

DIGITÁLIS SZUVERENITÁS ÉS FEGYVERRÉ TETT KÖLCSÖNÖS FÜGGÉS A DIGITÁLIS PIACOKON, KÜLÖNÖS TEKINTETTEL A SZELLEMI ALKOTÁSOK JOGÁRA

Harkai István*

1. Bevezető: a digitális platformok, mint kétoldalú piacok globális kontextusban

Napjainkra a világgazdaság egyik legfontosabb szegmensét a digitális platformszolgáltatások adják. Ezek között olyan globális óriások alakultak ki, amelyek gazdasági, politikai, társadalmi hatásaikat tekintve megkerülhetetlen szereplőkké váltak. A kétoldalú digitális platformok globális térnyerését az Egyesült Államok technológiai cégei dominálták az elmúlt két évtizedben. Ezek közé a tengerentúli vállalatok közé tartozik a Google-Alphabet, az Amazon, a Facebook/Meta, az Apple és a Microsoft. E cégek óriási, monopol-jellegű piaci dominanciára tettek szert, kihasználva a relatíve alacsony piacra jutási költségekből eredő, illetve a hálózati hatásból fakadó előnyöket.¹ E cégek globális jelenléttel bírnak, azonban két legfőbb piacuknak kétségtelenül Észak-Ame-

* Adjunktus, Szegedi Tudományegyetem, Állam- és Jogtudományi Kar, Összehasonlító Jogi és Jogelméleti Intézet. ORCID: 0000-0003-1584-4196. A tanulmány elkészítését a Magyar Tudományos Akadémia Bolyai János Kutatási Ösztöndíja támogatta.

¹ A fent felsorolt cégek piaci kapitalizációja meghaladja a 15 trillió USD-t. Árbevételeik együttesen 2 trillió USD körül mozognak évente, miközben a globális mobil-operációsrendszerek piacán 99%, a keresőpiacon 90% a részesedésük, a felhőszolgáltatásoknak pedig 65%-át uralják. Ezen statisztikai adatok alátámasztásához ld. *Largest Companies by Marketcap*. <https://companiesmarketcap.com/>; *Top publicly traded tech companies by revenue*. <https://companiesmarketcap.com/tech/largest-tech-companies-by-revenue/>; *The 100 largest companies in the world by market capitalization in 2025*. <https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-capitalization/>. A platformgazdaság erőviszonyaihoz, a platformokat működtető gazdasági modellekhez és a szabályozási keretrendszer elemzéséhez részletesen ld. Valentini Pál: *Mennyire innovatívak a Big Tech vállalatok? Közgazdasági Szemle*, 2024. 22–56. <https://doi.org/10.18414/KSZ.2024.1.22>; Yanis Varoufakis: *Technofeudalism – What Killed Capitalism*. London, The Bodley Head, 2023.; Frank Pasquale: *The Black Box Society – The Secret Algorithms That Control Money and Information*. Cambridge (Massachusetts) – London. (England), Harvard University Press, 2016.; Fabio Bassan: *Digital Platforms and Global Law*. Cheltenham (UK) – Northampton (MA, USA), Edward Elgar, 2021.; Gary Madden – Russel Cooper (szerk.): *The Economics of Digital Markets*. Cheltenham (UK) – Northampton (MA, USA), Edward Elgar, 2009.

rika és Európa számítanak. Ugyan Európa a maga közel 500 milliós lakosságával és magas vásárlóerejével, valamint az amerikaihoz hasonló kulturális közegével valóban természetes felvevő piaca az amerikai – és immár egyre növekvő mértékben kínai – digitális szolgáltatásoknak, saját maga nem tudott még kidolgozni olyan komplex digitális platformszolgáltatásokat, mint a fent nevezett óriások.² Ez egyértelmű versenyhátrányt jelent Európának.³

Ugyan Európa nem rendelkezik saját, nagyméretű digitális platformszolgáltatással, ettől még nagyon is fontos szereplő, mégpedig a hálózati infrastruktúrák, adatközpontok és mindenekelőtt a jogi szabályozás tekintetében. Ez utóbira már csak azért is rendkívüli mértékben szüksége van, mert az uniós állampolgárok jelentős mértékben kiszolgáltatottá váltak a külső – mindenekelőtt amerikai és kínai – technológiai óriások piaci erejének. Sőt, nem csak piaci erejének, hanem geopolitikai és jogi befolyásolásának. Hogy ennek a jelenségnek ellent tartson, az Európai Unió hozzákezdett ahhoz, amihez kiválóan ért: a jogalkotáshoz. Vagyis ahhoz, hogy szabályozási eszközökkel, európai érdekek mentén próbálja meg korlátozni a nagy online platformok piaci hatalmát. Ezek közé a szabályozási területek közé tartozik többek között a versenyjogi eljárásokkal és ágazatspecifikus szabályokkal kapcsolatos normák megalkotása, adatvédelmi bírságok kiszabása. Az online szolgáltatások megregulázásának körébe tartozik a GDPR,⁴ a CDSM irányelv,⁵ a DMA,⁶ a DSA⁷ és az AI Act⁸ is.

² Dan Ciuriak: *The Digital Revolution Has Transformed Geopolitics – Seeing can no longer be equated with believing*. *CIGI*, July 19, 2023. <https://tinyurl.com/478ke2ra> Vö. The future of digital regulation between the EU and the US. *CADÉ*, 12 Mar 2025. <https://tinyurl.com/msyk3bts>

³ Mario Draghi: *The future of European competitiveness. Part A – A Competitiveness strategy for Europe, September 2024*. Luxembourg, Publications Office of the European Union, 2025. 23–38. <https://tinyurl.com/3z4387ew>; és Mario Draghi: *The future of European competitiveness. Part B – In-depth analysis and recommendations, September 2024*. Luxembourg, Publications Office of the European Union, 2025. 67–91. <https://tinyurl.com/2e62s2c6>

⁴ Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet), HL L 119., 2016.5.4., 1–88. o.

⁵ Az Európai Parlament és a Tanács (EU) 2019/790 irányelve (2019. április 17.) a digitális egységes piacon a szerzői és szomszédos jogokról, valamint a 96/9/EK és a 2001/29/EK irányelv módosításáról, (CDSM irányelv) HL L 130., 2019.5.17., 92–125. o.

⁶ Az Európai Parlament és a Tanács (EU) 2022/1925 rendelete (2022. szeptember 14.) a digitális ágazat vonatkozásában a versengő és tisztességes piacokról, valamint az (EU) 2019/1937 és az (EU) 2020/1828 irányelv módosításáról (digitális piacokról szóló jogszabály, DMA), HL L 265., 2022.10.12., 1–66. o.

⁷ Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (2022. október 19.) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (digitális szolgáltatásokról szóló rendelet, DSA) HL L 277., 2022.10.27., 1–102. o.

⁸ Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete (2024. június 13.) 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 (a mesterséges intelligenciáról szóló rendelet), HL L 2024/1689, 2024.7.12.

Mindezen jogszabályok összességét értelmezhetjük az Európai Unió digitális szuverenitási stratégiájának részeként is, aminek a célja, hogy a kontinens visszaszerezze és megőrizze az ellenőrzést a digitális tér felett. Enélkül ugyanis az amerikai és kínai cégek szabnák meg az online gazdaság és a digitális platformok működési feltételeit.

Kína mindeközben külön fejlődési pályát járt be a platformgazdaságban. A kínai állam elejétől fogva tudatosan korlátozta a nyugati versenytársak tevékenységét és jelenlétét a „*Nagy Tűzfal*” politikája révén, amivel párhuzamosan tevőlegesen támogatta a hazai technológiai óriások felemelkedését. Ennek eredménye egy sajátos digitális ökoszisztéma lett, olyan óriásokkal, mint az Alibaba, a Tencent, a Baidu és a TikTok, illetve annak anyavállalata, a ByteDance, amelyek védett, protekcionista környezetben tudtak megerősödni, majd kilépni a nemzetközi piacokra. Ezzel egy időben a vállalatok továbbra is erőteljes állami kontroll alatt állnak, amely komoly kérdéseket vet fel a digitális szuverenitás és annak érvényesíthetősége tekintetében.⁹

Napjainkra tehát kialakult egy hárompólusú (USA–EU–Kína) digitális gazdaság, amely geopolitikai szempontból sem elhanyagolható kérdéseket vet fel. Az innováció élén továbbra is az Egyesült Államok jár. Erre gyors ütemben zárkózik fel az állami kontroll alatt működő kínai technokapitalista modell. A két versenytárs mögött egyelőre lemaradva az EU igyekszik megteremteni a saját stratégiai autonómiáját a digitális platformágazatban. A legégetőbb kérdés ebben a szektorban nem pusztán gazdasági és versenyjogi aspektusokkal bír, hanem – ahogy arra fentebb már utaltam – komoly geopolitikai vonatkozásai is vannak. Mégpedig azért, mert ahol a piacokat néhány transznacionális vállalat kontrollálja, ott felmerül a kérdés: ki ellenőrzi valójában az adatokat, a kommunikációs csatornákat és az online diskurzus tereit? Az Egyesült Államok innovátorai¹⁰ sokáig a szabad és szabályozásoktól mentes internet hívei voltak. Kína ezzel szemben már igen korán a szuverén ellenőrzés modelljét építette fel. Európa pedig – ráébredve saját technológiai és innovációs lemaradására¹¹ – igyekszik olyan, a digitális platformgazdaságra és a digitális egységes piacra szabott normarendszert megalkotni, amely a közös értékeket (adattvédelem, szabad és tisztességes verseny) és Európa igényeit helyezi előtérbe. E három, alapjaiban eltérő törekvés érzékeny pontokon metszi egymást, amely természetes feszültséget generál. Transzatlanti feszültségek fakadnak például abból, hogy az EU technológiai szabályait az Egyesült Államok saját cégeit sújtó, protekcionista intézkedések sorozataként érzékeli, miközben az uniós jogalkotó a piacok tisztességes és versengő jellegét és a fogyasztók védelmét kezeli prioritásként.¹²

⁹ Ciuriak i. m.

¹⁰ Az Egyesült Államok története során végig elől járt az innovációban. Ennek összefoglalásához ld. Walter Isaacson: *Innovátorok. Hogyan indította el egy csapat hacker, zseni és geek a digitális forradalmat*. Budapest, HVG Könyvek, 2015.

¹¹ Érdemes ehelyütt röviden felidézni, hogy az iwiw nevű magyar közösségi weboldal lényegében a Facebook előfutárának is tekinthető. A felületet 2002-ben alapították, két évvel a Facebook előtt. Tevékenységét 2014-ig folytatta, amikor az oldal megszűnt. 2012 januárjában 4,7 millió felhasználóval rendelkezett. Az iwiw története egy azon innovációk közül, amelyek az ezredforduló Európájában jöttek létre, majd az amerikai versenytársak térhódításával elenyésztek.

¹² Ciuriak i. m.; vö. The future of digital regulation... i. m. <https://tinyurl.com/msyk3bts>

A tanulmány legfőbb célja annak a kérdésnek a megválaszolása, hogy az Európai Unió szabályozói eszköztára – különösen a DMA, a DSA és az AI Act – képesek lesznek-e jogi eszközökkel ellensúlyozni a technológiai és innovációs lemaradást a globális platformgazdaságban. A kutatás módszertana a klasszikus dogmatikai, doktrínális és összehasonlító jogi megközelítéseket ötvözi a nemzetközi kapcsolatok fogalomrendszeréből kölcsönvett „fegyverré tett kölcsönös függőség” (*weaponized interdependence*) elméletével. A vizsgálat során azt a hipotézist kívánom igazolni, hogy a szellemi alkotások joga és a digitális piacok szabályozása már nem csupán jogtechnikai kérdés, hanem az uniós „szabályozási hatalom” (*regulatory power*) olyan stratégiai eszközei, amelyek célja a digitális szuverenitás visszaszerzése és a globális hálózati fojtópontok (*chokepoints*) feletti – legalább regionális – kontroll kiépítése és fenntartása.

2. Digitális szuverenitás geopolitikai összehasonlításban

A digitális szuverenitás kérdése néhány éve került a geopolitikai eszmecserék homlokterébe. A megközelítés lényege annak vizsgálata, hogy az állam vagy politikai közösség képes-e önállóan szabályozni és kontrollálni a digitális infrastruktúráját, adatait és technológiai folyamatait, miközben korlátozza a saját joghatósági területén történő más állami vagy vállalati befolyásszerzést.¹³ Az Európai Unióban a digitális szuverenitás stratégiai törekvéssé vált. Az uniós jogalkotó igyekszik biztosítani az alapértékek és jogok – ideértve az adatvédelmet, a szabad és tisztességes versenyt és az alapjogok védelmét – a digitális korban és térben is maradéktalanul érvényesüljenek. Kiemelten fontos szempont továbbá az is, hogy az Európai Unió cselekvőképessége fennmaradjon, sőt erősödjön egy olyan globális térben, amelyet egyelőre döntő részben Európán kívüli hatalmak határoznak meg.¹⁴ Ez pedig lényegesen többet kíván, mint az adatvédelmi, versenyjogi, platformjogi és szellemi alkotásokra vonatkozó átfogó szabályok meghatározása. A végső cél az kell, hogy legyen, hogy Európa visszaszerezze és megerősítse az ellenőrzést a digitális infrastruktúrák, adatok és technológiai szabványok felett.¹⁵

¹³ Stephane Couture – Sophie Toupin: What does the notion of „sovereignty” mean when referring to the digital? *New Media & Society*, Vol. 21., No. 10. (2019) 2305–2319. <https://doi.org/10.1177/1461444819865984> Vö. Luciano Floridi: The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philosophy & Technology*, Vol. 33, N. 3. (2020) 369–378. <https://doi.org/10.1007/s13347-020-00423-6>; Julia Pohle – Thorsten Thiel: Digital sovereignty. *Internet Policy Review*, Vol. 9., Issue 4. (2020) 1–19. <https://doi.org/10.14763/2020.4.1532>; Frész Ferenc: Az Európai Unió digitális szuverenitásának illúziója – A GDPR és az amerikai Cloud Act, avagy az Európai Unió és az USA geopolitikai és gazdasági küzdelmének két központi eleme. *Cyber Threat Report*, 2025. júl. 31. <https://www.cyberthreat.report/p/az-europai-unio-digitalis-szuverenitasanak>

¹⁴ Az uniós törekvésekhez lásd különösen: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. 2030 Digital Compass: the European way for the Digital Decade. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021DC0118>.

