.2

ÖSSZEFOGLALÓ

A Mesterséges Intelligencia Rendelettel (AIA) az Európai Unió egy újabb mérföldkőhöz érkezett el a technológiai jogi szabályozások terén. Hasonlóan az általános adatvédelmi rendelethez (GDPR), jelen esetben is a jogalkotás központi motívumaként jelenik meg a kockázatalapú megközelítés, ugyanakkor nem csak emiatt érdemes összevetni a két szabályozási rezsimet.
A személyes adatok védelme a Mesterséges Intelligencia Rendeletben is hangsúlyosan jelenik meg, ugyanakkor a GDPR szabályozásától eltérő mechanizmusok kerültek meghatározásra.
Az adatvédelmi tisztviselő a GDPR megfelelés egyik sarokköve, a személyes adatok védelmének egyik garanciális jogintézménye, amelyhez hasonló szerepkört a AIA nem hívott életre, ellenben az abban foglalt rendelkezések jelentős kihatással vannak rá. Jelen tanulmány az adatvédelmi tisztviselőnek a Mesterséges Intelligencia Rendelettel összefüggésben felmerülő feladatait és szerepét kívánja meg bemutatni.

KULCSSZAVAK
Adatvédelem, mesterséges intelligencia, adatvédelmi tisztviselő, kockázat alapú szabályozás

I. Bevezetés

2024. augusztus 1-jén hatályba lépett az Európai Parlament és a Tanács mesterséges intelligenciáról szóló 2024/1689 számú rendelete (továbbiakban: AIA),[1] amelyet aligha túlzás az elmúlt évek egyik legjelentősebb jogalkotási termékének nevezni.[2]

Az Európai Bizottság már 2018. április 25. napján kiadott közleményében úgy fogalmazott, hogy „*Ahogy korábban a gőzgép és a villamos energia, a mesterséges intelligencia is átalakítja világunkat, társadalmunkat és az ipart*”.[3] A történelmi párhuzam

[1] Az Európai Parlament és a Tanács (EU) 2024/1689 Rendelete a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról, valamint a 300/2008/EK, a 167/2013/EU, a 168/2013/EU, az (EU) 2018/858, az (EU) 2018/1139 és az (EU) 2019/2144 rendelet, továbbá a 2014/90/EU, az (EU) 2016/797 és az (EU) 2020/1828 irányelv módosításáról

[2] Burlacu, Fiorentina - Ghioaldă Lută, Gratiela Doina: The Crucial Importance Of The European Union Ai Act As The World's First Regulation On Artificial Intelligence. *Journal of Information Systems & Operations Management 17*(2), 2023. 59-63. o.

[3] A Bizottság Közleménye – A közös európai adattér kialakítása felé (COM(2018) 237 final)

aligha túlzó. Maga a közlemény már 2018-ban kitér a gazdasági lehetőségek értékalapú kiaknázásának igényére, amely magába foglalja a társadalmi szempontok és az egyéni jogok védelmének garantálását is. Ez utóbbiak közül kiemelt jelentőséggel bír a magánélethez való jog biztosíthatósága a személyes adatok védelmén keresztül.

Az AIA hatásai, értelmezése, tagálami jogalkalmazásra gyakorolt hatásai fokozatosan fognak testet ölteni, kérdések és megoldandó problémafelvetések sorát indikálva. Jelen tanulmányban az új rendelet és egy „régebbi" jogintézménynek kapcsolódási pontjait kívánom elemezni, elsődlegesen a már meglévő joggyakorlat és az AIA normaszövege alapján.

A tanulmány keretei ugyanakkor nem teszik lehetővé egy átfogó vizsgálat lefolytatását, éppen ezért e körben elsődlegesen az AIA által meghatározott MI-rendszerek kockázati megítélésében való lehetséges és potenciális adatvédelmi tisztviselői (továbbiakban: tisztviselő vagy DPO) feladatellátást kívánom elemezni, keresve a privacy by design ebbéli lehetséges értelmezését az új jogi keretrendszerben. Ugyanakkor figyelemmel az AIA kockázati rendszerére és az ahhoz fűződő kötelezettségekre, az elemzés a tiltott, illetve a magas kockázatú MI-rendszerek esetében fellépő tisztviselői szerepkör meghatározását tűzi ki elsődleges célként, mint ahol a legkritikusabb a védelmi funkciók meglétének kérdése.

A kockázat alapú megközelítés, amellyel a jogalkotó fordult az új technológiához, nem előzmény nélküli.[4]

Az AIA (26) preambulumbekezdésében a jogalkotó az alábbi indoklást fűzi a kockázatalapú megközelítés alkalmazásához: „*Az MI-rendszerekre vonatkozó, kötelező erejű szabályok arányos és hatékony rendszerének bevezetése érdekében egyértelműen meghatározott, kockázatalapú megközelítést kell alkalmazni. E megközelítés keretében az ilyen szabályok típusát és tartalmát hozzá kell igazítani az MI-rendszerek által keltett kockázatok intenzitásához és nagyságrendjéhez".*[5]

Az általános adatvédelmi rendelet (továbbiakban: GDPR) (74) preambulumbekezdése hasonló megközelítésről tesz tanúbizonyságot: „*Az adatkezelőt kötelezni kell különösen arra, hogy megfelelő és hatékony intézkedéseket hajtson végre, valamint hogy képes legyen igazolni azt, hogy az adatkezelési tevékenységek e rendeletnek megfelelnek, és az alkalmazott intézkedések hatékonysága is az e rendelet által előírt szintű. Ezeket az intézkedéseket az adatkezelés jellegének, hatókörének, körülményeinek és céljainak, valamint a természetes személyek jogait és szabadságait érintő kockázatnak a figyelembevételével kell meghozni".* [6]

[4] Ebers, Martin: Truly risk-based regulation of artificial intelligence how to implement the EU's AI Act. *European Journal of Risk Regulation*, 2024. 1-20. o. https://doi.org/10.1017/err.2024.78

[5] AIA (26) premabulumbekezdés

[6] GPDR (74) preambulumbekezdés

Hasonló logika érhető tetten a digitális szolgáltatásokról szóló rendelet (DSA) esetében is,[7] nem véletlenül. A kockázatalapú megközelítés a jogalkotásban a környezetvédelmi, egészségügyi, élelmiszeripari, pénzpiaci, bank és biztosítási szektor, vagy éppen a munkavédelmi szabályozás vonatkozásában figyelhetünk meg, azonban az utóbbi években mind szélesebb szabályozási tárgykörben nyer alkalmazást. A jogalkotás során a kockázat, mint logikai origó egyre dominánsabban jelenik meg a digitális piacok és a digitális társadalom tárgykörét érintő szabályozásában is.[8]

A „kockázat-társadalom" (risk society) fogalmát Ulrich Beck és Anthony Giddens nevéhez köthetjük,[9] ami az emberi döntéseknek a globális kockázatokat generáló aspektusára utal. Így válik értelmezhetővé, hogy a technológiai és politikai környezetünket alapjaiban befolyásoló modern digitális kockázatok azonosítása és kezelése a jogalkotók és a kormányok számára prioritássá vált.[10]

A jog, mint eszköz a felmerülő, technológiai kockázatok kezelése érdekében annyiban és úgy reagál, amennyiben az szükséges a megfelelő egyensúly elérése érdekében. E tárgykörben a kockázat egy adott technológia alkalmazása által megvalósított negatív következmény bekövetkezésének esélyét és nagyságát a bekövetkezés valószínűségének függvényében jelenti.[11]

A szempontrendszer ilyen módosulása célként jelöli meg a túlszabályozás elkerülését, ezzel pedig a jogalanyok megfeleléssel kapcsolatos költségeinek csökkentését, egy hatékonyabb, átláthatóbb és tisztességes magatartást előmozdításának érdekében. A jogalkotás e tekintetben a veszélyekkel arányos megközelítésre helyezi a jogalkalmazók kötelezettségének fő fókuszát, rugalmasságot és nagyobb felhatalmazást engedve a konkrét élethelyzetek megfelelő kezelésének céljából.[12]

II. Az adatvédelmi szabályozás keretei

1. Az elszámoltathatóság alapelve és a kockázat alapú megközelítés

A kockázat alapú megközelítés azt az ésszerűen elvárható előrelátást várja el az érintett szervezetektől, hogy a tevékenységük, vagy jelen esetben az új technológiák

[7] Hohmann, Balázs: A Digital Services Act és a Digital Markets Act termékekreés digitális szolgáltatásokra irányuló fogyasztói jogviszonyokat érintő rendelkezései. *In Medias Res 12*(2), 2023. 70. o. https://doi.org/10.59851/imr.12.2.4

[8] Efroni, Zohar: *The Digital Services Act: risk-based regulation of online platforms*. Internet Policy Review, 2021. https://policyreview.info/articles/news/digital-services-act-risk-based-regulation-online-platforms/1606 (2024.12.31.)

[9] Beck, Ulrich: *Risk society -Towards a new modernity*. München, University of Munich, 1992. 9-22. o.

[10] Efroni, 2021, i.m.

[11] Mezei Kitti – Träger Anikó: Kockázatok és reziliencia az online platformok és a mesterséges intelligencia európai uniós szabályozásában, *MTA Law Working Papers* 2024/1. 7. o.

[12] Mezei– Träger, 2024, i.m. 47. oldal

használata előtt felmérjék azok alkalmazásának lehetséges hatásait és megtegyék a szükséges intézkedéseket az esetleges kockázatok minimalizálása érdekében. Megfogalmazható ez az elvárás úgy is, mint az adott szervezet preventív compliance programja, vagyis a jogszabályi, de tágabb értelemben a társadalmi és etikai elvárásoknak megfelelő működés kialakításának kötelezettsége.

A kockázat alapú megközelítést a GDPR zsinórmértékként alkalmazza a privacy jellegű kockázatok értékelésének és kezelésének vonatkozásában, ugyanis amíg a személyes adatok kezelése negatív hatást képes kiváltani az érintettek jogaira és szabadságaira, addig a védelmi intézkedések meghozatala elvárt és indokolt.[13]

Amennyiben tehát a kockázatkezelést elfogadjuk preventív compliance tevékenységnek, úgy a GDPR által alapelvi szinten megfogalmazott elszámoltathatóság elvét is érdemes ebben a kontextusban értelmezni és vizsgálni.[14]

Az elszámoltathatóság elve[15] alapozza meg azt az adatkezelési keretrendszert, amelyben az adatkezelő az adatkezelés teljes életciklusára vetítetten, a tervezéstől a megvalósulásig folyamatszinten adminisztrálja tevékenységét, ezzel biztosítva a GDPR rendelkezéseinek való megfelelést a külvilág felé.[16] Az elszámoltathatóság transzparenciát eredményez,[17] amely az elvárásoknak megfelelő tájékoztatók, szabályzatok, nyilvántartások, eljárásrendek elkészítése és megismerhetősége révén átláthatóvá és nyomon követhetővé teszi az adott adatkezeléseket mind az érintettek, mind pedig a felügyeleti hatóságok irányába. [18]

A GDPR előírásainak való megfelelést önmagában nem fogja eredményezni csak a jogszabályok által expressis verbis megfogalmazott elvárások betartása, ezen túlmenően, az érintettek várakozásaira is figyelemmel kell lenni. Ezt a meggondolást támaszatja alá a jogos érdek vonatkozásában megfogalmazott, a (47) preambulumbekezdés „számíthat-e észszerűen" fordulata, amely a megfelelés egyik záróköveként jelöli meg az érintettek jogilag akceptálható előfeltevéseihez való igazodást.[19]

Ebből következik, hogy valamennyi adatkezelési művelet előtt fel kell mérni és értékelni kell a lehetséges kockázatokat úgy, hogy azok a strict jogszabályi előírásokon túl vegyék figyelembe az adott érintetti csoport azon jellemzőit is,

[13] Szabó Endre Győző: Az Adatvédelmi tisztviselőről, a GDPR szabályainak elemzése, *Infokommunikáció és Jog*, 2018/1. 3. o.

[14] De Hert, Paul – Lazcoz, Guillermo: When GDPR-principles blind each other: accountability, not transparency, at the heart of algorithmic governance. *European Data Protection Law Review 8*(1), 2022. 31. o. https://doi.org/10.21552/edpl/2022/1/7

[15] GDPR 5. cikk (2) bekezdés

[16] Péterfalvi Attila – Révész Balázs – Buzás Péter (Szerk.): *Magyarázat a GDPR-ról*, Budapest, Wolters Kluwer Hungary, 2021. 141. o.

[17] Hohmann Balázs: Interpretation the Concept of Transparency in the Strategic and Legislative Documents of Major Intergovernmental Organizations. *Közigazgatási és Infokommunikációs Jogi Phd Tanulmányok* 2(1), 2021. 48-68. o. https://doi.org/10.47272/KIKPhD.2021.1.4

[18] Péterfalvi – Révész – Buzás, 2021, i.m. 142. o.

[19] Szabó, 2018, i.m. 4. o.

amelyek esetleg befolyásolhatják az adatkezeléssel szemben támasztott elvárásaikat úgy, hogy a döntés mechanizmusa és eredménye transzparens módon dokumentált és adott esetben egy hatósági eljárásban (bizonyos esetben érintetti megkeresés esetén is) bemutathatóvá váljon.[20]

Az elszámoltathatóság elve egyszersmind a kockázatkezelés megfelelősségének ellenőrizhetőségét, a kockázatkezelési mechanizmusok áttekinthetőségét is szolgálja.

A GDPR számos rendelkezését tartalmaz a „megfelelősségi" intézkedésekkel és azok igazolhatóságával összefüggésben, mint például az adatkezelési tevékenységek belső nyilvántartásának (GDPR 30. cikk), adatvédelmi hatásvizsgálat (GDPR 37. cikk) elvégzésének, adatvédelmi incidensek során elvárt eljárásoknak (GDPR 34. cikk) és az adatvédelmi tisztviselő kijelölésének (GDPR 37. cikk) szabályai.[21]

Jelen tanulmány fókuszában ez utóbbi, vagyis az adatvédelmi tisztviselő jogintézménye áll, ami egyszerre része és támogatója az elszámoltathatóság érvényesülésének, következésképp a GDPR-ban meghatározott kockázatkezelés hatékonyságának záloga is.

2. Az adatvédelmi tisztviselő helye és szerepe a kockázatkezelésben

Az adatvédelmi tisztviselő kijelölésének, jogállásának és feladatainak szabályait a GDPR 4. szakasza tartalmazza, ugyanakkor a nevezett szervezeten belüli funkció már jóval az általános adatvédelmi rendelet előtt is létezett. Az adatvédelmi tisztviselő az Egyesült Államok nagyvállalatai működésének és szervezeti kultúrájának szerves részét képezte. A „privacy officer", vagy a „chief privacy officer" olyan munkatársat jelölt, akinek a magánélet védelmi körébe tartozó személyes adatok kezelésének jogszerű és etikus kezelése, az ehhez kapcsolódó belső folyamatok kialakítása és támogatása volt a feladata.[22] Az európai jogrendszerbe az Európai Parlament és a Tanács a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK irányelve (továbbiakban: irányelv) ültette át az adatvédelmi tisztviselő jogintézményét, ugyanakkor a kijelölés az adatkezelők esetében nem vált kötelezettséggé, csupán olyan opcióvá, amelyhez bizonyos előnyöket társított a

[20] Hohmann Balázs: *A mesterséges intelligencia közigazgatási hatósági eljárásban való alkalmazhatósága a tisztességes eljáráshoz való jog tükrében*. In: Török Bernát – Ződi, Zsolt (szerk.): *A mesterséges intelligencia szabályozási kihívásai – Tanulmányok a mesterséges intelligencia és a jog határterületeiről*. Budapest, Ludovika Egyetemi Kiadó, 2021. 403-422. o.
Szőke Gergely László: *Big Data and Algorithms in the Public Sector and Their Impact on the Transparency of Decision-Making*. In: Hansen, Hendrik, et al. (Szerk.): *Central and Eastern European eDem and eGov Days 2018 : Conference proceedings*. Wien, Facultas Verlag, 2018. 301-303. https://doi.org/10.24989/ocg.v331.25
[21] Péterfalvi – Révész – Buzás, 2021, i.m. 141. o.
[22] Justine Brown*: Rise of the Chief Privacy Officer*. Government Technology, 2014. https://www.govtech.com/data/rise-of-the-chief-privacy-officer.html (2024.12.31.)

jogszabály, azonban kötelezővé nem tette azt még a nagy kockázatú adatkezeléseket végző szervek vagy szervezetek részére sem.

A 29. cikk szerinti munkacsoport (továbbiakban: Munkacsoport) WP 243 rev.01 számú iránymutatása részletesen foglalkozott az adatvédelmi tisztviselő feladatainak és hatáskörének kérdésével, amely alapelvek napjaink joggyakorlatát is alapjaiban határozzák meg.

A Munkacsoport az elszámoltathatóság alapköveként hivatkozott az adatvédelmi tisztviselőre, mely funkció segíthet a jogszabályi megfelelésben, illetve feladatköréből fakadóan a bizalom, így pedig a végsősoron a vállalkozások versenyelőnyét is képes előmozdítani.[23]

Az adatvédelmi tisztviselő az általános adatvédelmi rendelet komplex védelmi rendszerének egyik alapeleme, az elszámoltathatóság és így a rendeletben foglalt előírásoknak való megfelelés központi garanciája. A rendelet (77) preambulumbekezdése szerint „*A megfelelő intézkedéseknek az adatkezelő vagy adatfeldolgozó általi végrehajtásához, valamint a megfelelés általuk való bizonyításához - különösen ami az adatkezeléssel kapcsolatos kockázat beazonosítását, valamint a kockázat forrásának, jellegének, valószínűségének és súlyosságának a felmérését illeti -, továbbá a kockázat mérséklésével kapcsolatos bevált gyakorlatoknak az azonosításához útmutatással szolgálhatnak különösen a jóváhagyott magatartási kódexek, a jóváhagyott tanúsítási eljárások, a Testület iránymutatásai vagy az adatvédelmi tisztviselő által nyújtott iránymutatások*". Mindezen státuszát az adatvédelmi tisztviselőnek a (49) preambulumbekezdésben foglaltak töltik fel valódi tartalommal, mely szerint „*az adatvédelmi tisztviselőt, függetlenül attól, hogy az adatkezelő alkalmazottja-e vagy sem, olyan hatáskörrel kell felruházni, hogy feladatát teljesen függetlenül gyakorolhassa*."

Az adatvédelmi tisztviselő megkülönböztetett helye és szerepe az adatvédelmi jogszabályok érvényesülését szolgáló jogintézmények között aligha megkérdőjelezhető. A GDPR rendelkezéseivel összhangban álló adatkezelői – és bizonyos esetekben adatfeldolgozói- magatartást függetlenül, tanácsadással előmozdító funkció átfogó felkészültséget igényel.

A szerepkör komplexitására és súlyára tekintettel az Infotv. korábban meghatározott végzettség megléte esetében tette lehetővé a belső adatvédelmi felelősi pozíció betöltését. Ennek értelmében „*jogi, közigazgatási, informatikai vagy ezeknek megfelelő, felsőfokú végzettséggel*",[24] lehetett csak valaki belső adatvédelmi felelős. A GDPR ettől eltérően nem végzettség orientáltan, hanem kompetencia alapon határozza meg a kijelölés feltételeit. Így az adatvédelmi tisztviselőnek mindenekelőtt

[23] 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

[24] Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 24. § (1) bekezdés 2018. július 25-ig hatályos szövege.

megfelelő szakmai rátermettséggel, szakmai ismeretekkel és a feladatellátást lehetővé tevő képességekkel kell rendelkeznie.[25]

A GDPR által alkalmazott követelményrendszer egyszerre tekinthető megengedőbbnek és szigorúbbnak, mint a korábbi magyar szabályozás. Megengedőbb, hiszen a jogalkotó által korábban megjelölt végzettség hiányában is lehetőséget biztosít adatvédelmi tisztviselői feladatok ellátására, ugyanakkor az átfogó és komplex ismeretek kritériumrendszere a korábban statikus elvárásokat dinamikussá tette. Hiszen a rendeletben foglalt „*az adatvédelmi jog és gyakorlat szakértői szintű ismerete*" kitétel permanens elvárásként azonosítható, amelynek az adatvédelmi tisztviselők csak folyamatos képzés és ismereteik naprakészen tartása mellett tudnak megfelelni!

Különösen igaz ez a (97) preambulumbekezdés ismeretében, amely értelmében az adott tisztviselő *szakértelmének megfelelő szintjét*, mint elvárást mindig az adatkezelő vagy adatfeldolgozó konkrét tevékenységének, továbbá a személyes adatok védelmének elvárt szintje alapján lehet meghatározni.[26]

Mint az látni fogjuk, az adatvédelmi tisztviselő naprakész szakmai ismereteinek rendeletből fakadó követelményének különös jelentősége lesz az AIA megfelelés vonatkozásában is, hiszen a mesterséges intelligencia rendszerek személyes adatokkal való kapcsolata során elengedhetetlen a tisztviselői kontrollfunkciók hatékony működése.

2.1. Adatvédelmi tisztviselő kijelölése

A GDPR egyértelmű rendelkezéseket tartalmaz arra nézve, hogy mely adatkezelőknek és adatfeldolgozóknak kötelező adatvédelmi tisztviselőt kineveznie. A kijelölési kötelezettség elsődlegesen a szervezetek tevékenységével áll összefüggésben. Kötelező a kijelölés a közhatalmi vagy egyéb, közfeladatot ellátó szervek esetében, továbbá azon adatkezelőknél és adatfeldolgozóknál, ahol a főtevékenység végzése olyan adatkezelést eredményez, amely jelentős hatást képes gyakorolni az érintettek magánéletére.[27]

Az AIA összefüggésében a fő kérdés az, hogy módosulhat-e a jelenleg kialakult, adatvédelmi tisztviselői kijelölésre irányadó joggyakorlat akkor, ha az adott adatkezelő vagy adatfeldolgozó bizonyos MI-rendszerek alkalmazását kezdi meg?

Következésképp jelen körben semmiképp sem a közhatalmi szervek, illetve közfeladatot ellátó szervek kötelező kijelölés eseteit, hanem a GDPR 37. cikk (1) bekezdés b)[28] pontjában rögzített feltételek vizsgálatát kell, hogy érintse a vizsgálat.

[25] Péterfalvi – Révész – Buzás, 2021, i.m. 418. o.
[26] U.o. 419. o.
[27] U.o. 413. o.
[28] Hivatkozott szakasz úgy fogalmaz, hogy az adatkezelő vagy az adatfeldolgozó fő tevékenységei olyan adatkezelési műveleteket foglalnak magukban, amelyek jellegüknél, hatókörüknél és/vagy céljaiknál fogva az érintettek rendszeres és szisztematikus, nagymértékű megfigyelését teszik szükségessé.

Az adatkezelő, adatfeldolgozó főtevékenységének, illetve az érintettek rendszeres és szisztematikus, nagymértékű megfigyelésének megítélésével vonatkozó állásfoglalásában az adatvédelmi munkacsoport is részletesen foglalkozott.[29] Főtevékenység alatt a munkacsoport az adatkezelő, adatfeldolgozó céljainak eléréséhez szükséges legfontosabb műveleteket érti azzal, hogy a „fő tevékenység" definíciójának ki kell terjednie valamennyi olyan aspektusra is, amely az adott szerv (legyen az adatfeldolgozó vagy adatkezelő) tevékenységének elválaszthatatlan részét képezi.[30]

Ugyancsak értelmezésre szorul a „nagy mértékű" kitétel. Azt a Munkacsoport is leszögezte, hogy egzakt határértékeket nincs lehetőség megállapítani, azonban vannak olyan szempontok, amiket a mérlegelés során alapul kell venni:

- Az érintettek száma, vagy konkrét, vagy népességarányos meghatározással,
- Az adatok mennyisége és/vagy a kezelés alá vont adatok köre,
- Az adatkezelési tevékenység permanenciája,
- Az adatkezelési földrajzi kiterjedtsége.