¹⁵ A stratégia európai megjelenéséhez lásd különösen: Tambiama Madiega: Digital Sovereignty for Europe. EPRS Ideas Paper – Towards a more resilient EU. *EPRS Ideas Paper*, July 2020. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI\(2020\)651992_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf) Vö. Frész i. m.

A digitális szuverenitás és a platformok vonatkozásában markáns törésvonal bonthatkozik ki, illetve mélyül el az Egyesült Államok és az Európai Unió között. A konfliktus egyik első forrása a transzatlanti adatáramlás kérdése volt. A GDPR szigorú szabályokat határoz meg a személyes adatok EU-n kívülre irányuló továbbítása vonatkozásában, kivéve, ha a célország nem nyújt biztos, az uniós joggal megegyező szintű védelmet.¹⁶ Ezzel párhuzamosan az Egyesült Államok elfogadta a Cloud Act törvényt,¹⁷ amely kötelezi az amerikai joghatóság alá tartozó szolgáltatókat, hogy akár külföldön tárolt adatokat is adjanak át az amerikai hatóságoknak.¹⁸ A két jogszabály kollíziója szembetűnő: az uniós adatvédelmi elvek és az amerikai nemzetbiztonsági adatigények összeférhetetlennek tűnnek egymással, egyszerre nem teljesíthetők maradéktalanul.¹⁹ Ez a konfliktus kiviláglik az ún. *Schrems I-II* ügyekből²⁰ is, amelyek érvénytelenítették a korábbi EU–USA adatcsere keretrendszereket (Safe Harbor, illetve Privacy Shield). Az Európai Unió Bírósága (a továbbiakban: EUB) ugyanis kimondta, hogy az amerikai megfigyelési törvények (pl. FISA 702)²¹ túlzott mértékben avatkoznak be az európai polgárok magánszférájába, és nem biztosítanak megfelelő jogorvoslatot, így az Egyesült Államok nem tekinthető „megfelelő védelmet nyújtó” országnak.²² Az ítéletek következménye az lett, hogy az Európai Unió és az Egyesült Államok között

¹⁶ Ld. a GDPR 44–50. cikkei, a személyes adatok harmadik országokba vagy nemzetközi szervezetek részére történő továbbítása vonatkozásában.

¹⁷ Clarifying Lawful Overseas Use of Data Act (CLOUD Act), Pub. L. No. 115-141, Div. V, 132 Stat. 1213-25 (2018).

¹⁸ 2713 §. Required preservation and disclosure of communications and records.

¹⁹ A GDPR és a Cloud Act kollíziójához lásd: Initial legal assessment of the impact of the US Cloud Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence. Vö. Paul Schwartz – Karl-Nikolaus Peifer: Data Localization Under the CLOUD Act and the GDPR. *Computer Law Review International – A Journal of Information Law and Technology*, 1/2019. 1–10. <https://doi.org/10.9785/cr-2019-200102>; Peter Swire: When does GDPR Act as a Blocking Statute: The Relevance of a Lawful Basis for Transfer. *Cross-Border Data Forum*, November 4, 2019. <https://doi.org/10.2139/ssrn.3473187>

²⁰ A Schrems I. és II. ügyekben az EUB megsemmisítette az EU–USA adattovábbításra vonatkozó keretrendszereket (*safe harbor*, illetve *privacy shield*). Ennek indoka az volt, hogy az amerikai nemzetbiztonsági szervek tömeges és aránytalan adathozzáférése sértette az uniós alapjogokat. Az EUB ezen felül az adatkezelőket a célország tényleges védelmi szintjének eseti vizsgálatára kötelezte. Ld. C-362/14. Maximilian Schrems vs. Data Protection Commissioner és Digital Rights Ireland Ltd. ECLI:EU:C:2015:650; C-311/18. Data Protection Commissioner vs. Facebook Ireland Ltd, Maximilian Schrems. ECLI:EU:C:2020:559.

²¹ Az EUB a Schrems II. ügyben a tömeges megfigyeléseket lehetővé tevő amerikai jogszabályok közül a külföldi hírszerzésről szóló törvény 702. szakaszát külön is kiemelte (*Foreign Intelligence Surveillance Act – FISA 702*), valamint a 12333. számú elnöki rendeletet (*Executive Order 12333*) is nevesítette. Ezek a jogszabályok egyedi bírósági engedély és bűncselekmény megalapozott gyanúja nélkül lehetővé teszik az amerikai hírszerző szervek részére a külföldi, nem amerikai állampolgárok elektronikus kommunikációs adataihoz való tömeges hozzáférést. Ld. Schrems II. ügy, 178–185. pontok.

²² A tömeges adathozzáférés aránytalanságát az EUB már a Schrems I. ügy 94. pontjában kimondta, hogy az ilyen gyakorlat sérti az Európai Unió Alapjogi Charta 7. cikkében foglalt magánélet tisztelgetben tartásához fűződő jogot. A Schrems II. ügy 180–184. pontjaiban az EUB pedig azt mondta ki, hogy a FISA 702. szakasza nem tartalmaz megfelelő korlátozásokat és garanciákat a nem amerikai állampolgárokkal szemben. Ezen túlmenően az ítélet 192. pontja lefektette, hogy az amerikai jog nem biztosít az Alapjogi

állandósult az adatáramlás jogi alapjait illető bizonytalanság, amelyet ideiglenes megoldásokkal²³ próbáltak meg orvosolni.

A digitális szuverenitás kérdéséhez nem csak az adatáramlás, hanem az adatlokalizáció kérdése is szorosan kapcsolódik. Az adatlokalizáció olyan jogszabályi vagy politikai követelmény, amely előírja, hogy egy adott ország polgárai, illetve üzemeletői által generált adatokat fizikailag is az adott ország területén lévő szervereken kell tárolni és kezelni.²⁴ Ami e tekintetben Kínát illeti, a távolkeleti nagyhatalom a kiberbiztonság és adatbiztonság, valamint az adatlokalizáció vonatkozásában szigorú előírásokat alkalmaz, különös tekintettel a személyes és a kritikus adatokra. Ennek fényében nem meglepő, hogy a külföldi felhőszolgáltatók csak kínai partnerrel – például 21Vianet – együttműködve végezhetik tevékenységüket. Nemzetbiztonsági okokra hivatkozva a hatóságok pedig bármikor hozzáférhetnek a belföldön tárolt adatokhoz, miközben bizonyos adatokat – például az állampolgárok személyes adatait – tilos külföldre továbbítani. Ezzel párhuzamosan a kínai kormányzat a külföldön tárolt adatokat nemzetbiztonsági kockázatnak tekinti. A határokon átnyúló digitális szolgáltatást nyújtó kínai techcégek esetében ezzel éppen ellentétes aggályok merültek fel. Számos nyugati ország joggal tart attól, hogy felhasználói adatok kerülhetnek a kínai kormány kezébe, mivel ezek a cégek mélyen integrálódtak a kínai állami gépezetbe, kiszolgálva a kormányzati adatigényeket.²⁵

Kínához képest az Európai Unió az adatlokalizáció és a szabad adatáramlás vonatkozásában alapvetően megengedőbb volt, amennyiben az adatvédelem magas szintje biztosítva volt. Az utóbbi időben azonban az EU-ban is teret nyertek az olyan vélemények, amelyek szerint egyes érzékeny adatkategóriák esetén (például kormányzati adatok, egészségügyi adatok) ki kell építeni az európai adattárolás és feldolgozás kereteit, infrastruktúráját. Ennek a megváltozó vélekedésnek lett a gyümölcse az EU *Gaia-X*

Charta 47. cikkének megfelelő, bíróság előtt érvényesíthető jogorvoslati jogot az uniós polgárok számára az USA hírszerző szervezeteivel szemben.

²³ A megoldást az amerikai és európai döntéshozók a harmadik adattovábbítási keretrendszer (*EU-US Data Privacy Framework*) kialakításában találták meg. Az Európai Bizottság által elfogadott határozat (A Bizottság 2023/1795 végrehajtási határozata az (EU) 2016/679 európai parlamenti és tanácsi rendelet szerint a személyes adatoknak az EU-USA adatvédelmi keret által biztosított megfelelő szintű védelméről) jogalapját a Joe Biden elnök által kiadott 14086. számú elnöki rendelet teremtette meg (*Executive Order 14086*), amely a korábbi EUB ítéletek kritikáira reagálva bevezette a szükségesség és arányosság elvét az amerikai hírszerzési gyakorlatba, és létre hozott egy új jogorvoslati fórumot is (*Data Protection Review Court*). Ez a megoldás is ugyanakkor úgy tűnik, hogy csak ideiglenes, mert a megfigyeléseket lehetővé tevő amerikai törvények érdemben továbbra sem változtak.

²⁴ Az adatlokalizáció követelményének részletszabályaihoz lásd a nem személyes adatok Európai Unióban való szabad áramlásának keretéről szóló, 2018. november 14-i (EU) 2018/1807 európai parlamenti és tanácsi rendelet 3. cikk 5. pontját.

²⁵ A kínai adatszuverenitási rendszert a következő három jogszabály határozza meg: *Cybersecurity Law of the People's Republic of China*, *Data Security law of the People's Republic of China* és *Personal Information Protection Law of the People's Republic of China*. E jogszabályokban meghatározott adatlokalizációs előírások érvényesüléséhez és a külföldi felhőszolgáltatásokra kényszerített helyi partnerségekre ld. Lizhi Liu: *The Rise of Data Politics: Digital China and the World. Studies in Comparative International Development*, Vol. 56. (2021) 55–58. <https://doi.org/10.1007/s12116-021-09319-8>

kezdeményezése,²⁶ amely célul tűzte ki az európai felhőinfrastruktúra megteremtését, csökkentve ezáltal az amerikai függésnek való kitettséget. Erre reagálva az amerikai szolgáltatók ún. *szuverén felhőmegoldásokat* kezdtek kínálni az európai ügyfeleknek. A Google és az Amazon például európai adatközpontokat is nyitott.²⁷ Az adatok fizikai elhelyezkedése azonban nem jelent automatikusan adatszuverenitást, mert az amerikai Cloud Act hatálya alól nem mentesít az adatok tárolási helye, ezért egy amerikai cég egy európai adatközpontból is továbbíthat adatot az Atlanti-óceán túlsó partjára, amennyiben ennek a törvényi feltételei fennállnak.²⁸ Vagyis a teljes adatszuverenitás és technológiai autonómia eléréséhez nem elég az európai adattárolási infrastruktúra megteremtése, hanem technológiai-intézményi-jogi lépések kellenek. Ebből következő, hogy Európának szüksége van európai tulajdonú felhőszolgáltatásokra, titkosítási megoldásokra, saját fűlvezetőgyártó-kapacitás kiépítésére.²⁹

Az európai törekvések globális kontextusban értelmezendők. Minden nagyhatalom megpróbálja érvényre juttatni saját szuverenitási igényeit a digitális, online térben. Az Egyesült Államok, amely a digitalizáció és az internet fejlődésének élharcosa volt, lázasan igyekszik megőrizni technológiai vezető szerepét, amelyben olyan eszközöket is felhasznál, mint az extraterritoriális jogérvényesítés és egyfajta jogi norma-export.³⁰ Kína és Oroszország ugyancsak a szuverén kibertér koncepcióját kívánja

²⁶ GAIA-X: Driver of digital innovation in Europe. Featuring the next generation of data infrastructure. Vö. Simona Autolitano – Agnieszka Pawlowska: Europe's Quest for Digital Sovereignty: GAIA-X as a Case Study. *Instituto Affari Internazionali Papers*, Vol. 21., N. 14. (2021); Andreas Baur: European ambitions captured by American clouds: digital sovereignty through Gaia-X? *Information, Communication & Society*, Vol. 29., No. 2. (2026) 417–434. <https://doi.org/10.1080/1369118X.2025.2516545>

²⁷ Advancing digital sovereignty on Europe's terms; AWS Digital Sovereignty Pledge: Control without compromise.

²⁸ A Cloud Act 2713. §-a lefekteti az adatszolgáltatási kötelezettség extraterritoriális hatályát, kimondva, hogy az elektronikus hírközlési szolgáltató köteles eleget tenni az adatszolgáltatási kötelezettségeinek a birtokában, őrzetében vagy ellenőrzése alatt álló (*possession, custody, or control*) adatok tekintetében, függetlenül attól, hogy az adott kommunikáció, rekord vagy egyéb információ az Egyesült Államokon belül vagy kívül helyezkedik-e el. Vagyis a szimpla európai adatlokalizáció nem mentesít az amerikai joghatóság alól, ha az amerikai szolgáltató technológiai vagy jogi hozzáférési képessége fennmarad. Ez kiválóan megvilágítja azt stratégiát is, ami szerint az amerikai felhőszolgáltatók az európai partnerekkel (pl. T-Systems) együttműködve szuverén felhőszolgáltatásokat kínálnak. Ha a titkosítási kulcsok feletti rendelkezés kizárólag az európai partnernél maradna, az amerikai anyagcég elveszthetné az adatok feletti tényleges ellenőrzési kontrollt, mentesülve ezáltal a Cloud Act szerinti adatszolgáltatási kötelezettség alól. Vö. Schwartz–Peifer i. m. 1–5.

²⁹ A technológiai autonómia hiányából fakadó európai kitettség orvoslását célozza az Európai Parlament 2026. január 22-i állásfoglalása az európai technológiai szuverenitásról és a digitális infrastruktúráról [2025/2007(INI) – *European technological sovereignty and digital infrastructure*]. A saját európai fűlvezetőgyártó-kapacitás stratégiai megteremtésének jogszabályi háttéréhez pedig lásd az Európai fűlvezető-ökoszisztémájának megerősítését célzó intézkedési keret létrehozásáról és a 2021/694 rendelet módosításáról szóló, 2023. szeptember 13-i (EU) 2023/1781 európai parlamenti és tanácsi rendeletet (csiprendelet), amely a fűlvezetők gyártásában 20%-os európai részesedés elérését tűzte célul 2030-ig. Vö. Frész i. m.

³⁰ A témához lásd különösen: Harkai István: Régi klisék új köntösben? Territorialitás és jogi földrajz a szerzői jogban, különös tekintettel a határtalan internetre. *Iustum Aequum Salutare*, 2023/3. 109–142.; István Harkai–Péter Mezei: Recalibrating Territoriality in Platform End-User License Agreements. In:

megvalósítani. Ami tehát az analóg, több pólusú világban polarizáció címszó alatt zajlik, az megfigyelhető az online térben is. Az online és offline tér pedig kölcsönhatásban áll egymással, mert az analóg, offline stratégiai döntések fókuszában és hátterében is egy-szerre állnak adatok és a digitális kontroll kérdései.³¹

Ezt a fentebb említett jelenséget „*techno-nacionalizmusnak*” is nevezhetjük, amely fogalom arra utal, hogy az államok a technológiai- és adatfölény megszerzését kulcsfontosságú nemzetbiztonsági és gazdasági-jóléti kérdésnek tekintik.³² Ez a gondolkodásmód az globális internetes infrastruktúra és elérés széttöredezéséhez vezethet („*splinternet*”), ahol az egyes régiók, geopolitikai blokkok saját jogszabályi keretrendszerük logikája mentén próbálják meg a világhálót és az azon folyó digitális, online tevékenységeket szervezni. Vagyis a multipoláris világrend globális szembenállása leképeződni látszik a digitális, online térben is, amely kihívás elé állítja nem csak a nemzetállami, hanem a nemzetközi jogalkotókat is.³³

3. Az adat, mint vagyoni értékű jog

A digitális platformok korában az adat a világgazdaság egyik legfontosabb erőforrásává vált. A modern gazdaságok működését immár nem csak a rendelkezésre álló, kibányászható nyersanyagok, ritkaföldfémek, a mezőgazdasági termőterületek nagysága, a hozzáférhető tengeri erőforrások, a humántőke és infrastruktúra határozzák meg, hanem az a mérhetetlen mennyiségű adattömeg, amely a digitális, online platformokon és olyan eszközökön keletkezik, amelyek egymással és az internettel is összeköttetésben állnak. A hagyományos erőforrásokhoz képest az adatok jogi státusza, illetve annak körvonalai kevésbé jól meghatározottak. A hagyományos, kontinentális polgári jogi dogmatika nehezen tudja az adatot a meglévő keretrendszerbe illeszteni. Az adat ugyanis nem dolog. Nem bír fizikai léttel, legfeljebb csak az adathordozó, amire rögzítik, bár ez, a felhőszolgáltatások világában, szintén egyre távolabb esik a hagyományos

Dusan Popovic – Rainer Kulms (szerk.): *Repositioning Platforms in Digital Market Law*. Cham, Springer Nature Switzerland, 2024. 55–81. https://doi.org/10.1007/978-3-031-69678-7_3

³¹ Oroszország és Kína álláspontjához részletesen ld. Nyáry Gábor: Az adatok geopolitikája: az Internet mitikus szabadságától a digitális szuverenitás felé. *Cyberblog*, 2020.12.07. <https://tinyurl.com/ypkb39uw>; Nyáry Gábor: Kiberdiplomácia: hatalom, politika és technológia a geopolitika ötödik dimenziójában. In: Molnár Anna – Molnár Dóra (szerk.): *Kiberdiplomácia*. Budapest, Ludovika, 2022. 27–53.; Molnár Dóra: *Nagyhatalmi kiberdiplomácia – az Egyesült Államok, Kína és Oroszország a nemzetközi kiberporondon*. In: Molnár–Molnár (szerk.) i. m. 73–92.; Julien Nocetti: *A Splintered Internet? Internet Fragmentation and the Strategies of China, Russia, India and the European Union*. IFRI Studies – Geopolitics of Technology Center, 2024. 6–32.

³² A techno- és innovációs nacionalizmus kérdésköréhez lásd különösen: Sapna Kumar: Innovation Nationalism. *Connecticut Law Review*, Vol. 51., No. 2. (2019) 205–246.; Nyáry i. m.; Jing Li – Daniel M. Shapiro – Anastasia Ufimtseva – Peng Zhang: Techno-nationalism and cross-border acquisition in an age of geopolitical rivalry. *Journal of International Business Studies*, Vol. 55. (2024) 1190–1203. <https://doi.org/10.1057/s41267-024-00721-7>; Yadong Luo: Illusion of techno-nationalism. *Journal of International Business Studies*, Vol. 53. (2022) 550–567. <https://doi.org/10.1057/s41267-021-00468-5>

³³ Liu i. m. 47–56.

magánjogi felfogástól.³⁴ Az adat továbbá nem része a szellemi alkotások jogának sem, nem lehet szellemi terméknek tekinteni, legalábbis nem közvetlen módon. Ettől persze igaz, hogy a digitális adatok maguk rejthetnek szellemi – első sorban szerzői és kapcsolódó jogi oltalom alatt álló – alkotásokat, illetve az adatbázis maga *sui generis* és szerzői jogi oltalom alatt állhat.³⁵ Vagyis közvetett módon lehet szó az adatok, illetve azok előállítása, összeállítása, tárolása tekintetében különféle jogszabályi oltalmi formákról, azonban ezen túlmenően is fontos lenne végre megnyugtatóan tisztázni, hogy maga az adat, mint digitális vagyoni eszköz, lehet-e a hagyományos értelemben vett tulajdonjog tárgya,³⁶ kezelhető-e vagyoni értékű jogként?

A magyar jogrendszerben a vagyoni értékű jog hagyományosan olyan – akár – forgalomképes, pénzben kifejezhető, értékkel bíró jogot jelent, amely nem kapcsolódik konkrét dologhoz, de önállóan átruházható vagy felhasználására, használatára illetve hasznosítására engedély adható. Ilyen lehet például a szellemi alkotás (szerzői mű, kapcsolódó jogi teljesítmény, védjegy, szabadalom), a földhasználati jog, vagy a haszonélvezeti jog. A kérdés tehát adja magát: tekinthetjük-e az adatokat vagyoni értékű, tulajdoni jellegű jognak, amely átruházható? A jelenlegi európai és magyar magánjogi gondolkodás a személyes adatot nem tekinti ilyen vagyoni értékű jognak, hanem az adott természetes személy információs önrendelkezési joga részeként gondol rá.³⁷ Ezzel szemben az angolszász megközelítésben felmerült olyan érv, miszerint az online

³⁴ Az adat, mint vagyoni értékkel bíró elem és a polgári jogi dolog fogalom dogmatikai bászorolásának problémájához, illetve a kontinentális dologi jogi fogalmi keretekhez részletesen ld. Parti Tamás: *A digitális adatok tulajdoni adaptációja, a digitális javak vagyoni jogi kölcsönhatásainak tükrében*. PhD értekezés. Károli Gáspár Református Egyetem, 2023. 192–234. https://real-phd.mtak.hu/1873/1/Parti_Tamas_Disszertacio_watermark.pdf Az adatokkal kapcsolatos szerződések típusairól részletesen ld. Neil Cohen – Christiane Wendehorst: *ALI-ELI Principles for a Data Economy – Data Transactions and Data Rights*. American Law Institute and the European Law Institute, ELI Final Council Draft, 2021. 48–124. <https://tinyurl.com/ycxfztzy>

³⁵ Parti i. m. 165–175. Emellett pedig érdemes megemlíteni, hogy az adatok adatbázis formájában szellemi oltalom tárgyát képezik, méghozzá kétféle módon. Az egyik a *sui generis* oltalom, amely az adatbázis előállításába történő befektetést védi, a másik pedig az adatbázisok szerzői, gyűjteményes műként történő oltalmazása, amennyiben az adatok összegyűjtése és még inkább elrendezése egyéni, eredeti jellegű alkotói tevékenység eredménye. Ennek részletszabályaihoz lásd: az adatbázisok jogi védelméről szóló, 1996. március 11-i 96/9/EK európai parlamenti és tanácsi irányelv 3–6. cikk, illetve a *sui generis* védelmet garantáló 7. cikk.

³⁶ A magánjogi dogmatika történetében nem az adat és a digitális javak az első olyan kategória, amely a dolog fogalmának és a tulajdonjog koncepciójának újra gondolását teszi szükségessé. A Polgári Törvénykönyvről szóló 2013. évi V. törvény 5:14. § (2) bekezdése kimondja, hogy a dologra vonatkozó szabályokat megfelelően alkalmazni kell a pénzre és az értékpapírokra, valamint a dolog módjára hasznosítható természeti erőkre. Ez a pont nyilvánvalóan nem vonatkoztatható az adataira. A jogalkotó ezzel a megfogalmazással az olyan erőforrásokat kívánta meg analógia útján a dolgok fogalmi körébe vonni, mint például a villamos áram, amelynek dologként való elfogadása az erőforrás eladhatóságát, illetve az áramlopás büntethetőségét volt hivatott biztosítani. Ez a törekvés a XIX-XX. század fordulóján igen hasonló, az adatok, digitális javak jogi értékelésével kapcsolatos vitákat generált a jogtudományban. Ld. Parti i. m. 208.

³⁷ Axel Metzger – Zohar Efroni – Lena Mischau – Jakob Metzger: *Data-Related Aspects of the Digital Content Directive*. *JIPITEC*, Vol. 9. (2018) 93–94.; Parti Tamás: *Adat – érték – vagyon – tulajdon relációk*. *Gazdaság és Jog*, 2022/9–10. 55–58.; Parti i. m. 43–86.

gazdaság fogyasztóit vagyoni jellegű jogok illetik meg saját személyes adataik felett, amelynek hasznosításáért egyfajta osztalék kellene, hogy megillesse őket.³⁸ Az adatnak ugyanakkor van egy olyan sajátossága, hogy egyszerre többen is birtokolhatják, lemásolhatják, miközben az adatok létrejötte és értéke maga is nagyban függ a felhasználás kontextusától.³⁹

Másfelől közelítve az adat afféle „közjóság”, amely felfogás maga után vonja az igényt arra, hogy az adatot bárki szabadon felhasználhassa. Ennek az álláspontnak a támogatói úgy vélik, hogy az adatok tulajdoni-jellegű jogosultságokkal való felruházása túl merevvé és lassúvá tenné az adatok felhasználhatóságát, amely pedig fékezne az innovációt. Ebből pedig következik, hogy az az entitás, amely túl szigorú adatvédelmi jogi konstrukciókat állít fel, lemarad az egyre gyorsuló globális versenyben. Ezért aztán az adatok felhasználására vonatkozó gyakorlat inkább egy köztes megoldás felé mozdult el. Eszerint az adatok felett bizonyos felügyeleti és hasznosítási jogokat kell biztosítani az érintetteknek. Európában a GDPR erős felügyeleti keretet ad a felhasználáshoz való hozzájárulás, a hozzáférés és a törlés joga tekintetében.⁴⁰ Emellett pedig a szintén uniós Data Act⁴¹ például a gépjárművek vagy okoseszközök által generált adatokhoz kapcsolódóan lehetővé tenné az eszköz használója számára, hogy a személyes adatnak egyébként nem minősülő információkhoz hozzáférjen, illetve azokat hasznosítsa. Ez a megközelítés közelebb áll egy kvázi vagyoni jogi jellegű kontrollhoz az adatok felett.⁴²

Parti Tamás a digitális adatok feletti tulajdonjog kialakulásának lehetőségeivel kapcsolatban rámutat arra, hogy Magyarországon már ma is léteznek olyan jogintézmények, amelyek valamilyen formában védik az adatokhoz, és azok felhasználásához fűződő felhasználói érdekeket. Ilyenek például a személyes adatok védelme, az adatbázisokra vonatkozó szerzői és *sui generis* oltalom, az üzleti titok védelme, illetve

³⁸ Az angolszász jogrendszerekben, mindenekelőtt az Egyesült Államokban a személyes feletti tulajdonjog (*property*) elismerése, illetve a technológiai vállalatok bevételeiből való, végfelhasználóknak, fogyasztóknak fizetendő adatosztalék (*data dividend*) kérdése az elmúlt évek egyik meghatározó vitatémája volt. Ezzel kapcsolatban ld. különösen: Steven H. Hazel: Personal Data as Property. *Syracuse Law Review*, Vol. 70., No. 4. (2020) 1056–1113. <https://doi.org/10.2139/ssrn.3669268> Egy másik megközelítés felveti, hogy az adatot a munka eredményének tekintsük. Ld. Imanol Arrieta-Ibarra – Leonard Goff – Diego Jiménez-Hernández – Jaron Lanier – E. Glen Weyl: Should We Treat Data as Labor? Moving Beyond „Free”. *AEA Papers and Proceedings*, Vol. 108. (2018) 38–42. <https://doi.org/10.1257/pandp.20181003>

³⁹ Parti i. m. 74. és 79.

⁴⁰ A szóban forgó kvázi felügyeleti jogokhoz ld. GDPR 6–7. cikk (az adatkezelés jogszerűsége és a hozzájárulás feltételei), 15. cikk (az érintett hozzáférési joga), 17. cikk (törléshez való jog). Vö. Alek Tarkowski – Francesco Vogelegang: The argument against property rights in data. Ensuring access to data though non-exclusive access rights. *Open Future Policy Brief*, #1., 2021. <https://tinyurl.com/mrtye29>

⁴¹ Az Európai Parlament és a Tanács (EU) 2023/2854 rendelete (2023. december 13.) a méltányos adathozzáférésre és -felhasználásra vonatkozó harmonizált szabályokról, valamint az (EU) 2017/2394 rendelet és az (EU) 2020/1828 irányelv módosításáról (adatrendelet), HL L, 2023/2854, 2023.12.22.

⁴² Az Adatrendelet és az adatokhoz fűződő vagyoni érdekek metszéspontjaihoz ld. Martina Eckardt – Wolfgang Kerber: Property rights theory, bundles of rights on IoT data, and the EU Data Act. *European Journal of Law and Economics*, Vol. 57., N. 1. (2024) 113–143. <https://doi.org/10.1007/s10657-023-09791-8>

olyan büntető törvényi tényállások, amelyek a személyes adatok tiltott megszerzésével és jogellenes felhasználásával kapcsolatosak.⁴³ Ennek ellenére Magyarországon sincs egyelőre olyan jogszabályi konstrukció, amely az adatok birtokosai számára valamiféle tulajdoni jellegű konstrukciót hozna létre. Parti szerint ez részben azzal magyarázható, hogy az adatok nem úgy működnek, mint a hagyományos tulajdon, vagy akár a szellemi tulajdon oltalmi tárgyai. A digitális adatok nagy mennyiségben előállíthatók, más adatokkal kombinálhatók és újrahasznosíthatók. A bennük rejlő információ értéke kumulatív és kontextusfüggő.⁴⁴ Az adat keletkezése gyakran egy összetett folyamat eredménye, ezért felmerül a lehetősége annak is, hogy az adatok – a *creative commons*-hoz hasonlóan⁴⁵ – egyfajta *data commons* erőforrásként kerülnek hasznosításra, ami megosztási kötelezettséget von maga után a digitális platformok részéről, amely pedig az adatokból származó piaci monopolhelyzet elkerülését segíthetné elő.