A Munkacsoport kitért az érintettek rendszeres és szisztematikus megfigyelésének elemzésére is. Az általános adatvédelmi rendelet e körben sem alkalmaz konkrét definíciót, csupán a (24) preambulumbekezdés utal az érintettek interneten való nyomon követesére és a profilalkotásra, ugyanakkor természetesen aligha értelmezhető ilyen szűkítően a fogalompár. Az iránymutatás a rendszeresség esetében az időben való szabályszerűen visszatérő jelleget hangsúlyozza, míg a „szisztematikus" kifejezést a módszeresség és megszervezettség jegyeinek meglétével tartja igazolhatónak. Érdemes megjegyezni, hogy a Munkacsoport iránymutatásában az érintettek rendszeres és szisztematikus megfigyelésének példájaként már hivatkozza az intelligens mérőberendezések, intelligens gépjárművek vagy éppen a lakásautomatizálás technológiáját[31], amelyek értelmezhetőek akár a mesterséges intelligencia előszobájaként is.

Az adatvédelmi tisztviselő kijelölésének kötelezettsége tehát az adatkezelő és adatfeldolgozó fő tevékenységének függvényében állapítható meg, amely fogalom viszont tágan értelmezendő, magába foglalva így nem csak az adott szervezet fő céljait, hanem az azokhoz szükségszerűen kapcsolódó tevékenységeket is. Könnyű belátni, hogy olyan esetekben, mikor az adatkezelő vagy adatfeldolgozó fő tevékenységének támogatása érdekében MI-rendszert alkalmaz, úgy fokozott figyelemmel szükséges ellenőrizni az adatvédelmi tisztviselő kijelölésére irányadó szabályokat, ugyanis az egyes MI-rendszerek a cél és felhasznált adatok függvényében akár olyan szervezeteknél is indikálhatják a DPO kijelölésének

[29] Article 29 Data Protection Working Party: *Guidelines on Data Protection Officers ('DPOs')* (wp243rev.01) (a továbbiakban WP 243 rev.01.) 9. o.
[30] U.o.
[31] WP 243 rev.01., i.m. 9-10. o.

szükségességét, amelyeknél ilyen rendszerek alkalmazása nélkül egyébként erre nem lenne kötelezettség.

2.2. Az adatvédelmi tisztviselő feladatai

Az adatvédelmi tisztviselő az adatvédelmi jogszabályokról és azok helyes alkalmazásáról tanácsot ad adatkezelőnek, ideértve adatkezelő munkavállalóit is. A tanácsadás mellett a megfelelés ellenőrzése képezi a legfontosabb kötelezettséget, ugyanis mind a jogszabályok, mind pedig az adatkezelőre, adatfeldolgozóra irányadó belső szabályok érvényesülését felügyeli a DPO. [32]

A megfelelés ellenőrzése magába foglalja többek között az információk beszerzését, az adatkezelési tevékenységek elemzését épp úgy, mint a tájékoztatások és adott esetben ajánlások kiadásának lehetőségét is. [33] A beépített adatvédelem elvéből következik, hogy valamennyi, a személyes adatok kezelését magába foglaló művelet és folyamat tervezésének már a legelején, megfelelő időben szükséges bevonni az adatvédelmi tisztviselőt, aki így a tanácsadást és megfelelésellenőrzést már a kockázatok feltérképezésének fázisában is biztosítani tudja.[34]

A tisztviselőnek megkülönböztetett szerepe és feladata van az adatvédelmi hatásvizsgálatok, illetve a felügyeleti hatóságokkal való kapcsolattartás biztosításának tekintetében. [35]

Az általános adatvédelmi rendelet kockázatközpontú logikája az adatvédelmi tisztviselő feladatainak meghatározásában is megjelenik, ugyanis a 39. cikk (2) bekezdése alapján a DPO feladatait „*az adatkezelési műveletekhez fűződő kockázat megfelelő figyelembevételével, az adatkezelés jellegére, hatókörére, körülményére és céljára is tekintettel végzi*". A Munkacsoport egyfajta „józan ész" szerinti zsinórmértékként hivatkozik a bekezdésben foglaltakra, mint ami a tisztviselő feladat-priorizálását hivatott előmozdítani, lehetővé téve a kockázatokra tekintettel a különböző adatkezelési művelet közötti figyelem- és erőforrásmegosztást. [36]

A tanácsadás és ellenőrzés tehát az adatvédelmi tisztviselői feladatok alap attribútumai. Ezek mentén értelmezhető az adatkezelői, adatfeldolgozói szervezetrendszerben elfoglalt helye a pozíciónak, ami a megfelelést és annak bizonyíthatóságát hivatott garantálni. Ezen szerepkör a beépített adatvédelem elvének érvényesülésével megteremti annak lehetőségét, hogy valamennyi, a személyes adatokat érintő folyamat felett emberi kontroll érvényesüljön, amely kitétel különösen az AIA függvényében nyer majd többlet jelentést.

[32] Szabó, 2018, i.m. 8. o.
[33] WP 243 rev.01., i.m. 20. o.
[34] Szabó E. in. 2018, i.m. 8. o.
[35] WP 243 rev.01., i.m. 20. o.
[36] WP 243 rev.01., i.m. 21. o.

III. A Mesterséges Intelligencia Rendelet: kockázatalapúság és a magánélet védelmének egyes kérdései

1. AIA és a személyes adatok védelme

Az AIA maga is számos rendelkezést tartalmaz a természetes személyek személyes adatainak védelmével összefüggésben. Érdemes ezen a ponton utalni az AIA (10) preambulumbekezdésére, amely értelmében *az MI-rendszerek forgalomba hozatalára, üzembe helyezésére és használatára vonatkozó, e rendelettel megállapított harmonizált szabályoknak meg kell könnyíteniük, hogy az érintetteket a személyes adatok és egyéb alapvető jogok védelmére vonatkozó uniós jog értelmében megillető jogok és egyéb jogorvoslatok ténylegesen érvényesüljenek, illetve lehetővé kell tenniük az említett jogok és egyéb jogorvoslatok érintettek általi gyakorlását.*

A személyes adatok fokozott védelmére irányuló kötelezettségek vonatkozásában elégséges csupán megemlíteni az AIA 10. cikk (2) és (5) bekezdésében foglalt, a nagy kockázatú MI-rendszerek által használt tanító-, validálási és a tesztadatkészletek személyes adatokat érintő előírásait, vagy éppen az 50. cikk (3) bekezdését, amely az érzelemfelismerő rendszer vagy a biometrikus kategorizálási rendszer alkalmazásával összefüggésben utal kifejezetten az ilyen adatok védelmére.

Látható, hogy az AIA hangsúlyosan kezeli a személyes adatok védelmének kérdését, amit alátámaszt többek között a hivatkozott preambulumbekezdés megfogalmazása is, ahogy a jogalkotó azt megkülönböztető jelleggel, külön nevesítve emelte ki a többi alapjog közül. Az MI-rendszerek, különösen a profilalkotás és az automatizált döntéshozatal területén valójában szignifikáns kockázatokat hordoznak a természetes személyek személyes adatainak védelme terén, így indokolt és célszerű is fokozott figyelmet fordítani a két szabályozási rezsim egymással való kölcsönhatására.

2. Az AIA kockázatrendszerének kontextusa

Látható, hogy mind a GDPR, mind az AIA – hasonlóan más, technológiai tárgyú szabályozásokhoz- esetében kockázat alapú megközelítést érvényesített a jogalkotó. Az AIA alkalmazásában is azt a bevett gyakorlatot követi a jogalkotó, miszerint a kockázat az nem más, mint a kár bekövetkezési valószínűségének és az említett kár súlyosságának kombinációja.[37] A kockázat, mint központi fogalom egyszersmind annak beismerése is, hogy a teljeskörű biztonság elérése nem reális. Ha pedig ezt elfogadjuk, akkor célként csak a kockázatok egy meghatározott szintre csökkentése jelölhető meg, olyan szintre, ami az adott közösség, társadalom számára még elfogadható.[38]

[37] AIA 3. cikk 2. pont

[38] Tóth András: Az Európai Unió Mesterséges Intelligencia Törvényéről. *Gazdaság és Jog*, 2024/5-6. 3-11. o.

Az AIA a kockázatalapú megközelítés jegyében az MI- rendszerek esetében az általuk hordozott és jelentett kockázat alapján négy csoportot különböztet meg. Így beszélhetünk elfogadhatatlan kockázattal, nagy vagy magas kockázattal, korlátozott kockázattal, illetve a minimális kockázattal működő MI-rendszerről. A jelzett kategóriákon kívül az AIA külön rendelkezéseket tartalmaz az úgynevezett általános célú MI- rendszerek (GPAI) tekintetében. [39] A kockázat alapú besorolás esszenciális jelentőségű, ugyanis a jogalkotó az eltérő csoportokhoz eltérő követelményeket, jogalkalmazói magatartásokat rendel. Ezen megközelítésben manifesztálódik az az európai uniós jogalkotásban megfigyelhető bináris szemlélet, ami az alapvető jogok védelmét hivatott előmozdítani, nevezetesen, hogy minden alapvető jognak van egy „lényege", amit védeni kell, ugyanakkor ezen túlmenően a jogvédelem az optimalizálásra törekszik. Az alapvető jogokat tehát a lehető legnagyobb mértékben kell védelmezni, azokat csak az arányosság elvét figyelembe véve lehet korlátozni.[40]

Az AIA által megjelölt MI-rendszerkategóriák tehát egyfajta *alapjogi lépcsőt* is megtestesítenek. A társadalmi érdekekre és egyéni jogokra különböző kockázatot jelentő MI-rendszerekkel szemben más védelmi szintet vár el a jogalkotó, ami egyszersmind azt is jelenti, hogy a jogalkalmazóknak erre figyelemmel kell saját belső megfelelési keretrendszerüket felkészíteni és átalakítani. Az MI-rendszerek bevezetését és használatát megelőzően tehát nem csak az expressis verbis megfogalmazott regulációs elvárásoknak, hanem a mindenkor fennálló társadalmi és egyéni jogvédelmi igényeknek is meg kell tudni felelnie a jogalkalmazóknak.

Ezen a ponton érdemes részleteiben is megvizsgálni az AIA által megjelölt MI-rendszerek kockázati kategóriáit, kiemelt figyelemmel a személyes adatok megjelenésére.

Az AIA 5. cikk taxatív felsorolásban határozza meg, hogy milyen MI-rendszerek használata tilalmazott. Így

- tudatalatti, manipulatív technikák alkalmazása, amelyek célja, hogy egy személy viselkedését befolyásolja, vagy döntési képességét lerontsa,
- adott személy életkor, fogyatékosság, társadalmi vagy gazdasági deprimáltságból eredő sebezhetőségét célzottan kihasználó alkalmazás,
- egyének vagy csoportok viselkedés vagy személyes tulajdonságaik, személyiségi jegyeik alapján történő értékelése, osztályzása,
- egyes személyek kockázatértékelése a bűncselekmény elkövetésére való esély meghatározása érdekében,
- arcfelismerőadatbázis létrehozása vagy bővítése interneten elérhető, vagy zártláncú televízió-felvételek nem célzott lekérdezésével,

[39] U.o.

[40] Almada, Marco – Petit, Nicolas: The EU AI Act: Between Product Safety and Fundamental Rights. *Robert Schuman Centre for Advanced Studies Research Paper No. 2023/59*.