A személyes adatok forgalomképes vagyonelemmé válása ezen túlmenően a digitális magánszféra egyébként is bomladozó egységét bonthatná meg, mert a piaci logika egyszerűen felülírná az emberi méltóság és az önrendelkezéshez való jog logikája által diktált hasznosítási formákat és a pusztá nyereséget helyezni előtérbe.⁴⁶ Emellett komoly hatást gyakorolhatna az innovációra és a versenyre, ha az adatok mozgását és felhasználását túl szigorú, tulajdoni jellegű szabályokhoz kötnénk. Ne felejtjük ugyanis, hogy mind a hagyományos tulajdonjogi konstrukció, mind pedig a szellemi tulajdon abszolút szerkezetű és negatív tartalmú jogviszonyt keletkeztet, ahol a tulajdonjog átszállása, illetve a szellemi termék felhasználása szigorú szerződéses keretek között történhet. A digitalizáció és az online platformok térhódítása pedig már régen megmutatta, hogy a szellemi alkotások online felhasználásának jogosítása meglehetősen nehézkesen működik az online térben. Az is evidens ugyanakkor, hogy a túl laza, vagy éppen egyáltalán nem létező szabályrendszer miatt a személyes és személyhez nem kapcsolódó digitális adatok szabad prédává tétele ugyancsak sértheti a jogbiztonságot.

Erre tekintettel az EU az arany középút kialakítására törekedve az *adatközösségek* (*data altruism*) kialakítását igyekszik elősegíteni, ami egyfajta *fair use*-jellegű adatfelhasználást tenne lehetővé.⁴⁷ Ez biztosítaná az adatok széles körben történő felhasznál-

⁴³ Parti (2022) i. m. 58–60.

⁴⁴ Parti (2022) i. m. 56–58.; vö. Liu i. m. 47–48.

⁴⁵ A *Creative Commons* (CC) egy globálisan elterjedt nyílt licenclési rendszer, amelyek a hagyományos, szigorú szabályokon alapuló szerzői jogi felhasználási és engedélyezési keretekhez képest rugalmasabb, standardizált felhasználási feltételeket tesznek lehetővé. A *data commons* kifejezés ennek szinonimája, amely leginkább *adat-közjószágként* értelmezhető. A megközelítés célja, hogy a digitális platformok által felhalmozott adatok ne maradjanak az adott technológiai vállalat kizárólagos hatókörében, hanem a megfelelő adatvédelmi garanciák biztosítása mellett közös erőforrásként váljanak hozzáférhetővé és hasznosíthatóvá a társadalom, a kutatók és a kisebb piaci szereplők számára, az innováció és a kutatás elősegítése céljából.

⁴⁶ Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content. 7. Vö. Metzger et al. i. m. 93.

⁴⁷ Az adataltruizmus fogalmát az Európai Parlament és a Tanács 2022/868 rendelete az európai adatkormányzásról és a 2018/1724 rendelet módosításáról (adatkormányzási rendelet) vezette be. A fogalom alatt olyan önkéntes adatmegosztást ért, amely az érintetteknek a rájuk vonatkozó személyes adatok kezeléséhez való hozzájárulásán, vagy az adatbirtokosoknak a nem személyes adataik felhasználására

nálhatóságát, miközben garanciákat biztosítana az adatok eredeti gazdáinak. Az adat nem válna tulajdonjog tárgyává, de a technológiai óriások sem tudnák azt kizárólagos jelleggel és legfőképpen ingyenesen saját céljaikra felhasználni. Az arany középút egyfajta közérdekű felhasználás lenne, amelynek a fő kedvezményezettje a kutatás és innováció lenne.⁴⁸ A végső cél tehát az adatok tekintetében egy olyan egyensúlyi állapot megtalálása lenne, amelyben az adatok eredeti gazdái is részesülnének az adatvagyon értékéből, miközben nem akadályoznánk az innováció előrehaladását.

4. A szerzői jog és tartalommoderáció, geopolitikai kontextusban

A számítástechnika, a digitalizáció és még inkább az internet megjelenése fenekestől forgatta fel a szerzői és kapcsolódó jogi értékláncokat.⁴⁹ A közvetítő szolgáltató online platformok felfoghatatlan mennyiségű, szerzői és kapcsolódó jogi oltalom alatt álló művet és teljesítményt tesznek a nyilvánosság számára hozzáférhetővé. Hogy védjék a platformok üzleti modelljeit, és kimentsék őket a végfelhasználók által elkövetett, tömeges méretű jogsértésekből fakadó felelősség alól, mind az amerikai, mind pedig az európai jogalkotó létrehozta az ún. *védett kikötő* (*safe harbor*) intézményét. Ennek lényege, hogy amennyiben a platform üzemeltetője felállít egy értesítési és eltávolítási mechanizmust, amelyen keresztül a jogosultak a tudomására tudják hozni, ha jogsértő tartalom kerül a platform tárhelyére, amelyet ezt követően azonnal eltávolít, úgy mentesülnek a jogsértésből származó negatív következmények alól. Az Egyesült Államokban ezt az intézményt a DMCA⁵⁰ vezette be.⁵¹ Európában pedig egy több lépcsős, immár több mint két évtizede zajló jogalkotási folyamat eredményeként került sor az

vonatkozó engedélyén alapul, anélkül, hogy ezért olyan díjat számítának fel vagy kapnának, amely meghaladja az adataiknak közérdekű célokra való rendelkezésre bocsátása esetén felmerült költségeik ellentételezését. Adatkormányzási rendelet, 2. cikk 16. pont. Vö. Corina Kruesz – Felix Zopf: The Concept of Data Altruism of the draft DGA and the GDPR: Inconsistencies and Why a Regulatory Sandbox Model May Facilitate Data Sharing in the EU. *Data Protection Law Review (EDPL)*, Vol. 7., No. 4. (2021) 569–571. <https://doi.org/10.21552/edpl/2021/4/13>

⁴⁸ Az adatok árúként, illetve a magántulajdon tárgyaként (*data-as-commodity*) történő kezeléséhez, illetve ennek kritikai értékeléséhez, valamint a technológiai óriások adatmonopóliumának letöréséhez, a kutatás, az innováció és a közérdeket szolgáló adatközösségek (*public adat commons*) európai modelljéhez részletesen ld. Jan J. Zygmuntowski – Laura Zoboli – Paul F. Nemitz: Embedding European values in data governance: a case for public data commons. *Internet Policy Review – Journal on Internet Regulation*, Vol. 10., Issue 3. (2021) 1–29. <https://doi.org/10.14763/2021.3.1572>

⁴⁹ E folyamat legújabb állomása a mesterségesintelligencia-alapú szolgáltatások megjelenése, amely komoly kihívás elé állította a kreatív- és szórakoztatóipari értékláncok jogosultjait. A kérdéskörhöz részletesen ld. Dávid Ujhelyi: *If Legislation is a Hammer, Could AI Be a Nail? The Possibility and Viability of AI Legislation in International and EU Copyright Law*. In: Marcell Szabó – Laura Gyeney – Petra Lea Lángos (eds.): *Hungarian Yearbook of International Law and European Law*. Baden-Baden, Nomos Verlagsgesellschaft, 2025. 31–61. <https://doi.org/10.5771/9783748955481-29>

⁵⁰ Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998).

⁵¹ Az internetszolgáltatók felelősségkorlátozását (ún. *safe harbor* intézményét), valamint az ehhez kapcsolódó értesítési és eltávolítási (*notice and takedown*) eljárást a DMCA 512. paragrafusa kodifikálta.

egyes közvetítő szolgáltatók típusainak meghatározására és a tevékenységükhöz passzoló felelősségi és mentesülési rendszer kialakítására.⁵²

Az európai jogfejlődési ív egyik csúcspontja a CDSM irányelv 17. cikke,⁵³ amely elsődleges felelősséget telepít az online tartalommegosztó platformszolgáltatók vállára, *expressis verbis* kimondva, hogy ezek a szolgáltatók elsődleges felhasználói a szerzői műveknek és kapcsolódó jogi teljesítményeknek, amiből következik, hogy engedélyt kell kérniük a jogosultaktól, és felhasználási díjat kell fizetniük.⁵⁴ Ez lényegében egy *ex ante* jellegű tartalomszűrést jelent, hiszen a 17. cikk hatálya alá eső platformoknak minden tőlük telhetőt meg kell tenniük annak érdekében (*best effort*), hogy a végfelhasználók által feltöltött tartalmakat jogosítsák. Ez technikai szempontból egy *upload filter*, vagyis a feltöltést ellenőrző szoftveres, automatizált mechanizmus megteremtését jelenti.

A CDSM irányelv 17. cikke által bevezetett, elsődleges platformfelelősséget kimondó és jogosítási kötelezettséget előíró rendelkezés érdekösszeütközéshez vezetett az Európai Unió és az Egyesült Államok között. Az amerikai technológiai vállalatok és kormányzati szereplők nehezményezték, hogy a 17. cikk cenzúráként működik, ami sérti a szólásszabadságot.⁵⁵ A 17. cikk az EU-n belül is feszültséget keltett. A lengyel kormány az Európai Unió Bírósága előtt támadta meg a rendelkezést, amiről úgy vélte,

⁵² Az európai közvetítő szolgáltatókra vonatkozó felelősségi rendszer fejlődése három főbb jogalkotási szakaszra bontható. Az alapot az elektronikus kereskedelemről szóló, 2000. június 8-i 2000/31/EK európai parlamenti és tanácsi irányelv fektette le, amely az amerikai modellhez hasonló mentesülési rendszert, valamint általános nyomon követési tilalmat vezetett be a passzív szolgáltatók számára. Ezt a rendszert a CDSM irányelv 17. cikke alakította át, amely az online tartalommegosztó szolgáltatókra (OCSSP) már egy sokkal szigorúbb, aktív szűrési és engedélykérési kötelezettségekkel járó (ún. *notice and stay down*) felelősségi modellt alkalmaz. Az átfogó rendszerszintű reformot végül a Digitális szolgáltatásokról szóló rendelet (DSA – (EU) 2022/2065) az alapvető mentességek fenntartása mellett a platformok méretével és jellegével (pl. VLOPs – nagyon nagy online platformok) arányos, szigorú átláthatósági és tartalommoderálási kötelezettségeket vezetett be, míg a Digitális piacokról szóló rendelet (DMA) a technológiai „kapuőrök” (*gatekeepers*) gazdasági erejét és versenytorzító hatásait korlátozza *ex ante* szabályozási eszközökkel.

⁵³ A CDSM irányelv magyarországi átültetéséhez ld. Baranyi Róbert – Ujhelyi Dávid: A digitális szerzői jogi szabályozás lépcsője – a CDSM irányelv átültetésének háttere és eredményei. *Fontes Iuris*, 2021/3. 36–45.

⁵⁴ A CDSM irányelv 17. cikkének dogmatikai hátteréhez, a tartalommegosztó platformok (OCSSP) elsődleges felhasználói státuszához, és az ebből fakadó engedélykérési kötelezettségekhez ld. Ondrej Woznica: Control or Compensation: Distorted Narrative and Aftermath of Article 17 CDSM. *GRUR International*, Vol. 73., N. 7. (2024) 631–646. <https://doi.org/10.1093/grurint/ikae076>

⁵⁵ A CDSM-irányelv körüli európai–amerikai érdekösszeütközéshez, valamint a nagy amerikai technológiai platformok (elsősorban a Google és a YouTube) masszív, a 17. cikket érintő lobbitevékenységéhez ld. Annemarie Bridy: The Price of Closing the Value Gap: How the Music Industry Hacked EU Copyright Reform. *Vanderbilt Journal of Entertainment & Technology Law*, Vol. 22., Issue 2. (2020) 323–358.; Joao Pedro Quintais: The New Copyright in the Digital Single Market Directive: A Critical Look. *European Intellectual Property Review*, Vol. 42., N. 1. (2020) 28–41. <https://doi.org/10.2139/ssrn.3424770>; Ujhelyi Dávid: A politikai paródia célját szolgáló felhasználások szerzői jogi megítélése. *In Medias Res*, 2022/1. 49–65. <https://doi.org/10.59851/imr.11.1.4>

hogy sérti az Alapjogi Chartában foglalt alapjogokat.⁵⁶ Az Egyesült Államok az uniós jogalkotási lépéseket több szempontból is kritizálta. Egyrészt úgy vélte, hogy az amerikai honosságú technológiai vállalatok üzleti modelljeinek többletköltséget és jelentős piaci kockázatot jelent, hiszen a bonyolult szűrőrendszerek kialakítása és működtetése, illetve a tartalmak jogosítása valóban plusz anyagi teherrel jár. Ezen felül a határozott uniós jogalkotói fellépés precedenst teremthet arra nézve, hogy más joghatóságok is hasonló keretrendszerben próbáljanak meg gátat szabni az amerikai vállalatok korlátlan terjeszkedésének. Donald Trump elnök ezért ezt a kérdést beemelte a kereskedelmi háborús narratívába, felröva az EU-nak azt, hogy cenzúrázza az amerikai vállalatokon keresztül zajló információáramlást és visszaveti az innovációt.⁵⁷ Az érintett vállalatok is – például a Meta – az uniós platformszabályokat vámokhoz, sőt, szankciókhoz hasonlították, aminek a hátterében azt sejtik, hogy az Unió így próbálja meg az egyébként versenyképtelen digitális és technológiai szektorát protekcionista eszközökkel felzárkóztatni a világ élvonalához.⁵⁸

A tartalommoderáció nem csak szerzői jogi szempontok miatt vált fontossá, hanem geopolitikai aspektusai is vannak. Ezek között az egyik legfontosabb az illegális tartalmak feltöltésének lehetővé tétele, illetve a felkerült tartalmak moderálása, eltávolítása. Különösen érzékeny e tekintetében a platformokon jelen lévő gyűlöletbeszéd, terrorizmus, dezinformáció vagy választási manipuláció céljából készített és terjesztett tartalom. Az Egyesült Államokban e körben a *Communications Decency Act*⁵⁹ 230.