- természetes személyek érzelmeiből következtetni képes MI-rendszer alkalmazása munkahelyi vagy oktatási környezetben,
- biometrikus kategorizálási rendszerek alkalmazása, amelyek célja a természetes személyek faji, politikai, szexuális életük, vallási vagy világnézeti meggyőződésük, szakszervezeti tagságuk kikövetkeztetése megvalósulhasson,
- „valós idejű" távoli biometrikus azonosító rendszerek használata nyilvános helyen, bűnüldözési célból, amely kitétel alól ugyanakkor a rendelet biztosít kivételt.

A tiltott Mi-gyakorlatok tehát azokat a célokat és körülményeket jelölik, amelyek mentén az új technológia nem válik alkalmazhatóvá. Ugyanakkor a megjelölt felhasználási tilalmak mindegyikének előfeltétele a személyes adatok[41] kezelése, amelyek nélkül nem volna lehetséges az adott rendszer alkalmazásáról beszélni. Ez alól esetleg az első tilalom, a *tudatalatti, manipulatív technikák* esetében merülhet fel annak lehetősége, hogy nem személyre szabott, hanem bizonyos csoportjellemzők alapján alkalmazott felhasználásra is lehetőség nyílik, azonban ebben az esetben is megvalósul a személyes adatok kezelése annyiban, hogy a befolyásolni kívánt személy meghatározott paraméterei (mint például életkor, lakóhely, iskolai végzettség stb., amelyek szintén személyes adatnak minősülnek) teszik a manipulációs kísérlet „célpontjává".

Érdemes ugyanakkor megjegyezni, hogy lehetséges – különösen a szubliminális technikák esetében- olyan eljárás, ami kifejezett perszonális targetálás nélkül kíván ilyen rendszert alkalmazni, amely esetben személyes adatok nem kerülnek felhasználásra, azonban ezek hatékonysága messze elmarad a személyre szabott alkalmazási lehetőségekkel szemben, így jóval nagyobb valószínűséggel számíthatunk e körben is a személyes adatok potenciális megjelenésére.

A tiltott MI- gyakorlatok egyszersmind a személyes adatokra, így pedig a természetes személyek jogaira és szabadságaira vonatkozó legsúlyosabb kockázatokat jelölik, tehát a rendeletben kifejtett esetek kivételével nincs helye a forgalomba hozatal, üzembe helyezés vagy használat vonatkozásában mérlegelésnek, ha az adott rendszer célja kimeríti a felsorolt kategóriák valamelyikét.

A tiltott MI-gyakorlatokkal összefüggésben az adatvédelmi tisztviselői feladat főszabály szerint a prevencióra korlátozódik, vagyis a GDPR 39. cikk (1) bekezdés b) pontja értelmében ellenőrzi az irányadó jogszabályoknak való megfelelést, és amennyiben elfogadjuk azt, hogy a nevezett tilalmak személyes

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

adatok felhasználásával kell, hogy együtt járjanak, úgy a megfelelés e körben csak az előzetes észlelést és bevezetést meggátoló tevékenységként értelmezhető.
A gyakorlatban azonban nem feltétlenül lehet ilyen egyértelmű válaszvonalakat húzni. Erre példaként érdemes említeni az AIA 5. cikk (1) bekezdés f)[42] pontjában foglaltakat. Hivatkozott pontban egyértelmű jogalkotói szándék fedezhető fel: az emberi érzelmeket, mint a magánélet (privacy) legbelsőbb, legszemélyesebb magját kívánják oltalomban részesíteni. Mégis kettős feltételrendszer rajzolódik ki. A tilalom maga ugyanis csak a munkahelyi, illetve oktatási intézmények területére korlátozódik, kivéve, ha a használata, üzembe helyezése vagy forgalomba hozatala orvosi vagy biztonsági okokból történik.

A hatályos magyar szabályozás értelmében munkahelyi környezetben a munkavállaló a munkaviszonnyal összefüggő magatartása körében ellenőrizhető, amihez a munkáltató technikai eszközt is alkalmazhat.[43] Ugyanakkor a megfelelő tájékoztatás mellett természetesen az ilyen ellenőrzésnek is meg kell felelnie a GDPR 5. cikkében rögzített alapelveknek, így -többek között- a tisztességes adatkezelés elvének is. Ez zárja ki az olyan elektronikus megfigyelőrendszer alkalmazásának lehetőségét, amely alkalmas a munkavállalók és az általuk végzett tevékenység folyamatos, állandó jellegű megfigyelésére.[44]

Munkahelyi környezetben a természetes személyek érzelmeiből következtetést levonó MI-rendszer alkalmazása csak abban az esetben lehet jogszerű, ha annak célja orvosi vagy biztonsági okokra visszavezethető ellenőrzés, vagyis a munkavállalók fizikai, egészségi állapotának megóvását, megőrzését biztosító technológiai környezet kialakítását szolgáló intézkedésnek felel meg. Nehéz volna egy ilyen rendszer jogszerű működtetését elképzelni a GDPR 35. cikk szerinti adatvédelmi hatásvizsgálat lefolytatása nélkül, amelyben – mint az elszámoltathatóság egyik eszköze- az adatvédelmi tisztviselőnek a tanácsát kötelező kikérni.

A tiltott MI-rendszerek kiszűrése, amennyiben azok személyes adatokat is kezelnének, egy olyan feladat, amelybe az adatvédelmi tisztviselő bevonása – a beépített és alapértelmezett adatvédelem kötelezettségének való megfelelés okán is- elkerülhetetlennek mutatkozik. Ez természetesen nem csak az adatkezelő szervezetre, hanem magukra az adatvédelmi tisztviselőkre is többlet kötelezettséget

[42] A természetes személyek érzelmeiből következtetést levonó MI-rendszerek forgalomba hozatala, e konkrét célra történő üzembe helyezése, illetve használata a munkahelyek és az oktatási intézmények területén, kivéve amennyiben az MI-rendszer használata, üzembe helyezése vagy forgalomba hozatala orvosi vagy biztonsági okokból történik.

[43] A munka törvénykönyvéről szóló 2012. évi I. törvény (Mt.) 11/A. § (1) bekezdés

[44] NAIH: *Munkahelyi kamerás megfigyelés szabályai és jogszerűsége*. https://naih.hu/files/dr-Horuczi-Szilvia_A-munkahelyi-kameras-megfigyeles-szabalyai_PPT_STARII-zarokonferencia.pdf (2024.12.31.)

telepít, hiszen a GDPR 37. cikk (5) bekezdésében foglalt *szakmai rátermettség*[45] kifejezés magába kell, hogy foglalja azokat az ismereteket is, amelyek az adatvédelmi jogszabályok és joggyakorlat ismeretén túl elengedhetetlenek a teljeskörű feladatellátáshoz.

Ez utóbbi értelmezést támasztja alá az EDBP riportja is, amelyben az Európai Adatvédelmi Testület kifejti azon álláspontját, miszerint az adatvédelem és a magánélet védelmét biztosító jogi környezet gyorsan és dinamikusan változó terület, amiből következik, hogy az adatvédelmi tisztviselőknek nem elégséges pusztán az ehhez kötődő joggyakorlat és jogszabályi környezet naprakész ismerete. A szakmai ismereteknek ki kell terjedniük az európai adatvédelmi irányelvekkel kapcsolatos új irányokra is, kiváltképp az úgynevezett „Big Five" jogszabályokra is (a digitális szolgáltatásokról szóló rendelet, digitális piacokról szóló jogszabály, adatkormányzási rendelet, adatrendelet és a mesterséges intelligencia rendelet).[46]

3. A nagy kockázatú MI-rendszerek

Az AIA a tiltott MI-rendszereket követően rendelkezik az úgynevezett nagy kockázatú MI-rendszerekről.

Egy MI-rendszer nagykockázatúként való besorolása nem csak az ellátott funkciótól függ, hanem attól is, hogy milyen cél érdekében és milyen módon kerül alkalmazásra. [47]

A rendelet két fő kategóriáját különbözteti meg a fejezetben tárgyalt MI-rendszereknek:

a)az MI-rendszereket az AIA III. mellékletben felsorolt területek valamelyikén kívánják használni;[48]

b) az MI-rendszerek az egészségre és a biztonságra nézve károsodás, vagy az alapvető jogokra nézve kedvezőtlen hatás kockázatát jelentik, és az említett kockázat megegyezik a károsodás vagy a kedvezőtlen hatás azon kockázatával, amelyet a III. mellékletben már említett nagy kockázatú MI-rendszerek jelentenek, vagy annál nagyobb.[49]

A biometrikus azonosítás és az érzelemfelismerő rendszerek, amennyiben nem esnek a tiltott MI-rendszerek meghatározási körébe, úgy magas kockázatúnak fognak minősülni.[50] Az ilyen rendszerek forgalomba hozói kötelesek tájékoztatást

[45] GDPR 37. cikk (5) Az adatvédelmi tisztviselőt szakmai rátermettség és különösen az adatvédelmi jog és gyakorlat szakértői szintű ismerete, valamint a 39. cikkben említett feladatok ellátására való alkalmasság alapján kell kijelölni.

[46] EDPB*: Coordinated Enforcement Action Designation and Position of Data Protection Officers* (2023)

[47] Tóth, 2024, i.m. 3-11. o.

[48] AIA 7. cikk (1) bekezdés a) pont

[49] AIA 7. cikk (1) bekezdés b) pont

[50] Barkane, Irena: Questioning the EU proposal for an Artificial Intelligence Act: The need for prohibitions and a stricter approach to biometric surveillance. *Information Polity 27*(2), 2022. 147-162. o. https://doi.org/10.3233/IP-211524

nyújtani az érintettek részére a rendszer működéséről. A tájékoztatási kötelezettség alól csak abban az esetben lehet mentesülni, ha az alkalmazott rendszert bűncselekmények felderítése, megelőzése és kivizsgálása céljából jogszabály engedélyezi, azonban ekkor is biztosítani kell harmadik felek jogainak és szabadságainak megfelelő védelmét az uniós rendelkezésekkel összhangban.[51]

A kockázat alapú megközelítés megjelenik e körben is, ugyanis az AIA nem tekinti nagy kockázatúnak az adott MI-rendszert, ha annak működése nem jelent jelentős kockázatot a természetes személyek egészségére, biztonságára vagy alapvető jogaikra nézve ideértve természetesen azt is, ha nem történik lényeges befolyásolás a döntéshozatal eredményére.

Ugyanakkor, ha egy III. mellékletben említett MI-rendszer profilalkotást végez, azt minden esetben nagy kockázatú rendszerként kell azonosítani.[52]

Az AIA differenciált megközelítést alkalmaz a kötelezettségek tekintetében attól függően, hogy a magas kockázatú mesterséges intelligencia rendszerek vonatkozásában az egyes szereplők milyen minőségben jelennek meg. Az előírások részletes felsorolása meghaladná a jelen tanulmány rendelkezésére álló lehetőségeket, így ezen a ponton csak utalnék a megfelelésértékelés követelményére, amely – hasonlóan a GDPR által többek között a hatásvizsgálati mechanizmus során támasztottokhoz- nem csupán egy egyszeri, hanem egy folyamatos nyomon követést vár el, a változások jellegéhez mérten pedig felülvizsgálati kötelezettséget is támaszt a rendszerrel összefüggésben.[53]

Fontos harmonizációs rendelkezést tartalmaz az AIA 27. cikke, amely az alapjogi hatásvizsgálat kötelezettségéről rendelkezik. Azon magas kockázatú MI-rendszerek bevezetése előtt, amelyek alkalmazói az AIA 27. cikk (1) bekezdésben foglaltaknak megfelelnek, alapjogi hatásvizsgálatot szükséges elvégezniük, aminek ki kell térnie a rendszer alkalmazásának folyamatleírására, a rendszer használatának gyakoriságára, az érintettek csoportjának meghatározásra, ezen személyi körre irányuló kockázatok bemutatására, a feltárt kockázatok csökkentésére irányuló intézkedésekre- ideértve a belső irányítás és panaszkezelés szabályait is- továbbá az emberi felügyeleti mechanizmus ismertetésére. [54]

Ugyanezen cikk (4) bekezdése rendelkezik arról, hogy amennyiben a GDPR, vagy a bűnügyi adatvédelmi irányelv alapján elkészített adatvédelmi hatásvizsgálat alapján már az alkalmazó megfelelt a fentebb hivatkozott kötelezettségek bármelyikének, úgy az alapvetőjogi hatásvizsgálatnak ki kell egészítenie az említett adatvédelmi hatásvizsgálatot.[55]

[51] Tóth, 2024, i.m. 3-11. o.
[52] AIA 6. cikk (3) bekezdés d) pont
[53] AIA 43. cikk
[54] AIA 27. cikk (1) bekezdés
[55] AIA 27. cikk (4) bekezdés

A GDPR 35. cikk (2) bekezdése értelmében amennyiben az adatkezelőnél van adatvédelmi tisztviselő kinevezve, úgy az adatvédelmi hatásvizsgálat elvégzésekor annak szakmai tanácsát kötelező kikérni.[56]

Az AIA által meghatározott alapvetőjogi hatásvizsgálat esetében tehát mindenképp megállapítható az adatvédelmi tisztviselő kötelezettségének megjelenése abban az esetben, ha a magas kockázatú MI-rendszer a hivatkozott cikkben szabályozott személyes adatokat érint, és amire nézve e körben adatvédelmi hatásvizsgálat készült. Ilyetén megállapítható, hogy közvetve maga az AIA is tartalmaz feladatellátási kötelezettséget az adatvédelmi tisztviselők számára, hiszen nevezett adatvédelmi hatásvizsgálatnak kiegészített részévé kell tenni az alapjogi hatásvizsgálatot. Ez pedig- a rendelet nyelvtani értelmezését alapul véve- azt indikálja, hogy az adatvédelmi hatásvizsgálat keretrendszerét kell kiegészíteni az AIA vonatkozó rendelkezéseivel, így, ha magát az alapjogi hatásvizsgálatot nem is az adatvédelmi tisztviselő folytatja le, egyfajta ellenőrzési funkciót a két vizsgálati anyag egységesítésében el kell látnia.

4. Az emberi felügyelet szerepe és kötelezettsége

Az AIA egyik központi garanciális elemének tekinthető az MI-rendszerek vonatkozásában az úgynevezett emberi felügyelet biztosításának kötelezettsége. A humán kontroll garanciális elemként való megjelenése felveti annak kérdését, hogy az adott MI-rendszer tekintetében kötelezett szervezet meglévő kontrollszervei milyen szerepben kell, hogy megjelenjenek.[57]

Az AIA (73) preambulumbekezdése a nagy kockázatú MI-rendszerek esetében kifejti, hogy azokat „*úgy kell megtervezni és fejleszteni, hogy a természetes személyek felügyelhessék működésüket, valamint biztosíthassák rendeltetésszerű használatukat és hatásaik kezelését a rendszer életciklusa során. E célból a rendszer szolgáltatójának a forgalomba hozatalt vagy üzembe helyezést megelőzően megfelelő emberi felügyeleti intézkedéseket kell meghatároznia. Így különösen, az ilyen intézkedéseknek adott esetben garantálniuk kell azt, hogy a rendszer olyan beépített működési korlátokkal rendelkezzen, amelyeket maga a rendszer nem tud felülbírálni, és reagáljon az emberi üzemeltetőre, valamint hogy az emberi felügyeletet ellátó természetes személyek rendelkezzenek az e feladat ellátásához szükséges szakértelemmel, képzéssel és felhatalmazással”.*[58]

A Belga Adatvédelmi Hatóság (továbbiakban: BAH riport) 2024 szeptemberében kiadott egy információs füzetet, amely a mesterséges intelligencia rendszerek működését értelmezi a GDPR perspektívájából.

Az információs füzetben a BAH kiemeli, hogy mind a GDPR, mind pedig az AIA szigorú rendelkezéseket tartalmaz a személyes adatok biztonságos kezelésére

[56] GDPR 35. cikk (2) bekezdés

[57] Levitina, Anna: Humans in automated decision-making under the GDPR and AI Act. *Revista CIDOB d'Afers Internacionals* 138, 2024. 121-143. o. https://doi.org/10.24241/rcai.2024.138.3.121/en

[58] AIA (73) preambulumbekezdés

az adatkezelés teljes életciklusára vonatkozóan. A GDPR a 32. cikk (1) bekezdésében megfogalmazott a „*tudomány és technológia állása*" kitétel a technológia semlegesség talaján, a megfelelő védelmi szint mindenkori garantálását várja el az adatkezelések tekintetében. Az AIA alapul véve a GDPR által lefektetett elvárásokat, kiterjedt és komoly elvárásokat támaszt mindenekelőtt a magas kockázatú MI-rendszerek vonatkozásában, ugyanis ezek a rendszerek az adatkezelési folyamatokon túlnyúlóan is súlyos kockázatokat jeleltethetnek a természetes személyekre nézve, hiszen akár a tanító adatokban fellépő torzítások, vagy a tanító adatok manipulálása többlet kockázatot eredményezhet a természetes személyekre nézve. Ezen kockázatok kezelése érdekében az AIA preventív intézkedéseket vár el, amelyek között a kockázatelemzés és a rendszer működésének folyamatos ellenőrzésén túl megjelenik az emberi felügyelet meglétének biztosítása is. [59]

Ugyancsak kitér a BAH az automatikus döntéshozatal kérdésére. A GDPR lehetőséget biztosít arra, hogy az érintettek mentesüljenek az automatikus döntéshozatali eljárás alól, illetve kérhetik az ember által biztosított felülvizsgálatot. Az AIA a magas kockázatú MI-rendszerek tekintetében minden szereplőre kiterjedően írja elő a humánkontroll meglétét, így többek között a tanító adatok ellenőrzése, a rendszer teljesítményének mérése és felügyelete mellett a döntéshozatali folyamatba való beavatkozást is lehetővé kell tenni az emberi kontroll számára.

Külön kiemelendő az elszámoltathatóság kérdésköre, amelynek GDPR szerinti kötelezettségéről a korábbiakban már részletesen is szó esett. Az AIA nem nevesíti külön az elszámoltathatóságot, azonban átfogó kockázatkezelési rendszert vár el. A kockázatok értékelésének két folyamatlépése van. Az első, mely során az MI-rendszer kockázati besorolását kell azonosítani. Ennek eredményeképp pedig különböző szintű lépések megtétele válik szükségessé az eredmények függvényében. A magas kockázatú MI-rendszerek vonatkozásában részletesebb elemzést és alapjogi hatásvizsgálatot vár el a rendelet. Ilyen esetben átfogóbb dokumentálási kötelezettség lép érvénybe, továbbá az emberi felügyelet megfelelő biztosítását is érvényre kell juttatni.[60]

IV. Összegzés

A mesterséges intelligencia szabályozása és az általa jelentett jogi kockázatok mérséklése mind jogalkotói, mind pedig jogalkalmazói oldalon komoly kihívást jelent. Közhelyes kijelentésnek tűnhet, azonban jelen esetben valóban messzemenőkig érvényes kijelentésnek tekinthető, hogy a rendkívül gyorsan változó technológiai környezet talán sose látott feladatok elé állítja a jogalkalmazókat.

[59] Data Protection Authority of Belgium General Secretariat: *Artificial Intelligence Systems and the GDPR – A Data Protection Perspective*. Brussel, Data Protection Authority of Belgium General Secretariat, 2024.
[60] U.o.

Az AIA, hasonlóan a további „Big Five" jogszabályokhoz, kockázatalapú megközelítést vár el, felismerve és elismerve ezzel a teljeskörű, valamennyi aspektusra kiterjedő jogalkotás lehetetlenségét. Így viszont az AIA hatálya alá tartozó jogalanyokra hárul a folyamatos kockázatértékelés kötelezettsége. A megfelelés garantálása azonban nem képzelhető el a személyes adatok védelmére rendelt folyamatok és belső jogintézmények megfelelő szinkronizációja nélkül.
Mint az láthatóvá vált, az adatvédelmi tisztviselők dedikált feladatokkal rendelkeznek a különböző kockázatú MI-rendszerek jogszerűségének ellenőrzésében is. Az MI-rendszerek ugyanis éppen a természetes személyekre irányuló kiterjed hatások okán olyan kockázatot jelentenek, amelyeket a DPO-nak elkerülhetetlenül ellenőrizni és felügyelnie kell.

A hatósági joggyakorlat fog tudni majd választ adni arra a kérdésre, hogy a DPO a szervezeten belül milyen formában kell, hogy részt vegyen az MI megfelelés folyamatában, nota bene, mennyire lesz összeegyeztethető a tisztviselő és mondjuk az *AI Officer*[61] munkaköre, esetleg megállapításra kerül-e az összeférhetetlenség a két pozíció között?

Meglátásom szerint kijelenthető, hogy az adatvédelmi tisztviselőnek, amennyiben az MI-rendszer személyes adatokat is kezel, annak teljes életciklusa alatt felügyeletet kell gyakorolnia, mely feladatnak az ellenőrzésen túl ki kell terjednie az adatkezelési folyamatok elszámoltathatóságának garantálására hivatott eszközök összhangba tételére az AIA által elvárt dokumentációs kötelezettséggel épp úgy, mint az adatvédelmi eljárások MI specifikus átdolgozására. Ez természetesen többlet terhet és feladatot jelent, aminek az adatkezelő által biztosított erőforrások allokálásában is érződnie kell.

[61] Fontos megjegyezni, hogy az AIA nem tartalmaz rendelkezést egy, az érintett szervezeten belül dedikált személy vagy szervezeti egység létrehozására, amelynek feladata volna az MI-rendszerek megfelelésének garantálása. Ettől függetlenül több, mint valószínű, hogy a gyakorlat elő fog hívni ilyen pozíciókat, hiszen a komplex jogalkotói elvárások meg fogják követelni azt.

KORKÉP AZ ONLINE ÓRIÁSPLATFORMOK ÉS KERESŐPROGRAMOK PROBLEMATIKÁJÁRÓL

dr. Joó Patrik Zsolt
Doktorandusz, Pécsi Tudományegyetem Állam-és Jogtudományi Doktori Iskola
A szerző elérhetősége: drjoopatrik@gmail.com

DOI: 10.47272/KIKPhD.2024.3.3

ÖSSZEFOGLALÓ

A digitális gazdaságot uraló online óriásplatformok megkerülhetetlenül megjelennek az átlagember hétköznapjai mellett, a politika, a jog és a kultúra színpadán egyaránt. A „tech sztárok" és monumentális cégeik, felemelkedése és működése körüli hősi mítosz felszíne alatt, a szabadversenyt gáncsoló, offshore hálózatokkal, tömeges felvásárlásokkal és részvénypiaci manipulációval operáló aktorok találhatóak. Jelen tanulmány az ezzel kapcsolatos problémák elemzésére törekszik.

KULCSSZAVAK

Online óriásplatformok, nagyon népszerű keresőprogramok, digitális kapitalizmus, duo-és monopólium, offshore, megfigyelési kapitalizmus

I. Fogalom és tipizálás

1. Online platformok

Az online óriásplatformok és nagyon népszerű keresőprogramok fogalmi meghatározásához elsősorban tisztázni szükséges az ezeket magában foglaló online platform fogalmat. Ez nem egy egyszerű feladat, mivel a megnevezés magában foglalja az interneten elérhető, funkcióban és használatban egyaránt eltérő szolgáltatási típusok és variációk sokaságát.[1] Az online platform kifejezésbe beleértendők az olyan különféle formában és méretben létező platformok,[2] mint a keresőmotorok (Google, Bing), a közösségi média felületek (Facebook, X) a piacterek (Amazon, Ebay, Alibaba), a kreatív tartalomszolgáltatók (TikTok), az alkalmazásáruházak, a blogok és még sok más típusú online felület.[3] A platform tipizálásnak rengeteg féle megközelítése létezik – funkció, felhasználói interakció, monetizációs modell, földrajzi fókusz vagy technológiai megvalósítás alapján történő –, amelynek oka részben abban rejlik, hogy különböző célokat különböző

[1] Ld. a fogalommeghatározási problémákra: Hohmann, Balázs: A Digital Services Act és a Digital Markets Act termékekre és digitális szolgáltatásokra irányuló fogyasztói jogviszonyokat érintő rendelkezései. *In Medias Res 12*(2), 2023. 70. o. https://doi.org/10.59851/imr.12.2.4

[1] A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: Online platformok és a digitális egységes piac Lehetőség kihívás Európa számára, COM (2016) 288. 2. pont.