⁵⁶ C-401/19. Lengyel Köztársaság vs. Európai Parlament és az Európai Unió Tanácsa. ECLI:EU:C:2022:297. A lengyel kormány megsemmisítési keresetében azzal érvelt, hogy a CDSM-irányelv 17. cikk (4) bekezdés b) és c) pontjában előírt, a tartalmak megelőző szűrésére vonatkozó kötelezettségek *de facto* előzetes cenzúrát valósítanak meg, sértve az Alapjogi Charta 11. cikkében garantált véleménynyilvánítás és tájékozódás szabadságát. Az EUB a keresetet elutasította és a rendelkezéseket hatályban tartotta, elismerve ugyan, hogy a szűrési kötelezettség valóban korlátozza a véleménynyilvánítás szabadságát, azonban ezt a korlátozást indokoltnak és arányosnak ítélte. A Bíróság érvelése szerint továbbá a jogalkotó megfelelő és elégséges garanciákat (például a jogszerű felhasználások [paródia vagy az idézés], a túlzott blokkolás tilalmát, valamint hatékony panasz- és jogorvoslati mechanizmusokat) épített be a 17. cikkbe annak érdekében, hogy biztosítsa a szellemi tulajdon védelme és a felhasználók alapjogai közötti méltányos egyensúlyt.

⁵⁷ Az európai szabályozási törekvések tengerentúli fogadtatásához ld. Clotilde Bomont: Trump takes aim at 'overseas extortion' of American tech companies: the EU-US rift deepens. *European Union Institute for Security Studies – Commentary*, 27 February 2025. <https://tinyurl.com/yc7wsuubh>; illetve U.S House Judiciary Committee: Europe's Threat to American Speech and Innovation: Part II. (Meghallgatás és jelentés, 2026. február 4.). A CDSM-irányelv 17. (korábban 13.) cikke által kiváltott vitákhoz ld. Sascha Segan: Europe's Article 13 Copyright Rule Is a Transatlantic Trade War. *PCMag*, March 27, 2019. <https://www.pcmag.com/opinions/europes-article-13-copyright-rule-is-a-transatlantic-trade-war>

⁵⁸ Az amerikai technológiai óriások, mindenekelőtt a Meta kritikájához ld. Walter Flanagan: It's Time for U.S. Competition Regulators to Learn from the EU's Digital Markets Act. *Georgetown Law Technology Review*, December 2025. <https://tinyurl.com/zcmuv37m>; Zach Meyers: *Why tech firms should not stoke transatlantic tensions*. Centre for European Reform, 2025. 1–4. https://www.cer.eu/sites/default/files/insight_ZM_techfirms_24.1.25.pdf. A digitális szuverenitás és a digitális protekcionizmus dogmatikai és geopolitikai értelmezéseihez ld. továbbá Anu Bradford: Europe's Digital Constitution. *Virginia Journal of International Law*, Vol. 64., No. 1. (2023) 55–61.

⁵⁹ Communications Decency Act of 1996, Pub. L. No. 104-104, tit. V, 110 Stat. 56, 133–43 (codified as amended in scattered sections of 47 U.S.C.).

cikkét kell megemlíteni, amely mentesíti a platformokat az ilyen tartalmakért vállalt felelősség alól.⁶⁰ Az amerikai megközelítés ugyanis az, hogy a túl szigorú platform-szabályozás veszélyezteti a szólásszabadságot, ezért a kérdés rendezését a platformok önszabályozására bízták.⁶¹ Így aztán nem is meglepő, hogy a tengerentúlon egyelőre nincs átfogó szabályozás, hanem széttagolt, részleges jogalkotási kísérletek vannak. Európában éppen ellenkezőleg, jóval szigorúbb megközelítés érvényesül. Ennek egyik legutóbbi megnyilvánulása a DSA rendelet, amely kötelező kockázatértékeléseket, auditokat, gyors eltávolítási mechanizmusokat ír elő a nagy platformüzemeltetők számára az illegális tartalmak és más káros jelenségek, például álhírek kezelésére.⁶² A DSA szigorú szabályai olyannyira kivívták Washington ellenszenvét, hogy Donald Trump 2025-ben a NATO biztonsági garanciáinak felülvizsgálatával fenyegetőzött, figyelmeztetve arra, hogy amennyiben az EU túl messzire megy az amerikai honosságú cégek regulálásában, akkor az USA válaszetorziókat fog foganatosítani, például kereskedelmi szankciók formájában.⁶³

Miközben tehát Európában uniós szinten igyekeznek jogszabályi keretek közé szorítani nagy platformok tevékenységét, amelyet az amerikai kormányzat nem szível, Kínában a platformok állami cenzúra hatálya alá esnek. Ennek legfőbb jogszabályi háttereként a 2017-es Kiberbiztonsági törvény⁶⁴ szolgál. A kínai közösségimédia-, videómegosztó- és más platformok kötelesek proaktívan előre szűrni és távol tartani a platform felületeitől minden olyan tartalmat, amely politikailag érzékeny lehet, vagy egyéb más tiltott információt (például pornográf vagy erőszakos tartalom) tartalmaz. Az extrém centralizáltság pedig akkor tekinthető geopolitikai szempontból problémának, ha a kínai fejlesztésű platformok elkezdnek más országokban is szolgáltatást nyújtani. A nyugati országok például attól tartanak, hogy a kínai platformokon keresztül nem csak a kínai befolyás érkezik, hanem fordított irányban, a végfelhasználók internetes magatartásának nyomai és személyes adatai a kínai állam számára is megismerhetővé válnak. Indiában például 2020-ban nemzetbiztonsági okokra és

⁶⁰ A 230. § kimondja, hogy az interaktív számítógépes szolgáltatások nyújtói nem tekinthetők a más által szolgáltatott információk közzétevőjének vagy szerkesztőjének (*publisher or speaker*), így főszabály szerint mentesülnek a harmadik felek által közzétett tartalmakért való felelősség alól [(c) (1) bek.]. A rendelkezés tartalmazza az ún. „*Irgalmas samaritanus*” (*Good Samaritan*) elvet is, amely lehetővé teszi a szolgáltatók számára a kifogásolható tartalmak jóhiszemű moderálását vagy szűrését anélkül, hogy ezzel elveszítenék felelősségmentességüket [(c) (2) bek.]. Fontos továbbá az (e) (2) bekezdés, amely rögzíti, hogy a 230. § mentessége nem érinti a szellemi tulajdonjogokat (pl. szerzői jog), így ezen a területen továbbra is a DMCA speciális felelősségi szabályai az irányadók.

⁶¹ Bradford (2023) i. m. 2–5.

⁶² Uo. 12.

⁶³ Bomont i. m.; Duc Minh Nguyet Nguyen – Philip Luck: The New Containment Doctrine: How the United States Is Using Trade to Stop Digital Regulation. *CSIS*, March 9, 2026. <https://tinyurl.com/4tuwssfw> Defending American Companies and Innovators From Overseas Extortion and Unfair Fines and Penalties. The White House, February 21, 2025. <https://tinyurl.com/4e2f7x5f>; The Foreign Censorship Threat: How the European Union's Digital Services Act Compels Global Censorship and Infringes on American Free Speech – Report. Interim Staff Report of the Committee on the Judiciary of the U.S. House of Representatives, July 25, 2025. <https://tinyurl.com/yb63x2pt>

⁶⁴ Cybersecurity Law of the People's Republic of China.

adatvédelmi aggályokra hivatkozva több mobilalkalmazást – ideértve a TikTok-ot és a WeChat-et – is betiltottak. Vagyis jól megfigyelhető, hogy az államok számára nem csak az adatok és azok lokalizációja, hanem a tartalom- és információáramlás is végső soron szuverenitási kérdés lett.⁶⁵

Az online közvetítő platformokra rótt tartalommoderációs és más kötelezettségek és ezek szerzői és kapcsolódó jogi vetületei a globális információs térben gyakorolt hatalomról is szólnak. Az egyes államok és nemzetközi integrációk – mint amilyen például az EU – a saját értékeiket és érdekeiket igyekeznek a platformszabályozásban megjeleníteni. Európában ez jelenti például a kulturális és alkotói ipar érdekeinek védelmét és a szerzői és kapcsolódó jogi jogosultak pozícióinak megerősítését az idegen honosságú platformüzemeltetőkkel szemben.⁶⁶ Ezzel szemben az Egyesült Államok a saját vállalatai globális vezető szerepét helyezi előtérbe, miközben hangsúlyozza, hogy a túlzott európai platformszabályozás sérti a szólásszabadság elvét.⁶⁷ Kína a pártállami kontrollt fenntartásában érdekelt, amely természetszerűleg torzítja az alkotói szabadságot és a közéleti párbeszédet. Ha csak ezt a három nagy entitást nézzük, akkor a fent felvázolt törésvonalak és érdekrendszerek egy töredezett internet kialakulását hozhatják el, ahol a platformokra regionális együttműködésenként, szövetségi rendszerként, országonként eltérő szabályok vonatkoznak. Ez pedig a platformüzemeltetők globális terjeszkedést szem előtt tartó üzleti modelljének is kihívást jelent. A végfelhasználók szempontjából pedig mindez azzal a veszéllyel fenyeget, hogy a digitális, online tartalmakhoz való hozzáférés és a véleménynyilvánítás lehetősége még inkább területfüggő lesz.

5. Iparjogvédelem és üzleti titok a globális technológiai verseny és dominancia szolgálatában

A XXI. század a szabadalmak és üzleti titkok védelme tekintetében valóságos hadszíntérre válhat. A nagyhatalmi versengésnek mindig is volt egy fontos technológiai vetülete. A nagyhatalmi, hegemon szerep és a fölény kialakításának nemcsak tőke- és humán erőforrás igénye van, hanem olyan technológiai megoldásokra is szükség van, amelyekkel a versenytársak nem rendelkeznek. Ebben a versenyben a szellemi alkotások jogának kiemelkedő szerepe van, és pedig nem csak a tudás és az alkotásból származó haszon miatt. Ezért aztán nem is meglepő, hogy mind az Egyesült Államok, mind Kína stratégiai fontosságúnak tartja a saját szellemi tulajdonvédelmi rendszerének megerősítését és továbbfejlesztését. Ebben a versenyben az Európai Unió is igyekszik lépést tartani, bár ez utóbbi inkább szabályozói és vitarendezői oldalról próbálja meg egyre inkább növekvő technológiai és innovációs lemaradását kompenzálni.

Szabadalmak tekintetében az elmúlt két évtized drasztikus változást hozott. Kína szabadalmi nagyhatalommá fejlődött. Már 2011-ben megelőzte az Egyesült Államokat az egy évben benyújtott szabadalmi bejelentések száma tekintetében. A WIPO statisztika

⁶⁵ Nyáry (2020) i. m.; Bradford i. m. 66–68. Vö. Government Bans 59 mobile apps which are prejudicial to sovereignty and integrity of India, defence of India, security of state and public order.

⁶⁶ Woznica i. m. 638., illetve 646.

⁶⁷ Bradford i. m. 12.

tikai szerint 2023-ban a kínai bejelentések száma meghaladta a 70 ezret, miközben az USA-ban ez a szám csak 60 ezer körül volt.⁶⁸ A kínai előretörés különösen a *kritikus technológiák* körében jelentős. Ebbe a kategóriába tartozik például az akkumulátoripar, a biotechnológia, a mesterséges intelligencia és a félvezetőipar. Egyes területeken – például az OLED kijelzők, akkumulátorok – terén a kínai cégek világelsővé váltak.⁶⁹ Mindezt a kínai állam tudatos stratégiával, jelentős K+F beruházásokkal, állami szubvenciókkal érte el, amelyek segítségével támogatja a szabadalmazást, kvótákat és bónuszokat juttatva a vállalatoknak saját szabadalmi portfóliójuk bővítésére. A mennyiségi nyomulás persze kérdéseket vet fel. A kínai szabadalmak közül sok csak belföldön használható kisebb újítás, miközben a nemzetközi szabadalmi jogdíjbevételek tekintetében továbbra is az Egyesült Államok vezet.⁷⁰ Ehelyütt megjegyzendő, hogy Kína startégiája túlmutat a bejelentett szabadalmak és az abból várható licencdíjak maximalizálásán. Peking célja a technológiai önellátás és standardalkotás. Az elvárás ezzel kapcsolatban az, hogy 2035-ig a kínai cégek hazai és nemzetközi szintén egyaránt szellemi tulajdoni nagyhatalommá váljanak.⁷¹

Kína nem csak a hazai szellemi tulajdon-vagyont építi nagy léptekkel, hanem érdekelt abban is, hogy a rivális nagyhatalmaktól annyi ipari titkot kémleljen ki, amennyi csak lehetséges. Az amerikai–kínai kereskedelmi háború egyik fő hivatkozási alapja éppen a kínai „*IP visszaélések*” vádja volt. Eszerint Kína évtizedeken át a technológiatranszfer kikényszerítésével, ipari kémkedéssel és hackertámadásokkal szerzett meg nyugati üzleti titkokat, know-how-t. 2018-ban az Egyesült Államok Kereskedelmi Képviselőjének irodája jelentésében elmarasztalta Kínát, kimondva, hogy a rivális gyakorlata sérti az amerikai érdekeket, amely később a büntetővármok kivetésének egyik alapvető indokául szolgált.⁷² Az amerikai igazságügyi minisztérium 2018-ban meghirdette a *China Initiative* programot, amely kifejezetten a kínai gazdasági kémke-

⁶⁸ A globális szabadalmi trendek alakulásához ld. WIPO Executive Summary Patent Cooperation Treaty Yearly Review 2023. The International Patent System, 3–4.

⁶⁹ WIPO Patent Cooperation Treaty – Yearly Review 2024. The International Patent System. The Top PCT applicants, 39.

⁷⁰ A kínai szabadalmak számának robbanásszerű emelkedése és a technológia valós piaci értéke között valóságos szakadék alakult ki, amely rávilágít arra, hogy a globális használati mintaoltalmi bejelentések 98%-a ugyan valóban Kínához kötődik, de ezek belföldi fókuszúak, érdemi újdonságvizsgálatot minden bizonnyal nélkülöznek. Ld. WIPO World Intellectual Property Indicators 2024, 7. Ezzel szemben a szellemi tulajdon monetizálása terén az Egyesült Államok fölénye továbbra is nyomasztó, mintegy tízszeres (162,52 milliárd USD az Egyesült Államok és 10,13 milliárd USD Kína esetében), ami egyértelműen az amerikai szabadalmak globális beágyazottságát és értékét tükrözi. Ld. World Bank – Charges for the use of intellectual property, receipts (BOP, current US\$). Vö.: Ciuriak i. m.