[3] OECD: What is an "online platform? *An Introduction to Online Platforms and Their Role in the Digital Transformation*, OECD Publishing, Paris, 2019. https://doi.org/10.1787/19e6a0f0-en

féleképpen érdemes megközelíteni. Az utóbbi évek két nagy európai rendeletében is eltérő megközelítést találunk. Amíg a Digitális Szolgáltatásokról szóló rendelet (továbbiakban: DSA) a digitális szolgáltatások működését és a felhasználók védelmét szabályozza,[4] addig a Digitális Piacokról szóló jogszabály (továbbiakban: DMA),[5] a digitális piacokon folyó versenyt felügyeli, és többek között a nagy cégek monopolhelyzetét igyekszik keretek közé szorítani. A variációk sokasága közül, érthetősége és átláthatósága okán, a dr. Papp János Tamás funkcionális eltérések oldaláról megközelített felosztását veszem alapul:

1. ábra: Funkcionális platform tipizálás

Forrás: Papp János Tamás: *A közösségi média platformok szabályozása a demokratikus nyilvánosság védelmében.* Egyetemi doktori disszertáció. Budapest, Pázmány Péter Katolikus Egyetem, 2021. 15. o.

Az ábrát látva, felmerül a kérdés, hogy milyen definícióval fedhető le ez a sokrétű és szerteágazó online tér variáció. Zódi Zsolt a következő fogalommeghatározást adja: az online platformok „*olyan weboldalak, amelyek embereket és más embereket vagy erőforrásokat kapcsolnak össze algoritmusokkal vezérelt adatfolyamok segítségével, és amelyekhez kellően nagy számú felhasználó csatalakozott ahhoz, hogy társadalmi hatásuk mérhető legyen*".[6] Ezt kiegészítve José Van Dijck a platformok közös elemeiként kiemeli, hogy hardveres infrastruktúrán alapulnak, működésük motorját

[4] Az Európai Parlament és a Tanács 2022. október 19-i (EU) 2022/2065 Rendelete a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról
[5] Az Európai Parlament és a Tanács 2022. szeptember 14-i (EU) 2022/1925 Rendelete a digitális ágazat vonatkozásában a versengő és tisztességes piacokról, valamint az (EU) 2019/1937 és az (EU) 2020/1828 irányelv módosításáról
[6] Zódi Zsolt: *Platformok, robotok és a jog.* Gondolat, Budapest, 2018. 103. o.

főleg a felhasználók által létrehozott adat tömeg képezi,[7] azokat üzleti modellek alapján meghatározott tulajdonviszonyok formalizálják, és felhasználói szerződések irányítják.[8] Továbbá közös jellemzőjük, hogy az adott platformon végbemenő folyamatok és szolgáltatások, algoritmusok– a platform lelkének tekinthető speciális, az adott platform tevékenységi körébe tartozó kódhalmazok – felhasználásával történnek. Ilyen algoritmusok végzik a Google indexelését, keresését és rangsorolását, ilyenek kezelik a Facebook hírfolyamát, az online boltok ajánlóit, a taxi, a szállás és a szolgáltatásközvetítők kereslet-kínálat összepárosítását is.[9]

2. Online Óriásplatformok

A 2000-es évek elején gombaként nővő platformok nagy része, a 2002-es „dotcom-buborék" következményeként hamar el is tűnt, viszont a megmaradtak közül páran, egyre nagyobb-és nagyobb teret hódítva, bizonyos esetekben a szabadpiac és a politika fölé nőve, megkerülhetetlenné, úgynevezett kapuőrökké („gatekeeper") váltak.[10] A DSA részben erre reagálva, a legfontosabb újításai között létrehozott két új többletkötelezettségekkel rendelkező platformfajtát, az „óriásplatform" (very large online platform, VLOP) és a „nagyon népszerű online keresőprogram" (VLOSE) kategóriáit.[11] Ezek olyan platformok [12]*„amelyek havonta átlagosan legalább 45 millió, a szolgáltatást aktívan igénybe vevővel rendelkeznek az Unióban.*" [13] A DMA (3) bekezdésében a kapuőrökről úgy ír, hogy azok a *„szolgáltatásaikon keresztül sok üzleti felhasználót képesek sok végfelhasználóval összekapcsolni, ami viszont lehetővé teszi számukra, hogy az előnyeiket – mint például a nagy adatmennyiségekhez való hozzáférésüket – átvigyék az egyik tevékenységi területről a másikra. Néhány ilyen vállalkozás a digitális gazdaságban teljes platform- ökoszisztémák felett gyakorol irányítást, és a meglévő vagy új piaci szereplők strukturális szempontból rendkívül nehezen tudnak velük versenyre kelni, bármennyire innovatívak és hatékonyak legyenek is ezek a piaci szereplők.*"[14]

Írásomban a DMA (3) bekezdésének megfogalmazásában említett, teljes platform- ökoszisztémákat leuraló vállalkozásokkal, különösen az Amazon, Facebook (Meta) és a Google (Alphabet)[15] gigacégek triumvirátusával, azok piaci

[7] Van Dijck, José Van – Poell, Thomas – De Waal, Martijn: *The platform Society. Public Values in a Connective World.* Oxford, Oxford University Press, 2018. 9. o. https://doi.org/10.1093/oso/9780190889760.001.0001

[8] Van Dijck, 2018, i.m. 9. o.

[9] Ződi, 2023, i.m. 63. o.

[10] *Digital Markets Act: Commison designates six gatekeepers*. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328 (2024.12.31.)

[11] Kis Kelemen Bence – Hohmann Balázs: Is There Anything New Under the Sun? A Glance at the Digital Services Act and the Digital Markets Act from the Perspective of Digitalisation in the EU. *Croatian Yearbook of European Law and Policy 19*(1), 2023. 225-248. o. https://doi.org/10.3935/cyelp.19.2023.542

[12] Ződi, 2023, i.m. 186. o.

[13] DSA 5.szakasz 33.cikk (1) bek.

[14] DMA (3) bek.

[15] *19 óriás: kijelölték a legnagyobb online platformokat és keresőmotorokat*. https://onlineplatformok.hu/cikk/19-orias-kijeloltek-a-legnagyobb-online-platformokat-es-keresomotorokat (2024.11.11.)

helyzetével, működésével és társadalomra gyakorolt hatásával kapcsolatos részproblémákra helyezem a hangsúlyt.

Ezzel részben alátámasztva az Európai Unió által alkotott rendeletek szükségességét, részben megalapozva egy jövőbeli dolgozatnak, ami kifejezetten az egyes problémákra adott válaszok sikerességét kívánja majd taglalni.

II. Korkép

1. A posztfordizmus zaja

Az internet forgalmának túlnyomó részét a 2010-es évek elejétől az online platformok generálták, így mára már közhely, hogy a különféle típusú életünket megkönnyítő – és paradox módon egyszerre komplikáltabbá tevő – technológiai vívmányok, átszővik az átlagember mindennapját. Kevés olyan része maradt az életnek, amit nem „fed le" valamilyen applikáció. Az online tevékenységek sokaságának, (csevegés, megosztás, kommentelés, ismerkedés, keresés, vásárlás, zenehallgatás, videónézés) lehetőségét megteremtő platformok, „olyan rendszert rejtenek, amelynek logikája és működése több a folyamat megkönnyítésének látszatánál. Ezek valójában aktívan formálják az életünket és a társadalom szerveződését."[16] Az online látott videók, cikkek, képek is többek puszta szórakoztató vagy érdekes tartalmaknál. Ezek sokszor tudatalatt hatnak ránk és formálják a gondolkodásunkat, világképünket, valamint ahogy azt Albert Bandura feltárta –a Tanzániában vetített szappan operákon keresztül[17],– a TV-ben (igaz ez az online térre is) látott tartalmak, műsorok élet értelmezési narratívákat adnak és viselkedési mintákat szabnak meg. Ez működhet a társadalom számára kedvezően – mint az Bandura esetében is történt a HIV vírus elleni védekezés kapcsán –, és természetes működhet destruktív, butító módon is. Az internet túlnyomó része mára már olyan hulladék – szebb szóval zaj – ami szennyezi a fogyasztó elmélyét. A posztfordizmus korára jellemző e mellett, hogy „*nő a dolgozók kiszolgáltatottsága, amit az is jelez, hogy egyre kevesebben vannak, akik élesen el tudják választani a munkát és a magánéletet. Még álmunkban is kísért a Tőke, mondja Fisher; egybeolvad az üzemcsarnok és a nappali, állapítja meg Han.*"[18] A korlátlan, tudatosságot mellőző, zsigeri ingerekre ható, emésztetlen tartalomfogyasztásnak és a céges világ által sokakra erőltetett munka függőségnek (divatosan „hustle culture") meg is van az ára. Súlyos boldogtalanság, figyelem-és önképzavar, valamint tömeges, stressz okozta betegségek, mint a kiégés és depresszió[19] burjánzik a nyugati társadalmakban. Sajnos megfigyelhető a

[16] Van Dijck, 2018, i.m. 9. o.

[17] Smith, Deborah: The theory heard'round the world. *Monitor on Psychology 33*(9), 2002. 30-32. o. https://doi.org/10.1037/e301142003-030

[18] Barcsi Tamás – Diósi Szabolcs: Hasznos test, dividuum, nyersanyag. A felügyelő társadalomtól az (ön)ellenőrző és megfigyelési kapitalizmusig. *Magyar Filozófiai Szemle* 2022/3. 181.o.

[19] Karim, Fazida, et al: Social media use and its connection to mental health: a systematic review. *Cureus 12*(6), 2020. 3.o. https://doi.org/10.7759/cureus.8627

szolidáris és a közösségi cselekvés válsága, ami többek között abban is mutatkozik[20], hogy a – a neoliberális kapitalizmus rendszerének természetéből fakadó – rendszerszintű problémák megoldása (mint a társadalmi leszakadások, klímaváltozás, elérhetetlen ingatlanárak, minőségi mentális és fizikai egészségügy, valamint a folyamatos munkakényszer) az egyénekre hárítódik, akik a milliókat érintő helyzetet „egyéni szociális problémaként" igyekeznek kezelni.[21]

2. Az online szólás kormányzói

A 2024-es adatok szerint, a világ lakosságának 62.3 % használ közösségi médiát, az átlagos napi fogyasztás pedig 2 óra 23 perc.[22] Papp Gábor szavaival élve „ők lettek az online szólás kormányzói". Az adott platform tulajdonlásához az azon folyó tartalmak feletti kormányzás társul, ami óriási társadalmi felelősséggel jár. Ezek a platformok átalakítják az információáramlás és a tájékozódás korábbi módozatait, amely folyamat nem nyugodtabb, jól értesült polgárokból álló közösségekhez vezetett, hanem az elsekélyesült, végletekig polarizált tömeghez. Kontrolljuk kiterjed arra, hogy ki, hogyan, és mit mondhat vagy közvetíthet a nyilvánosság számára, valamint képesek nyíltan vagy rejtetten („shadowbanning")[23] cenzúrázni, törölni az információkat, ezzel eldöntve, hogy mit, és mit nem láthatnak a felhasználók[24]. A szolgáltatásaik alkalmasak felhasználóik akár aktív navigálással történő manipulálására, és – mivel a rendelkezésükre álló, szinte korlátlan anyagi forrásokból kétségtelenül kiváló minőségű szolgáltatásokat képesek nyújtani – piaci monopóliumra törnek.[25]

III. Monopol– és Oligopol valóság

A sarki kis boltoknál és a piaci virágárusoknál talán még igaz, de a komolyabb tényezőjű cégek esetén nem, vagy alig érvényesül a neoklasszikus közgazdaságtan Adam Smith-i, vállalkozók közötti szabad verseny képe,[26] amelyben a piaci szereplők azért versenyeznek, hogy a fogyasztók igényeit a lehető legjobban

[20] Fenyvesi Balázs: *Miért veszélyes a teljesítményelv kiterjesztése életünk minden részére?*. https://merce.hu/2021/07/03/miert-veszelyes-a-teljesitmenyelv-kiterjesztese-eletunk-minden-reszere/ (2024.12.31.)