⁷¹ Outline for Building an Intellectual Property Powerhouse (2021-2035), China; Guidelines for the Construction of a Comprehensive Standardization System for the National Artificial Intelligence Industry. Vö. Li Mi: Accelerating Innovation: The Rapid pace of Patent Granting in China. *ROUSE*, 17 Oct 2024. <https://tinyurl.com/2ny5zpy4>

⁷² Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974. Office of the United States Trade Representative Executive Office of the President, March 22, 2018. <https://tinyurl.com/yudbtsnu>

dés elleni fellépést tűzte zászlajára.⁷³ Ennek keretében számos vádemelés történt olyan ügyekben, ahol vagy kínai állampolgárságú egyéneket – kutatókat, mérnököket, haccereket –, vagy egyenesen a kínai hírszerzéshez kötődő személyeket vádoltak üzleti titkok ellopásával.⁷⁴ 2023-ban például lebukott egy korábban a Google alkalmazásában álló mérnök, aki mesterséges intelligenciával kapcsolatos üzleti titkokat lopott el a Google-től. Az illetőt gazdasági kémkedésért ítélték el az Egyesült Államokban.⁷⁵ Ez a probléma kitűnően rávilágít arra, hogy a szellemi tulajdon védelme mára nemzetbiztonsági, sőt geopolitikai kérdéssé, illetve szükségszerűséggé vált. Ezt felismerve az USA exportkontrollt is alkalmaz. 2019-től kezdve fekete listára tette többek között a Huawei-t és a ZTE-t, amelyeknek bizonyos amerikai technológiai vállalatok nem szállíthatnak.⁷⁶ Ez továbbá felveti azt a geopolitikai kérdést is, hogy egy adott szövetségi rendszeren – például a NATO-n – belül megtűrhető-e olyan technológia, például a digitális hálózatokban, amely nem nyugati, hanem kínai szabvány. E lépések legfőbb célja az, hogy Kína ne tudja a legfejlettebb technológiákra rátenni a kezét, vagy megtanulva az előállítás lépéseit, technológiai ugrást végrehajtani az egyes szektorokban.⁷⁷

A kínai ipari kémkedés nem csak az Egyesült Államokban okozott fejtörést. Európában is nagyon sok gondot okozott a jelenség. Az öreg kontinensen ráadásul fontos érdek továbbra is a kínai piacra jutás, ami miatt a döntéshozók és hatóságok igyekeznek az ilyes fajta incidenseket diplomatikusabban kezelni. Ezzel párhuzamosan Európában is zajlik a kínai aktivitással szembeni védelmi mechanizmusok átgondolása és kiépíté-

⁷³ The China Initiative. A US government national-security program, created to address economic espionage, disproportionately targeted Asian Americans and academic communities for administrative errors and harmed academic freedom and open science. <https://www.apajusticetaskforce.org/the-china-initiative>

⁷⁴ Uo. Vö. Ciuriak i. m. A United States v. You, 74 F.4th 378 (6th Cir. 2023) ügyben jogerősen 14 év börtönt kapott Xiaorong You technológiaplopásért, a United States v. Xu, No. 22-4020 (6th Cir. 2024) során pedig Yanjun Xu hírszerzőt 20 év szabadságvesztés büntetésre ítélték repülőgépipari kémkedésért. Az APT41 elleni United States v. Qian et al. (D.D.C., 2020) vádirat kiberkémkedést dokumentált, bár az elkövetők jelenleg is szökésben vannak.

⁷⁵ United States v. Linwei Ding, 3:24-cr-00141-VC (N.D. Cal., 2026).

⁷⁶ Az amerikai exportkorlátozások jogi alapját az Export Control Reform Act of 2018 (ECRA) és a Bureau of Industry and Security (BIS) listája adja. A Huawei technológiai elszigetelését a Foreign Direct Product Rule teljesítette ki, amely globális szinten tiltja az amerikai technológiával készült chippek eladását a vállalatnak. Ld. Export Administration Regulations: Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule) and the Entity List. Ruled by the Industry and Security Bureau on 05 19 2020. Vö. Ciuriak i. m.; Mórász Ferenc: Az amerikai és kínai MI-stratégia összehasonlítása. *Makronóm*, 2025. augusztus 5. <https://tinyurl.com/5n97525y>

⁷⁷ A magyarországi 5G hálózat kiépítése során alkalmazott stratégia éles ellentétben áll az uniós irányelvekkel. Az Európai Bizottság jelentése hangsúlyozza a magas kockázatú beszállítók kivezetésének szükségességét. Ld. A Bizottság közleménye az 5G kiberbiztonsággal kapcsolatos eszköztár végrehajtására. Brüsszel, 2023.6.15. C(2023) 4049 final. Vö. Ivana Karásková – Alicja Bachulska – Tamás Matura – Matej Šimalčík: *Careful or careless? Debating Chinese investment and 5G technology in Central Europe*. Policy Paper. 2021. 11–56.; Ivana Karásková – Konstantinas Andrijauskas – Alicja Bachaluska – Una Aleksandra Bērziņa-Čerenkova – Andreea Leonte – Tamás Matura – Matej Šimalčík: *Huawei in Central and Eastern Europe: Trends and Forecast*. Briefing Paper. 2021. 7–22.

se. 2019-ben elfogadásra került a külföldi befektetések átvilágításáról szóló rendelet,⁷⁸ amely lehetővé teszi a stratégiai ágazatokban a kínai felvásárlási kísérletek megakadályozását. 2016-ben megszületett az üzleti titok védelméről szóló irányelv⁷⁹ is, amely erősebb védelmet nyújt az üzleti titkoknak a tagállamokban, polgári jogi igényérvényesítési eszköztárral támogatva a fellépést. Ez már csak azért is fontos, mert az európai vállalatok számára is egyre értékesebb a know-how és a bizalmas üzleti információ, különösen a high-tech iparágakban.

A technológiai dominancia kiépítése és fenntartása szempontjából a szellemi alkotások joga elsődleges fontosságú, sőt, egyszerre alkalmas offenzív és defenzív módon támogatni az államok törekvéseit. Aki több és erősebb szellemi oltalom alatt álló technológiával rendelkezik, az nem csak a hasznosításból származó piaci előnyt szerzi meg, hanem diktálhatja a standardokat is. Ha például egy európai szabadalom szabványos technológia részévé válik, a fejlesztő lesz az, aki az ebből származó gazdasági hasznokat bezsebelheti. Az 5G területén ilyen vállalatnak tekinthető a Huawei, akik nagyon fontos szabványokhoz elengedhetetlen szabadalom (*standard essential patent*) jogosultja lett. A szellemi oltalom emellett segíthet kivédeni egy ellenérdekelt nagyhatalom jogszerűtlen felhasználásra, lemásolásra irányuló kísérletét, jogi útra terelve a versenyt. Az okostelefon-háborúknak (pl. Apple és Samsung) megfigyelhető volt, hogy a nagy cégek szabadalmi perek sorát indítják egymás ellen, ami a valóságban a vezető, domináns piaci pozíció megtartásáról szól.⁸⁰

A szellemi alkotások terén zajló nagyhatalmi versengés komolyan felveti a kérdést, hogy vajon a jelenleg fennálló nemzetközi szellemi tulajdonvédelmi rendszer a WTO és a WIPO keretein belül mennyire tartható fenn, illetve mennyire tudja kezelni ezt az egyre élesebbé váló versenyfutást. Kína, csatlakozva a WTO-hoz, elfogadta magára nézve kötelezőnek a TRIPS-egyezmény előírásait, ám azokat nemigen tartja be. Emellett egyik legfontosabb érve a jogsértést kiáltó nyugati vetélytársakkal szemben az, hogy sok európai és amerikai vállalat önként vitte be a technológiát Kínába a piacra jutás lehetőségéért cserébe. Kína ezt követően maga is képes volt fejlett technológiák előállítására, amit pedig védenie kell, mert maga is gyakran elszenvedti az innovációi jogtalan eltulajdonítását a szomszédos, nála fejletlenebb államoktól.⁸¹

⁷⁸ Az Európai Parlament és a Tanács (EU) 2019/452 rendelete (2019. március 19.) az Unióba irányuló közvetlen külföldi befektetések átvilágítási keretének létrehozásáról, HL L 79L, 23.12.2021., 1–14. o.

⁷⁹ Az Európai Parlament és a Tanács (EU) 2016/943 irányelve (2016. június 8.) a nem nyilvános know-how és üzleti információk (üzleti titkok) jogosulatlan megszerzésével, hasznosításával és felfedésével szembeni védelemről, HL L 157., 2016.6.15., 1–18. o.

⁸⁰ A technológiai szabványok feletti kontroll gazdasági jelentőségéhez ld. Who Is Leading the 5G Patent Race? 5G Report – January 2026. Vö. LexisNexis Report Shows Huawei, Qualcomm, Samsung, and Ericsson leading Patent Race in \$15 Billion 5G Licensing Market. A piaci dominancia megőrzésére irányuló szabadalmi jogviták klasszikus példája az Apple és a Samsung közötti pereskedések sorozata: Apple Inc. v. Samsung Electronics Co. Ltd. et al, No. 5:2011cv01846 – Document 1157 (N.D. Cal. 2012); Samsung Electronics Co. v. Apple Inc., 580 US (2016); Apple Inc. v. Samsung Electronics Co., Ltd. et al, No. 5:2012cv00630 – Document 1962 (N.D. Cal. 2014).

⁸¹ Kína WTO előírásainak való megfelelési nehézségeiről ld. 2023 Report to Congress on China's WTO Compliance. United States Trade Representative. A kínai „piacot technológiáért” (*quid pro quo*) modell elemzéséhez ld. Thomas J. Holmes – Ellen R. McGrattan – Edward C. Prescott: Quid Pro Quo:

A szellemi tulajdon különböző oltalmi formái nem csak a nagyhatalmi versengés „támadó” és „védekező” eszközei, hanem a puha hatalom (*soft power*) részei is. A magas technológiát kifejleszteni képes ország ugyanis az, amelyik megszabhatja a játékszabályokat, előírva az alkalmazandó szabványokat és protokollokat.⁸² Ez lehetővé teszi számára azt is, hogy akár a biztonsági „kiskapukat” is ellenőrizze. Emellett pedig az adott technológiát kifejlesztő hatalom a hozzáértő szakembereket is vonzáskörében tarthatja. Ezért aztán nem csoda, hogy az államok közötti technológiai és végső soron hatalmi versengés stratégiai tárgya lett a szellemi tulajdon védelme. Az Európai Unió például lemaradásban van a digitális szabadalmak terén, ezért megpróbálja ösztönözni az e téren zajló kutatásokat, illetve célul tűzte ki az *Európai Szabadalmi Rendszer* reformját. 2023-ban megkezdte működését az Egységes Szabadalmi Bíróság (*Unified Patent Court*) és bevezetésre került az egységes hatályú európai szabadalom. Az egyértelmű cél a versenyképes, gyors oltalomszerzés biztosítása az európai innovátorok számára.⁸³

Az üzleti titok eközben a gazdasági versenyfutás hírszerzési oldalát látja el munkával. Az Egyesült Államokban a 2020-as években több száz nyomozás zajlott párhuzamosan, amelyben a vád az amerikai üzleti titkok ellopása volt.⁸⁴ Ezt jellemzően a kínai kiber-felderítés végzi, amely széles spektrumon igyekszik szert tenni a nyugati titkokra a haditechnikától a kereskedelmi know-how-ig. A kínaiak ezzel szemben azt állítják, hogy a nyugat a szellemi tulajdonvédelmet *feketelistázásra* használja fel, amellyel a célja a kínai felemelkedés megakadályozása.⁸⁵

A fentiek tükrében nem túlzás azt állítani, hogy a szellemi alkotások védelme ma már nem pusztán jogtechnikai kérdés, hanem az államok jól felfogott geopolitikai-gazdasági-technológiai versenyfutásának része. Aki birtokolja a kulcstechnológiák szabadalmait és hatékonyan meg tudja védeni üzleti titkait, miközben ki tudja kémlelni a versenytársakét, az igen komoly előnyre tesz szert.

Technology Capital Transfers for Market Access in China. *The Review of Economic Studies*, Vol. 82., Issue 3, (2015) 1154–1193. <https://doi.org/10.1093/restud/rdv008>

⁸² A szabványok és protokollok nagyhatalmi törekvésekhez való felhasználásához ld. Henry Farrell – Abraham L. Newman: Weaponized Interdependence – How Global Economic Networks Shape State Coercion. *International Security*, Vol. 44., N.1. (2019) 42–79. https://doi.org/10.1162/isec_a_00351

⁸³ Az egységes, európai szabadalmi oltalom létrehozásához ld. Az Európai Parlament és a Tanács 1257/2012/EU rendelete az egységes szabadalmi oltalom létrehozásának területén megvalósítandó megerősített együttműködés végrehajtásáról, HL L 361., 2012.12.31., 1–8. o. Az Egységes Szabadalmi Bíróság felállításáról pedig a 2013/C 175/01 megállapodás az egységes szabadalmi bíróság létrehozásáról rendelkezett. Az egységes szabadalmi rendszer kritikájához ld. Reto M. Hilty – Thomas Jaeger – Matthias Lamping – Hanns Ullrich: *The Unitary Patent Package: Twelve Reasons for Concern*. Max Planck Institute for Intellectual Property and Competition Law, 2012. <https://doi.org/10.2139/ssrn.2169254>

⁸⁴ Survey of Chinese Espionage in the United States Since 2000. <https://tinyurl.com/5v6ce9f6>

⁸⁵ Az Európai Unió belső piaca és Kína stratégiai ágazataiban fennálló szigorú korlátozások rendszer-szintű aszimmetriájához ld. Áttekintés 03/2020: Az Unió válasza Kína államilag vezérelt beruházási stratégiájára. Curia Rationum – Európai Számvevőszék, 2020. Vö. US *Hegemony and Its Perils*. Ministry of Foreign Affairs People's Republic of China. February 2023; Mórász i. m.; Nemes Tamás: Már a látszatra sem ad Kína, szabad(almaztatott) a rablás. *Világgazdaság*, 2023.02.22. <https://tinyurl.com/yuhdtbtz>

6. Mesterséges intelligencia, mint stratégiai erőforrás és a digitális hatalom új színtere

A digitális platformok és az ezeken generált tömérdek mennyiségű adat által felvetett problémák és kérdések a nemzetközi, regionális és tagállami jogalkotókat folyamatos feladatokkal látták el az elmúlt három évtizedben. Ebbe a sorba illeszkedik, sőt, a ki-hívás mértékét tekintve ki is emelkedik a mesterséges intelligencia, ami ráadásul egy olyan keresztülfekvő technológia, amit jogalkotási területeken átívelő módon kell kezelni. Hatása van a platformok irányítására, a közbeszédre, a szellemi alkotások jogára, az adat- és a fogyasztóvédelemre. A mesterséges intelligencia mindennek a tetejében a nagyhatalmi versengésnek egyik elsődleges terepe lett. Mivel kevésbé innovatív e téren, mint versenytársai, az Európai Unió elsősorban magas szintű szabályozási eszközökkel igyekszik a kérdéskört megközelíteni. E tekintetben nem mehetünk el szó nélkül az AI Act, a DSA és a DMA mellett, amelyek együttesen az összeurópai hatékony jogérvényesítés eszközeiként szolgálnak az idegen honosságú technológiai cégekkel szemben.⁸⁶ Ettől eltérő felfogást vall az Egyesült Államok, amely a túl szigorú szabályozásban az innováció akadályát látja. Noha egymás versenytársai, az Európai Unió és az Egyesült Államok igyekeznek közösen fellépni a kínai technológiai nyomulással szemben a mesterséges intelligencia területén is. A felek 2021-ben létrehozták az *EU-US Trade and Technology Council*-t, amelyben egyöntetűen elutasítják az emberi jogokat szisztematikusan megsértő AI-rendszereket, kritizálva egyúttal Kína „*social credit*” modelljét.⁸⁷

A közös fellépés miéértje nem csak az emberi jogok melletti kiállással magyarázható. Legalább ennyire fontos aspektus az is, hogy a kínai fejlesztések az 1,3 milliárd állampolgárról készíthető és már készített adatot a saját AI-rendszereik tanítására,

⁸⁶ Az európai platform- és mesterségesintelligencia-szabályozás egyes metszéspontjaihoz ld. Kitti Mezei-Anikó Träger: *The Europea Approach to Artificial Intelligence. Ethical and Regulatory Implications. Acta Universitatis Sapientiae, Legal Studies*, Vol. 11., N. 2. (2022) 19–34. <https://doi.org/10.47745/AUSLEG.2022.11.2.02>; Fabian Ferrari: *State roles in platform governance: AI's regulatory geographies. Competition & Change*, Vol. 28, No. 2, 2024. 340–58. <https://doi.org/10.1177/10245294231218335> ; Philipp Hacker – Johann Cordes – Janina Rochon: *Regulating Gatekeeper Artificial Intelligence and Data: Transparency, Access and Fairness under the Digital Markets Act, the General Data Protection Regulation and Beyond. European Risk Regulation*, Vol. 15, Issue 1. (2024) 49–86. <https://doi.org/10.1017/err.2023.81>; Claudio Novelli – Phillip Hacker – Jessica Morley – Jarle Trondal – Luciano Floridi: *A Robust Governance for the AI Act: AI Office, Ai Board, Scientific Panel, and National Authorities. European Journal of Risk Regulation*, Vol. 16., Issue 2. (2025) 566–590. <https://doi.org/10.1017/err.2024.57>; Hans Graux – Krzysztof Garstka – Nayana Murali – Jonathan Cave – Maarten Botterman: *Interplay between the AI Act and the EU digital legislative framework*. (Study Requested by the ITRE committee) Brussels, European Parliament, 2025.

⁸⁷ Az európai és amerikai szabályozási megközelítések összehasonlító vizsgálatához ld. Camilla Scarpellino: *EU and US regulatory approach to AI: a comparative perspective. Luiss Policy Observatory Policy paper*, No. 10/2024. 1–12. Vö. TTC Joint Roadmap on Evaluation and Measurement Tools for Trustworthy AI and Risk Management (December 1, 2022) 1–11. A kínai social credit modellről ld. Chuncheng Liu – Akos Rona-Tas: *Trusting by Numbers: An Analysis of a Chinese Social Credit System Governance Infrastructure. Critical Sociology*, Vol. 51., N. 6. (2025) 1247–1265. <https://doi.org/10.1177/08969205241246528> Az európai mesterségesintelligencia-szabályozás tagállami vetületeihez és a szabályozás földrajzi aspektusaihoz ld. Ferrari i. m. 340–358.

tréningezésére használják fel, ami – már csak az adatok számossága okán is – versenyelőnyt jelenthet számukra. Ez a versenyelőny ugyanakkor törekeny, mert Kína ki van szolgáltatva azoknak a nyugati félvezetőgyártóknak, akik új generációs, nagy számítási műveleteket elvégezni képes mikrochipeket gyártanak. A világban zajló geopolitikai átrendeződés egyfajta szétkapcsolódással (*decoupling*) is együtt jár. Ez a digitális technológiák terén a minél nagyobb fokú önállóság megteremtésének igényét eredményezi. A cél immár az, hogy a nagyhatalmak a lehető legkevesébé függjenek ellenfeleiktől a ritkaföldfémek, a chipgyártás és az adatfeldolgozás és adatáramlás terén. Ez a magatartás szükségképpen eredményezi a nagy digitális és innovációs hálózatok fragmentálódását.⁸⁸

Márpedig e tekintetben a nagyhatalmak egymásra vannak utalva. Az Egyesült Államok egyik legfontosabb ritkaföldfém-beszállítója Kína. Ha Kína elvágja az Egyesült Államokat ezen forrásoktól, rendkívül megrághat és elnehezülhet az elektronikai eszközök gyártása szempontjából nélkülözhetetlen beszerzés. Európa ezzel szemben az amerikai és kínai technológiáknak (digitális platformszolgáltatások, felhőszolgáltatások, mesterséges intelligencia) van kiszolgáltatva. A kölcsönös függés elismerése és az ebből fakadó egyensúly felismerése és fenntartása helyett a regionális nagyhatalmak inkább az izoláció, a saját ökoszisztémák kiépítése irányába mozdultak el. Az Egyesült Államok a Chips Act-ben⁸⁹ foglaltaknak megfelelően tekintélyes beruházásokat eszközölt a chipgyártó kapacitásainak megnövelésére, amely példát Európa is követni igyekszik a Csiprendeletben foglaltak szem előtt tartásával.⁹⁰ Eközben pedig Kína szintén a hardvergyártó kapacitásai megnövelésére törekszik. Ezeket a törekvéseket lényegesen árnyalja, hogy a hatékony fejlesztésekre csak néhány szereplőnek – jellemzően a technológiai óriásoknak és a nagyhatalmaknak – van meg a kellő anyagi erőforrása. Egyelőre úgy fest, hogy ezek az erőforrások csak az Egyesült Államokban és Kínában állnak rendelkezésre. Ezért Európa inkább a szabályozási oldalról közelítve próbálhatja elérni, hogy a területén használt digitális technológiai megoldások, ideértve a mesterséges intelligenciát is, kövessék az európai értékrend által diktált szí-

⁸⁸ Kína nemzetközi térben betöltött szerepéhez és külkereskedelmi függőségéhez ld. Vörös Zoltán – Horváth Levente: Dominancia és függés? Kína az átalakuló nemzetközi térben. In: Vörös Zoltán – Tarrósy István (szerk.): Átalakuló világrend. Az unipoláris pillanat vége? Budapest, Ludovika, 2024. 37–60. https://doi.org/10.36250/01222_02 A kritikus nyersanyagok digitális gazdaságban betöltött szerepéhez és az ezzel kapcsolatos kihívásokra adott európai és kínai válaszokhoz ld. Viktória Lilla Pató: Strategic Dilemmas Related to Critical Raw Materials as the Engine of Digital Transition – The Power Relations of Brussels and the Beijing Effect. In: Tibor Navracsics – Laura Schmidt – Balázs Tárnok (szerk.): *On the Way to the Hungarian EU Presidency*. Budapest, Ludovika, 2023. 127–143. https://doi.org/10.36250/01172_10 Az ellátási láncok fontosságához és részleteihez ld. András Edl: Supply Chains and Space Capabilities in the New Space Age. In: Balázs Bartóki-Gönczy – Gábor Sulyok (szerk.): *The New Space Age – Legal and Policy Perspectives*. Budapest, Ludovika, 2024. 515–551. https://doi.org/10.36250/01208_20

⁸⁹ Creating Helpful Incentives to Produce Semiconductors – CHIPS and Science Act of 2022. Public Law No: 117-167. (08/09/2022).

⁹⁰ Csiprendelet i. m.

gorú jogszabályi környezetet.⁹¹ Ennek a szigornak saját gravitáló ereje van, amelyet „Brüsszel-hatásként” ismer a szakirodalom.⁹² Ennek lényege, hogy amennyiben egy nagy piacon szigorú normák vannak hatályban, a globális cégek kénytelenek igazodni ehhez. Vagyis lényegében az Európai Unió a fejlett jogalkotási rendszerével képes világstandardokat létrehozni. Erre példaként a GDPR, a DSA és a DMA is felhozható példaként, amelyek nagyon fontos, követendő standardokat alkotnak az adatvédelem és a digitális platformgazdaság terén.⁹³

Röviden összefoglalva, a mesterséges intelligencia – hasonlóan a világhoz – több pólusúvá válik. Az innováció és a fejlesztések terén az Egyesült Államok és Kína a domináns, míg Európa olyan szigorú, rendeleti szintű, tehát a tagállamokban közvetlenül alkalmazandó szabályozási keretrendszert igyekszik létrehozni, amely ezt a nagyhatalmi érdekek által diktált versengést értékalapú keretek közé szorítja. Ebben a törekvésben pedig vannak olyan vonások, amelyekben Kína is osztozik. Bár jóllehet Kína maga az *Új Generációs MI Fejlesztési Terv*⁹⁴ révén a világ vezető mesterségesintelligencia-nagyhatalma kíván lenni, hangsúlyozza, hogy a mesterséges intelligenciának etikusnak kell lennie, amely mindenki javát szolgálja egy globális együttműködés keretében.⁹⁵ Peking még arra is javaslatot tett, hogy erre a célra hozzanak létre nemzetközi szervezetet, amelynek még székhelyet – Sanghaj – is javasolt. A szervezet feladata a globális mesterséges intelligencia koordinálása és előnyeinek elosztása lenne.⁹⁶ A javaslat mögött természetesen jól felfogott geopolitikai szándék is meghúzódik, nevezetesen az, hogy az Egyesült Államok még mindig meglévő technológiai fölényét és egyoldalú szankciós politikáját Kína multilaterális keretben tudja ellensúlyozni. Peking még arra is hajlandó, hogy saját fejlesztéseit – vagy legalábbis egy részét – megossza a nyilvánossággal, amolyan „Linux-nyílt forráskód” módjára. Emellett persze titkos, hadászati célú fejlesztések is zajlanak, és ismert a fentebb már említett, az állampolgárok totális megfigyelését célzó rendszerek MI-alapú feljavítása is.

A mesterséges intelligencia kereskedelmi felhasználásán túl ismert annak katonai és hírszerzési felhasználása is. Ez a terület ráadásul sokkal fontosabb a nagyhatalmi versengés szempontjából. Amelyik hatalom ugyanis előnyre tesz szert a gépi tanulás, kvantitatív adattudomány és autonóm fegyverrendszerek fejlesztésében, fölénybe

⁹¹ Gleb Papishev – Keith Jin Deng Chan: AI regulatory strategies for digital sovereignty: The role of geopolitics and technological disparities. *Electronic Markets*, Vol. 36., N. 8. (2026) 1–12. <https://doi.org/10.1007/s12525-025-00870-z>

⁹² Arról, hogy az Európai Unió hogyan vált globális szabályozó hatalommá hagyományos katonai vagy politikai kényszerítő eszközök használata nélkül, részletesen ld. Anu Bradford: *The Brussels Effect – How the European Union Rules the World*. Oxford University Press, 2021. <https://doi.org/10.1093/oso/9780190088583.003.0003>

⁹³ Vasilis Georg Hatzopoulos: The EU as an exporter of digital rules and standards? The case of the DSA and the DMA. *Yearbook of European Law*, Online First, 1–25. <https://doi.org/10.1093/yel/yeag003>

⁹⁴ China's New Generation Artificial Intelligence Development Plan (2017).

⁹⁵ Uo. V. Guarantee measures (1) Develop laws, regulations, and ethical norms that promote the development of AI.