[21] Éber Márk Áron: *Kiégésre neveljük gyermekeinket?*. https://merce.hu/2023/02/28/kiegesre-neveljuk-gyermekeinket/ (2024.12.31.)

[22] Chaffey, Dave: *Global social media statistics research summary May 2024*. https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/ (2024.12.31.)

[23] Fowler, Geoffrey A.: *Shadowbanning is real: Here's how you end up muted by social media*. https://www.washingtonpost.com/technology/2022/12/27/shadowban/ (2024.12.31.)

[24] Papp, 2021, i.m. 27.o.

[25] Koltay András: *Trump elnök Twitter-fiókja és a szabadság halványodó amerikai álma*. https://index.hu/velemeny/2021/01/18/trump_elnok_twitter-fiokja_es_a_szabadsag_halvanyodo_amerikai_alma/ (2024.12.31.)

[26] Pogátsa Zoltán: *Van-e extraprofit? Mi egyáltalán a profit?*. https://merce.hu/2022/06/11/van-e-extraprofit-mi-egyaltalan-a-profit/ (2024.12.31.)

kielégítsék és ami szerint a piaci „láthatatlan kéz" elrendezéséből következően, végső soron állami beavatkozás nélkül mindenki számára előnyös megoldások születnek. Korunk valósága ehhez képest az, hogy a „létező kapitalizmust oligopóliumok és az azokat tulajdonló oligarchák által megvásárolt állam jellemzi."[27] A mára kialakult erőteljes piaci koncentrációt pedig „*magasabb árak, kevesebb startup-vállalkozás, alacsonyabb termelékenység és alacsonyabb bérek, magasabb jövedelmi egyenlőtlenség, kevesebb beruházás és a kisvárosok elsorvadása*"[28] jellemzi.

Példának véve a világ vezető gazdasági és katonai erejét, az USA-t, ahol megfigyelhetően alig egy-két szereplő határozza meg az adott iparágakat. A szénsavas üdítőitalok terén a Coca-Cola és a PepsiCo dominál, a gyorsposták esetében az UPS és FedEx szinte az egyedüli opciópáros, míg a bankkártyáknál túlnyomórészt a Visa és Mastercard jöhetnek szóba. [29] Pogátsa Zoltán közgazdász szerint „nem csak a reálgazdaság oligarchikus, hanem az azt birtokló pénzügyi világ is"[30]. Ezt igazolja a tény, hogy öt intézményes befektető – a Black-Rock, a Vanguard, a State Street, a Fidelity és a JP Morgan – tulajdonolja, például az S&P500 vállalati részvényeinek 80%-át[31]. A digitális érában is hasonló a helyzet, ahol a „geopolitikai színtéren a világ sikeres online társadalmi és gazdasági forgalmát lebonyolító cégek terén, megfigyelhető egy Kína (Tencent, Alibaba, Baidu és JD.com) - USA („big five tech giants" vagy GAFAM: Google, Amazon, Facebook, Apple és Microsoft[32]) között feszülő kétpólusú felállás. Jelenleg e téren az USA felé lejt a pálya,[33] hiszen napjaink legnépszerűbb portálja a Facebook, amit szorosan követ a YouTube, azt pedig az Instagram, a WhatsApp, a TikTok,[34] és a Messenger. (Azaz a világ hat legnépszerűbb közösségi oldalából négy a Meta amerikai gigacég kezében van). Mark Zuckerberg a 2010-es évek elején úgy fogalmazott, hogy „sok szempontból a Facebook inkább egy kormány mintsem egy vállalat. Hatalmas közösségünk van és minden más technológiai cégnél több szabályt alkalmazunk."[35]A social network-szolgáltatók területén a Facebooknak nagyjából 80%-os a súlya, míg a keresőmotorok esetéebn a 38 milliárd dolláros éves bevétellel rendelkező Google – ami csupán az Alphabet cég egy komponense – hegemónként szolgáltatja az internetes keresések 90%-át. Társadalmi szinten megszoktuk már, hogy ha valaminek utána akarunk nézni akkor a Google-hoz nyúlunk („Google a barátod"),

[27] Pogátsa Zoltán: *A Globális elit*. Budapest, Kossuth, 2022. 39. o.
[28] Tepper, Jonathan – Hearn, Denise: The *Myth of Capitalism: Monopolies and the Death of Competition*. New Jersey, Wiley, 2018. 37. o.
[29] Pogátsa, 2022, i.m. 36. o.
[30] Pogátsa, 2022, i.m. 37. o.
[31] Tepper – Hearn, 2018, i.m. 202.o.
[32] Ződi, 2023, i.m. 20. o.
[33] Van Dijck, 2018, i.m. 26. o.
[34] Ankit Vora: *The 20 Most Popular Social Media Platforms*. https://backlinko.com/social-media-platforms (2024.12.31.)
[35] Kirkpatrick, David: *The Facebook Effect. The inside story of the company that is connecting the world*. New York, Simon & Schuster, 2011. 254. o.

ha meg valakivel fel akarjuk venni a kapcsolatot akkor őt a legnagyobb eséllyel a Facebookon találjuk, és sorolhatnám. Ezeknél a platformoknál a teljes árukapcsolás („moat effektus")[36] létrejött, aminek a következménye, hogy az emberek többsége nem fog tudatosan alternatívát keresni.

IV. „A jéghegy alja"

1. A kezdet

Kezdeti gondolataim alapján, a fejlett világ legismertebb „sztár tech" vállalkozói vagy más néven „Big Tech oligarchái", tisztán és pusztán a zsenialitásuk okán gazdagodtak meg, valamint, hogy az a vállalat kerül a csúcsra, amelyik a jobb, hasznosabb technológiával rendelkezik.[37] Kimutatható, hogy az esetek nagy részében nem az nyer, amelyik a jobb technológiát vagy terméket nyújtja, hanem az, aki több tőkét tud szerezni maga mögé, és/vagy hatékony lobbierőt a megfelelő politikai döntéshozóknál. Jonathan Tepper kutatásában kimutatta, hogy a lobbizásra legtöbbet költő cégek volt, hogy évente öt százalékponttal verték meg az S&P500 tőzsdeindex eredményét.[38] Az ebből befolyó összegből pedig körforgásszerűen tehetik ezt meg újra és újra, ezzel is csökkentve a potenciális versenytársak esélyeit. A mindenki által ismert óriásplatform gigacégek, kockázati tőke társaságok általi megfinanszírozással, agresszív árazással, szisztematikus versenytársi eliminálással és tömeges felvásárlással – az Alphabet 258, a Meta Platforms 100 az Amazon pedig eddig 114 vállalkozást vásárolt fel[39]– váltak konkurenseik megkerülhetetlen infrastruktúrájává.[40] Az Amazon csupán a rajta lebonyolódó tranzakciókból, nagyobb összegű jutalékot (75 milliárd dollárt) képes realizálni, mint amennyit a magyar állam a költségvetési főösszegéből (65 milliárd). Nem volt ez mindig így. A részvénypiacon gyakori eset, hogy az adott cég valós értéke és a részvény ára – általában a céget körül lengő rajongói felhajtóerő („hype") vagy az 1982-ig tiltott cégek saját részvényfelvásárlása („buyback") hatására – radikálisan elválik egymástól.

Két példa erre, hogy „*az Amazon 1997-ben ment tőzsdére, 18 dolláros kibocsátási részvényárral, amely 2000-ra 100 dollár fölé nőtt. Történt ez annak ellenére, hogy a cég folyamatosan veszteséges volt.*"[41] A Tesla részvénye pedig éveken át úgy emelkedett, hogy a cég alapvetően nem volt nyereséges. Az csupán 2020-ban könyvelhetett el kisebb nyereséget mindeközben az árfolyama – botokkal való manipulálással [42]ugyan de –

[36] Chris Gallant: *How an economic Moat provides a competitive advantage*. https://www.investopedia.com/ask/answers/05/economicmoat.asp (2024.12.31.)
[37] Pogátsa, 2022, i.m. 8. o.
[38] Tepper, 2018, i.m. 189. o.
[39] Shale, Thomas: *Timeline of Amazon's Biggest Acquisitions*. https://www.feinternational.com/blog/timeline-of-amazons-biggest-acquisitions?utm_source=chatgpt.com (2024.12.31.)
[40] Ződi, 2023, i.m. 23. o.
[41] U.o.
[42] Pogátsa, 2022, i.m. 76. o.

megnyolcszorozódott.[43] Az amerikai álmot hajtó Tesla rajongók között nem egy széleskörűen ismert tény, hogy Elon Musk az induláshoz az amerikai államtól közel 500 milliós támogatást kapott, ami nélkül feltehetően el sem tudott volna indulni.[44]

A Google két korai nagy sikerű projektjében a YouTube-ban és a Google Books-ban közös pont, hogy mind a kettő indulásakor durván sértette a szerzői jogokat. A Google Books projektben előzetes engedélykérés nélkül kezdték el a kiadói jogokkal védett könyvek millióinak szkennelését. A YouTube esetében pedig figyelmen kívül hagyva a kiadói jogokat, az ezeket sértő felhasználói tartalmakat csak késve és vonakodva távolította el.[45] Az ellene folyó perek alatt a Google gazdasági szerepe olyan akkorára nőtt, hogy végül a bíróság „fair use"-nak minősítette a cég magatartását.[46] A YouTube is akkorára nőtt, hogy a nagy tartalom-előállítók számára kikerülhetetlen lett. A kérdés mindkét esetben az, hogy nőhetett volna-e a Google ekkorára, ha a kezdetekor nem sérti meg szisztematikusan a kiadói jogokat.[47]

A „Big tech oligarcák" szűk körének kialakulására jellemző (Peter Thiel, Jeff Bezos Elon Musk, Mark Zuckerberg), az egymás körbefinanszírozása, a többi feltörekvő piaci helyzetének szisztematikus ellehetetlenítése majd azok felvásárlás. Mark Zuckerberg-nek a kockázati tőkés Peter Thiel (Paypal alapító) –aki szerint „*a verseny a veszteseknek való*" – adta a legnagyobb összeget, ami különösen fontos volt ahhoz, hogy a sok tizezer hasonló kezdeményezés közül éppen a facebook váljon hegemónná.[48]A Jack Dorsey féle Twitterhez pedig többek között Jeff Bezos nyújtott nagy mennyiségű tőkét és sorolhatnám. Persze a gazdasági verseny kereteibe sok minden beleférhet. Ami tovább árnyalja a képet, hogy a segítők között gyakran megjelennek orosz oligarchák, kínai nagyemberek és az Uber esetében a szaúdi koronaherceg Mohammed bin Szalmán bőkezű finanszírozása is. Azé az úriemberé, aki még 2018-ban, a róla kritikus cikkeket író USA-ba disszidált, újságíró feldaraboltatásáról vált hírhedtté.[49]

2. Adóelkerülés

A tisztességes verseny felszámolása és korlátozása mellett, további probléma hogy a dollármilliárdokat kereső Big Tech cégek esetében „az adóelkerülés nem marginális ügyeskedés, hanem főáramú eljárás."[50] A 2020-as járványidőszakban négy fal közé szorult emberek többnyire online vásároltak, ami az Amazon egyik legjobb üzleti évét és Jeff Bezos átmeneti Forbes lista első helyét eredményezte, úgy, hogy