⁹⁶ Shanghai Declaration on Global AI Governance. Vö. Lang Ping: The Global Governance of Artificial Intelligence: Progress, Challenges and China's Role. *China-CEE Institute*, Vol. 6., No. 6. (2026) 1–11.

kerül versenytársaival szemben. Kína 1,3 milliárdos népessége miatt tagadhatatlan előnyben van, mert ennyi ember majdnem négyszer annyi adatot képes potenciálisan generálni, mint az Egyesült Államok lakossága egyedül. 2025-ben a kínai adatgazdaságban becslések szerint mintegy 48,6 trillió gigabájtnyi adat keletkezett, amelyet MI-fejlesztésekhez használtak fel.⁹⁷ Hogy Kína mégsem tudott hegemónná válni ezen a téren, az annak köszönhető, hogy a népköztársaság egyelőre nem rendelkezik a legfejlettebb mikrochipekkel, és nincs is meg az ezek fejlesztéséhez elengedhetetlen technológiája, felsőoktatási és kutatóbázisa. Furcsa paradoxon továbbá, hogy hiába áll elméletben rendelkezésre gigantikus méretű adathalmaz a MI-rendszerek betanítására, a kínai lakosság adatelérése a szabadságjogok korlátozása miatt még mindig korlátozottabb, mint a szabad országokban. Európa a két nagy vetélytárshoz képest ezen a téren is tetemes lemaradásban van. Sem vezető chip-technológiája, sem pedig elegendő adat nem áll rendelkezésre a legfejlettebb MI-rendszerek kifejlesztésére, ezért az uniós döntéshozók 200 milliárd eurós csomaggal kívánják serkenteni fejlesztéseket.⁹⁸

A digitális technológiák és az ezen területeken történő befektetések, különösen pedig azok megtérülési rátája hihetetlen tőkeigényesek. Ezért az államok mellett mára már számolnunk kell olyan globális jelenléttel bíró magáncégekkel, amelyek kulcskompetenciák és információk birtokában kvázi szuverén szereplőkké váltak.⁹⁹ Elég, ha csak a Meta vagy a Google tömegtájékoztatásban és dezinformációban betöltött szerepére gondolunk. Egyes technológiai óriások és MI-szolgáltatók hatalma és az egy évben előállított jövedelme mára vetekszik egyes államokéval az adatok, információk hozzáférhetősége és megismerése tekintetében. Ez már komolyan felveti a kérdést, hogy beszélhetünk-e a platformok által gyakorolt digitális, virtuális, infrastrukturális szuverenitásról.¹⁰⁰

⁹⁷ Liu i. m. 48–49. Vö. Kína katonai fejlesztéseihöz, különös tekintettel a mesterséges intelligencia és digitális alapú újításokra részletesen ld. Ryan Fedasiuk – Emily Weinstein – Anna Puglisi: *Kína külföldi technológiára irányuló kívánság listája*. Center for Security and Emerging Technology, 2021. 17–18.; Josh Baughman: The Path to China's Intelligentized Warfare: Converging on the Metaverse Battlefield. *The Cyber Defense Review*, Fall 2024. 29–36. <https://doi.org/10.55682/cdr/xch-heat>; Kevin Pollpeter – Amanda Kerrigan: The PLA and Intelligent Warfare: A Preliminary Analysis. CNA Research Memorandum. CRM-2021-U-030806-Final, 2021. 1–36; Sam Bresnick: *China's Military AI Roadblocks – PRC Perspectives on Technological Challenges to Intelligentized Warfare*. Center for Security and Emerging Technology, June 2024. 1–50. <https://doi.org/10.51593/20230042>; Elsa B. Kania: Artificial intelligence in China's revolution in military affairs. *Journal of Strategic Studies*, Vol. 44., No. 4. (2021) 515–542.

⁹⁸ Capitalising on Europe's Strengths. Investment Report 2025/2026 of the European Investment Bank Group, 2026. 207–250. Vö. EU launches InvestAI initiative to mobilise €200 billion of investment in artificial intelligence. *European Commission Press release*, Feb 11, 2025. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_467; The future of digital regulation... i. m. <https://tinyurl.com/msyk3bts>

⁹⁹ Pavel Bureš: Sovereignty and Transnational Corporations. *Gdanskie Studia Prawnicze*, Vol. 2., N. 59. (2023) 99–108. <https://doi.org/10.26881/gsp.2023.2.08>; Chee Hae Chung – Bryce Dietrich: Corporate Quasi-Sovereignty: Big Tech and the Politics of Sovereign Authority in the Digital Age. *SSRN*, January 19, 2026. 1–16. <https://doi.org/10.2139/ssrn.6149489> Vö. The Role of Advanced Technology: Reconfiguring the Post-2026 Geopolitical Order. *TRENDS Group*, 26 Dec 2025. <https://tinyurl.com/55ymn923>

¹⁰⁰ Maryanne Kelton – Michael Sullivan – Zac Rogers – Emily Bienvenue – Sian Troath: Virtual sovereignty? Private internet capital, digital platforms and infrastructural power in the United States.

Ebben a konstellációban az MI-fejlesztések még tovább növelhetik a technológiai óriások erejét. A mesterséges intelligencia területén zajló kutatások már nem pusztán üzleti kérdéssé, hanem a geostratégiai versengés eszközeivé váltak. Az Egyesült Államok ebben egészen odáig megy, hogy megpróbál szövetségi rendszereket kiépíteni. Erre példa a *Global Partnership on AI* kezdeményezés,¹⁰¹ amelyben a G7 országok és az Európai Unió vesznek részt. Kína hasonló kísérletet tett a fejlődő országok bevonására a *Digitális Selyemút program*¹⁰² részeként, amelybe afrikai és dél-ázsiai partnereket hívott meg. Ezeket a globálisan zajló folyamatokat az Európai Unió az AI Act szigorú szabályaival próbálhatja meg befolyásolni. Mivel a szabályozás – még ha mintaadó is lehet a világ többi régiója számára – önmagában nem elég az innovációs versenyben, az európai Csiprendelet igyekszik tetemes forrásokat mozgósítani az európai felzárkózásra. Ennek egyik első lépése a Gaia X MI-szolgáltatásai,¹⁰³ illetve az európai GPU-konzorcium terve.¹⁰⁴ A megteremteni kívánt digitális szuverenitás elengedhetetlen kelléke még az Európában keletkező adatok itteni tárolásának megoldása, a saját algoritmusok és európai szabványok fejlesztése. A mesterséges intelligencia tehát a digitális gazdaság és a számítástechnika egyfajta új szent Grálja lett. Aki lemarad a fejlesztésében, az kimarad a nagyhatalmi, geopolitikai versenyből.

7. Összegzés

A fentiekben arra tettem kísérletet, hogy bemutassam a digitális platformgazdaság, a szellemi tulajdonvédelem és a geopolitika kapcsolódási pontjait, amelyek a nagyhatalmi versengést egyre inkább meghatározzák. A legnagyobb technológiai vállalatok gazdasági ereje és adatok feletti monopóliuma mára politikai hatalommá alakult. Ennek szabályozása alapvető stratégiai érdeke minden szuverén államnak és a szoros nemzetközi együttműködésnek. A digitális platformágazat és a mesterséges intelligencia egyúttal a nagyhatalmi versengés egyik elsődleges terepévé váltak. Mind az Egyesült Államok, mind Kína, mind pedig az Európai Unió törekszik az ezek feletti minél

International Affairs, Vol. 98., Issue 6. (2022) 1977–1999. <https://doi.org/10.1093/ia/iia226>

¹⁰¹ Global Partnership on Artificial Intelligence (GPAI) 2020-ban, a G7 országok által alapított nemzetközi szakértői fórum, amelynek célja a mesterséges intelligencia felelősségteljes, az emberi jogokat és demokratikus értékeket tisztelőtben tartó fejlesztése és gyakorlati alkalmazás. E tevékenységét az OECD koordinálja. Ld. Global Partnership on Artificial Intelligence. <https://www.oecd.org/en/about/programmes/global-partnership-on-artificial-intelligence.html>

¹⁰² A Digitális Selyemút programról részletesen ld. Andrew Mazen Dahdal – Adel Abdel Ghafar: The Digital Silk road: „Tech-Diplomacy” as a Paradigm for Understanding Technological Adoption and Emerging Digital Regulations in MENA. *Asian Journal of Law and Society*, Vol. 12. (2025) 163–188. <https://doi.org/10.1017/als.2024.30>

¹⁰³ A Gaia-X egy német-francia kezdeményezésre indult projekt. Célja egy egységes, biztonságos és átlátható európai adat-infrastruktúra felépítése, amely elősegítheti az európai digitális- és adatszuverenitás megteremtését a nagy amerikai és kínai felhőszolgáltatásokkal szemben. Ld. What is Gaia-X. <https://gaia-x.eu/what-is-gaia-x/>.

¹⁰⁴ Az európai cselekvési tervhez részletesen ld. A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. „MI-kontinens” cselekvési terv. Brüsszel, 2025.4.9. COM(2025) 165 final.

szélesebb körű rendelkezési képesség kialakítására és növelésére. Ez szükségessé teszi a platformok politikai gazdaságtanának és jogszabályi hátterének pontos megértését, különösen az olyan területeken, mint a vagyoni értékkel bíró adatok jogi definiálása és szabályozásának kérdése, a jogellenes digitális tartalmak nyilvánossághoz juttatásának problémája, illetve a szellemi oltalmi formák biztosítása.

A platformok, a digitális tér, az adatgazdaság, az információs infrastruktúrák és a mesterséges intelligencia kutatása interdiszciplináris megközelítést követel, amelynek az egyik fontos iránya a geopolitikai-jogi metszéspont megtalálása és feltérképezése kell, hogy legyen. Ennek indoka, hogy mind a technológia, mind pedig az annak regulálására irányuló szabályozás a geopolitikai nagyhatalmi küzdelem részévé vált. Sőt, a szabályozás már nemcsak reakció, hanem egy tudatosan alkalmazott stratégiai eszköz, akár fegyver. Példaként elég, ha csak az Európai Unió *kvázi* exportált szabályozási normáira, vagy a Kína által épített, fentebb említett párhuzamos nemzetközi mechanizmusokra, vagy az Egyesült Államok jogi megoldásainak lopakodó szerződéses exportjára gondolunk. A jogi normák összességén túl pedig az olyan klasszikus, már-már elcsépeelt fogalmak is új értelmet nyernek, mint a szuverenitás és nemzetbiztonság. A digitális korban egy adatközpont, annak energiabiztonsága, vagy egy mesterséges intelligenciát működtető algoritmus ugyanúgy a nagyhatalmi stratégia része lehet, mint egy olajkút, földgázmező, vagy katonai támaszpont.

A digitális gazdaság által életre hívott új kihívásokat pedig integráltan kell vizsgálni. Erre kiváló terepet szolgáltat az USA–Kína–EU hármas, amelyben három különböző attitűd és szabályozási modell találkozik, illetve sok esetben ütközik egymással. Eközben mindhárom szereplő igen tanulékony, el-elcsen megoldásokat, miközben megpróbálja ellensúlyozni a versenytársak lépéseit, erősségeit, egyúttal felzárkóztatni gyengeségeit. Az EU például jelentős, követendő eredményeket ért el a szabályozás terén, viszont tényszerűen le van maradva az innovációban, fejlesztésekben. Az Egyesült Államokban éppen fordított a helyzet. Ott a fejlesztések exponenciális sebességgel zajlanak, miközben a jogszabályi környezet gyakran nem eléggé szofisztikált, kiforrott és szigorú olyan vállalatokkal szemben, amelyek információs monopóliuma mára megkérdőjelezhetetlenné vált. Eközben Kína egyrészt szigorú állami kontroll alatt tartja a digitális teret, másrészt viszont rájött, hogy a túlzott centralizáció és pártállami ellenőrzés lassítja az innovációt. Ezért Peking lehetővé tett némi versenyt a szektorban, ahová piaci ösztönzőket juttat.

Fontos további tanulság, hogy a jog hagyományos ágai a digitális térben összemosódnak. Az adatvédelem és a szellemi tulajdonvédelem összefügg a versenyjoggal, hiszen a platformok monopol helyzete az adatvagyonon és a felhasznált szerzői műveken és kapcsolódó jogi teljesítményeken alapul.¹⁰⁵ A szerzői jog egybe csúszik a platformszabályozással, mivel a tartalommoderáció egyszerre érinti a szabad véleménynyilvánításhoz való jogot, illetve a védett tartalmak hozzáférhetővé tételéből fakadó felelősséget. A platformok vizsgálata tehát nem merülhet ki a technológiai, piaci vagy jogi kérdések taglalásában. A geopolitikai megközelítés rávilágít arra, hogy a digitális tér-

¹⁰⁵ Szabó Endre Győző: A kétoldalú piacok elmélete és a személyes adatok védelme – A Google-ítélet elemzése versenyjogi és adatvédelmi szempontok szerint. In *Medias Res*, 2017/1. 172.

ben folyó küzdelem végeredményben a nagyhatalmi átrendeződésről is szól. Aki uralja az információt, formálni képes a diskurzust és hasznot tud húzni az innovációból. Az adat- és platformgazdaság, valamint a mesterséges intelligencia fejlődése mára döntő geopolitikai tényezővé vált, a globális versengés pedig az előttünk álló években várhatóan tovább éleződik. Ahhoz, hogy e folyamatokról teljes képet kaphassunk, a szabályozási környezetet is geopolitikai fénytörésben kell vizsgálnunk, hiszen a modern digitális platformok kétoldalú piakai éppen az állami érdekek, a jogrendszerek és a globális hatalmi törekvések ütközőzónájában formálódnak.

A tanulmány központi kérdése azon hipotézis köré épült, hogy az Európai Unió szabályozói eszköztára – különösen a DMA, a DSA és az AI Act – képes-e jogi eszközökkel ellensúlyozni a technológiai és innovációs lemaradást a globális platformgazdaságban. A vizsgálat során alkalmazott interdiszciplináris megközelítés igazolta a feltételezést, miszerint a szellemi alkotások joga és a digitális piacok szabályozása mára túllépett a klasszikus jogtechnikai kereteken, és az uniós „szabályozási hatalom” (*regulatory power*) stratégiai eszközévé vált. A kutatás során elvégzett hárompólusú (USA–Kína–EU) összehasonlító elemzés célja nem csupán a modellek ismertetése volt, hanem annak bizonyítása, hogy a digitális gazdaság a „fegyverré tett kölcsönös függőség” (*weaponized interdependence*) korszakába lépett. Míg az Egyesült Államok a piaci dominanciára és az innovációs előnyre, Kína pedig az állami kontrollra és az adatbőségre alapozza befolyását, az Európai Unió a jogalkotást használja fel geopolitikai ellensúlyként. A tanulmány rávilágított, hogy az EU a *hálózati fojtóponatok* (*chokepoints*) feletti kontrollt a „Brüsszel-hatás” révén, vagyis a szigorú normák globális exportjával igyekszik érvényesíteni, kényszerpályát jelölve ki a tengerentúli technológiai óriások számára.

A szigorú normatív környezet kialakítása és fenntartása csak addig lehet hatékony, amíg az uniós piac mérete és vásárlóereje megkerülhetetlen marad. Amennyiben ez a szigor nem párosul az európai technológiai bázis (Gaia-X, a csipgyártás) megerősítésével, Európa könnyen egyfajta „szabályozó múzeummá” válhat, amely bár megvédi polgárai jogait, elveszíti befolyását a technológia jövőben alakítása felett. Márpedig a jövő nagyhatalmi átrendeződését nem a fizikai határok, hanem a digitális csomópontok feletti kontroll fogja meghatározni. Az ezekért való küzdelemben az Európai Unió egyetlen esélye a stratégiai autonómia megteremtése és megőrzése, amely a szigorú normatív környezet mellé valódi technológiai szuverenitást teremt.