[43] U.o. 95.o.
[44] U.o. 85.o.
[45] Auletta, Ken: *Googled. The End of the World As We Know It.* London, Virgin Books. 2010. 152 -155. o.
[46] Raquel Xalabarder: Google Books and Fair Use: A Tale of Two Copyrights. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law 5*(1), 2014. 53–59. o.
[47] Ződi, 2023, i.m. 27. o.
[48] Pogátsa, 2022, i.m. 72. o.
[49] Kiss Soma Ábrahám: *Hasogdzsit élve daraboltak fel.* https://merce.hu/2018/10/17/hasogdzsit-elve-daraboltak-fel/ (2024.12.31.)
[50] Pogátsa, 2022, i.m. 31. o.

mindeközben a hivatalosan az ír adóparadicsomban bejegyzett cég egyetlen cent profitot sem jegyzett és így egyetlen cent nyereségadót sem fizetett.[51] A Tax Justice Network szakértői csoport 2020-as adatai szerint évente mindösszesen 427 milliárd amerikai dollárt kerülnek el a cégek és tulajdonosaik a világon adóparadicsomokon („tax haven") és offshore központokon keresztül.[52] Baljós előrejelzéseik szerint nagyjából 4.8 trilliárd (ami a már alapból is felfoghatatlan billió miliárdszorosát jelenti) dollárnyi adó összeget veszítenek el bizonyos országok az elkövetkezendő 10 évben ha ez így megy tovább.[53] Gabriel Zucman a „Hidden Wealth of Nations" című könyvében két fő adóelkerülési módszert jelöl meg. Az egyik az offshore, aminek a lényege, hogy az adott vállalat a tevékenységeit vagy nyereségét olyan országban végzi, ahol kedvezőbbek az adófeltételek (Svájc, Luxemburg, Kajmán szigetek, Egyesült Királyság és a Brit Virgin szigetek, Hollandia). Például, ha egy cég leányvállalatot alapít egy olyan országban, ahol alacsony vagy nulla a társasági adó, akkor az ottani leányvállalat nyereségét minimális adóval tudja elérni. A másik megoldási mód a transzferárazás. Ez olyan folyamatot takar, amikor egy több országban regisztrált telephelyekkel, leányvállalatokkal rendelkező vállalatcsoport, saját maga állapítja meg a telephelyek közötti kereskedelem árait, amivel optimalizálhatja az adófizetést úgy, hogy több profitot mutat ki abban az országban, ahol alacsonyabb az adókulcs[54]. A másik mód erre, hogy a magasabb adókulcsos ország leányvállalata – minimalizálva a nyereséget – alacsony áron vásárolja az adott szolgáltatást vagy terméket az alacsonyabb adókulcsú országban üzemelő testvérvállalatától. Ezek ma általános gyakorlatnak számítanak a multinacionális cégek körében, amit elősegít, hogy a világkereskedelem több mint 60%-a saját hálózataikon belül folyik.[55] Nem ártalmatlan, következmény nélküli pénzszerzési folyamatokról beszélünk. Ezen nyerészkedő és a „*krónikus még szindróma tüneteit mutató*" működés azzal jár, hogy számos ország gigantikus összegeket veszít az államkasszából.[56] Másrészt, a könnyen befolyásolható adóparadicsomok létezésükkel adó versenyt és zsarolási potenciált jelentenek a többi nemzetállammal szemben, így idővel ott is szükségszerűen elérhetővé válik az adócsökkentés és a dereguláció. Harmadrészt pedig a fejlesztési pénzek többszörösének elszivárgásán keresztül ellehetetlenítik a harmadik világ és az egyéb feltörekvő országok felzárkózását.[57] Cinikusan de annál keserűbben jegyzem meg, hogy talán ezen nem

[51] Pogátsa, 2022, i.m. 95. o.
[52] *The State of Tax Justice 2020*. https://taxjustice.net/reports/the-state-of-tax-justice-2020/ (2024.12.31.)
[53] *The State of Tax Justice 2023*. https://taxjustice.net/reports/the-state-of-tax-justice-2023/ (2024.12.31.)
[54] Zucman, Gabriel: *The Hidden Wealth of Nations: The Scourge of Tax Haven*. London, The University of Chicago Press, 2015. 103. o. https://doi.org/10.7208/chicago/9780226245560.001.0001
[55] Pogátsa, 2022, i.m. 24. o.
[56] Tóth Csaba Tibor: *Kiszámolták, mennyi adót kerülnek el a leggazdagabbak évente az adóparadicsomok segítségével* https://merce.hu/2020/11/29/kiszamoltak-mennyi-adot-kerulnek-el-a-leggazdagabbak-evente-az-adoparadicsomok-segitsegevel/ (2024.12.31.)
[57] *Facebook, Google and Microsoft 'avoiding $3bn in tax in poorer nations*. https://www.bbc.com/news/business-54691572 (2024.11.14)

is kívánnak olyan gyorsan változtatni, amióta a magas hozzáadott értékű munkán kívüli alantasabb főleg fizikai tevékenységeket (pl: a technológiai cikkekhez alapvető szükségű kobalt kibányászása vagy az Apple termékek összeszerelése) potom pénzért kiszervezték olyan harmadik világbéli országokba, ahol az EU-s munkavédelmi irányelvek, sőt még az egyéb alapvető tabuk, mint a gyermekmunka tilalma sem adott.[58]

3. A felhasználó, mint kiszolgáltatott termék

A technooptimisták azon kijelentésével szemben, hogy a technológiai fejlődés mindenkit felemel, Daron Acemoglu és Simon Johnson azzal érvel, hogy a „haladás soha nem automatikus. Korunk haladása is – ahogy történt ez az ipari forradalom kezdetén is, a vasútépítéssel vagy a Charles Dickens-i gyárkörülményekkel – egy szűk vállalkozói és befektetői csoportot gazdagít, miközben az emberek többsége hátrányos helyzetbe kerül, és alig profitál az újításokból.[59] Vegyük például azt, hogy a felhasználók tömege – azaz több mint az emberiség fele, – be van szorulva ezekbe a megkerülhetetlen és függőséget keltő terekbe, amely relációban a magáncégek javára erősen lejt a pálya. A hosszú és speciális jogi tudást igénylő felhasználási feltételek végig olvasására igen kevesen vállalkoznak, és még ha végig is olvassa valaki, a kattintások és adott oldalon eltöltött idő által létrehozott profiljának lekövetése, olyan bonyolult és valószínűleg titkosított algoritmusokkal történik, amelyek megismeréséhez magas szintű IT-tudás szükségeltetik. A viselkedési mintázatok kialakítása és a konkrét adatainak felhasználása a felhasználó szemszögéből nézve egy fekete dobozban zajlik[60], ahol nem tudja, hogy milyen módon kerül elé az adott videó és milyen folyamat során tolódik a másik hátra. Fontos újdonság, hogy a fekete doboz effektus mára már kiterjed a programozóira is. Polyák Gábor szerint az algoritmusok felett ténylegesen senki nem gyakorol kontrollt, mivel egy ponton túl, autonóm aktorrá válva, beprogramozásuk helyett, az öntanulási metódusaik alapján hozzák meg döntéseiket.[61]

Azt fontos hozzátenni, hogy a Google és a Facebook is profitorientált magancégek, egyéni szabályozásokkal, akik túlnyomórészt hirdetésekből szerzik a bevételüket.[62] De mennyi az elég és milyen áron? Üzleti politikájukban a képernyő előtt eltöltött idő és a kattintással adott jel az igazán fontos az algoritmus számára, mivel ezekből tud levonni értékes információkat. Szóval a kattintásaink és az adott oldalon eltöltött idő alapján óriási mennyiségű új tudást halmoznak fel rólunk,

[58] Katz–Lavigne, Sarah: *Cobalt Red: a regressive, deeply flawed account of Congo's mining industry*. https://www.opendemocracy.net/en/beyond-trafficking-and-slavery/cobalt-red-siddharth-kara-democratic-republic-congo-book-review/ (2024.11.11.)

[59] Acemoglu, Daron –Johnson, Simon: *Power and Progress: Our Thousand-Year Struggle over Tecnology and Prosperity*. New York, Public Affairs, 2023. 16. o.

[60] Pogátsa, 2022, i.m. 197.o.

[61] Polyák Gábor: *A digitális szolgáltatási koordinátor jogállása és jelentősége*. Előadás. Győr, 2024.10.25., Széchenyi István Egyetem, Új információs technológiák és jogállamiság Konferencia.

[62] Srnicek, Nick: *Platform capitalism*. Cambridge, Polity Press, 2017. 61. o.

mindezt azért, hogy hatékonyabban tudjanak eladni nekünk. A jövőnket jósolják meg különböző piaci szereplők és hirdetők hasznára, nem a miénkre."[63] Shoshana Zuboff helyzetjelentése 2018 óta nem veszített aktualitásából: „*a figyelem gazdaság korára még érvényes mondás volt, hogy ha valamilyen szolgáltatást ingyenesen veszünk igénybe, akkor mi vagyunk a termék. Ez, viszont mára már nem fedi le a teljes valóságot, mivel a felhasználók ebből az eleve kiszolgáltatott termék pozícióból mára egyszerű nyersanyaggá butultak le, melynek elsődeles szerepe, hogy a belőlük kinyert adatokat az algoritmusok jövőbeli magatartások előrejelzéséhez használják majd fel.*" [64] Jelenleg ott tartunk, hogy a valódi termékekké a felhasználók jövőbeli magatartásának előrejelzései váltak...

V. Záró gondolatok

Európa lemaradt a platformkészítésben és az MI versenyben is, így ő a szabályozási és rendeleti szinten igyekszik zászlóvivővé válni. A részbeni siker bizonyítéka az Általános adatvédelmi rendelet (GDPR), a platformok és felhasználók viszonyát érintő DSA, a piacszabályozó DMA és legfrissebben az Artificial intelligence Act (AI Act). A dolgozatomban megjelölt problémaköröket a jogalkotók észlelik ugyan de a felelősséget egyelőre erőtlenül áthárítják – önszabályozás, kockázatértékelés és kockázatcsökkentés keretében – a szabályozott jogalanyokra. Érthetően nem egyszerű a felállás, mivel a digitális érára fokozottan igaz a dinamikus változás, amit a jog maximum csak lekövetni próbálhat, valamint a platformcégek kapuőrei geopolitikai szempontok szerint gondolkodnak; hírhedtek arról, hogy kijátsszák a szabályozást, tesztelik az adatszuverenitás határait, és gyengítik, sőt olykor egyenesen aláássák a hatékony végrehajtást.[65]

Nehézség továbbá, hogy a szabályozás immanens része a korlátozás is, ami az innovációnak erősen és szükségszerűen gátat tud szabni. Ugyanakkor közel behozhatatlan hátrányt jelent azokkal szemben, akik szabadabb teret adnak. A már utópiának tűnő globális konszenzus mentén történő beavatkozás szükségessége e téren is kritikus. Mindenesetre e rendeletek sikeressége és gyakorlati megvalósulásának foka a szemünk előtt zajlik és fog még lezajlani.

[63] Zuboff, Shoshana: *The Age of Surveillance Capitalism: The Fight for a Human at the New Frontier of Power.* New York, Public Affairs, 2019. 16. o.

[64] Diósi Szabolcs – Barcsi Tamás: The legacy of disciplinary society – how relevant is Foucault's theory today?. *Évkönyv - Újvidéki egyetem magyar tannyelvű tanítóképző folyóirata 16*(1), 2021. 11-33. o. https://doi.org/10.18485/uns_evkonyv.2021.1

[65] Nieborg, David, et. al.: Introduction to the special issue on locating and theorising platform power. *Internet Policy Review 13*(2), 2024. 3-4.o. https://doi.org/10.14763/2024.2.1781