

Tóth András

AZ EU DIGITÁLIS ÉS TECHNOLÓGIAI SZABÁLYOZÁSA AZ EU JOGI IDENTITÁSA ÉS A GLOBÁLIS KIHÍVÁSOK HÁLÓJÁBAN

EU Digital and Technology Regulation in the Context of the EU's Legal Identity and Global Challenges

Dr. habil. Tóth András tanszékvezető habilitált egyetemi docens, Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar Magánjogi Tudományok Intézete Digitális és Technológia Jogi Tanszék; elnökhelyettes, Gazdasági Versenyhivatal; elnök, Versenytanács, toth.andras@gvh.hu

A tanulmány az EU digitális és technológiaszabályozását az EU jogi identitása és a globális verseny tükrében vizsgálja. A tanulmány fő állítása szerint az európai digitális szabályozás a fokozódó globális kereskedelmi és technológiai versenyben nem pusztán normatív keret, hanem geoökonómiai eszköz is. A tanulmány amellet érvel, hogy a digitalizáció kihívásai és az európai jog integrációja egy többtényezős struktúrában kapcsolódnak össze. A jog az Európai Unió számára nem csupán szabályozási technika, hanem az európai kulturális örökségen alapuló közös identitás konstitutív eleme. Ezzel párhuzamosan a digitális technológiai fejlődés globális, geostratégiai dimenziót nyert, amely az államok közötti verseny egyik meghatározó terepévé vált. Az EU e kihívásokra adott válasza szükségszerűen jogközpontú, ami részben a technológiai kiszolgáltatottságból fakadó védekező reflexként értelmezhető. A tanulmány bemutatja, hogy e védekező szabályozási dinamika visszacsatolás révén geoökonómiai hatalommá alakul, mivel az EU globálisan meghatározó piacának köszönhetően a szabályozás extraterritoriális hatást fejt ki. Ennek következtében az uniós digitális joganyag geopolitikai kontextusban akár kvázi-kereskedelmi eszközként is értelmezhető. A várható jogalkotási irányok elemzése arra utal, hogy rövid távon nem prognosztizálható koncepcionális fordulat: az új szabályozási csomagok a meglévő, erősen szabályozásvezérelt modell finomhangolását jelentik, amelyet az EU szerkezeti és szuverenitási adottságai tartósan konzerválnak.

KULCSSZAVAK:

EU, digitális átalakulás, digitális szabályozás, omnibusz

This study examines the digital and technology regulation of the European Union (EU) in light of the EU's legal identity and global competition. The main thesis of the study is that European digital regulation is not just a normative framework in the context of increasing global trade and technological competition, but also a geo-economic tool. The study argues that the challenges of digitalisation and the integration of European law are linked in a multi-factor structure. For the European Union, the law is not just a regulatory technique, but a constitutive element of a common identity based on European cultural heritage. At parallel with this, the development of the digital technology has gained a global, geostrategic dimension, which has become one of the defining fields of competition between states. The EU's response to these challenges is necessarily law-based, which can be interpreted in part as a defensive reflex arising from technological vulnerability. The study demonstrates that this defensive regulatory dynamic transforms into geo-economic power through feedback, as thanks to the EU's globally dominant market, the regulation exerts extraterritorial influence. As a result, EU digital legislation can even be interpreted as a quasi-commercial tool in a geopolitical context. An analysis of expected legislative trends suggests that no conceptual shift is foreseeable in the short term: the new regulatory packages represent a fine-tuning of the existing, heavily regulation-driven model, which is permanently preserved by the structural and sovereignty characteristics of the EU.

KEYWORDS:

EU, digital transformation, digital regulation, omnibus

BEVEZETÉS

A digitalizáció egy átfogó társadalmi, gazdasági folyamat, amelynek részeként az emberi élet egyre több aspektusa kerül „adatosításra”, és ezzel szoros összefüggésben az online térbe is. Mint folyamat, lehet jogvezérelt is, de nem feltétlenül. Az Európai Unióban (EU) például az, míg az Egyesült Államokban (USA) a jog inkább követő jellegű szerepet játszik. Az, hogy az EU-ban a digitalizáció jogvezérelt, azt jelenti, hogy az adatok és az adatokat kezelő, feldolgozó technológiák szabályozási célpontok lesznek. Az EU-ban a digitalizáció és benne a digitális technológiák jogvezéreltsége két okkal magyarázható: egyrészt az EU jogi természetű identitásával, amely szerint az EU eleve egyenlő a joggal/szabályozással (egyéb közös identitás híján), tehát az EU-t érő kihívásokra alapvetően a joggal vagy a jog eszközei által is válaszolni fog. A másik ok pedig ezzel szoros összefüggésben a digitalizációs globális szuverenitási kihívásaival kapcsolatos, amelyek miatt az EU-szabályozás egyfajta védekezőreflex-karaktert is kap.

A digitalizációnak megvannak a technológiái: ezek a digitális technológiák. Közülük kiemelkednek azok, amelyek alapvetőek a digitális társadalom és gazdaság működése szempontjából: ezek a digitális infrastruktúrák (például felhő, elektronikus hírközlés, adatközpontok, mesterséges intelligencia, azaz *artificial intelligence*, a továbbiakban: AI). Az EU szabályozási gyakorlatában a digitalizáció folyamatvezérelt és technológiaspecifikus megközelítése szorosan összefügg, nem feltétlenül választhatók el egymástól következetesen.

Ma a technológiai fejlődés, amely mindig is az emberi civilizáció velejárója volt,¹ szerve-
sen összekapcsolódik a globális fejleményekkel,² amelyeket többek között a nagyhatalmak
közötti verseny fokozódása jellemez. Ennek oka az USA elmúlt évtizedekben élvezett domi-
nanciájának megszűnése, és ezzel szoros összefüggésben az, hogy Kína vele összemérhető,
világméretű tényezővé válik.³ A technológia ma már a geopolitikai versengés egyik legfonto-
sabb területe, és a kritikus technológiák, például a mesterséges intelligencia feletti ellenőrzés
a globális állami érvényesülés forrásának tekinthető.⁴ Ezt figyelembe véve a digitalizáció és
digitális technológiák az EU-ban a szabályozással összefonódva még erős szuverenitásvédelmi
karaktert is kapnak.⁵ Jelen tanulmány célja tehát az EU digitális technológiai szabályozásának
a fentiek szerinti, kontextusközpontú bemutatása, és az ebből való következtetések levonása.
Ennek érdekében áttekinti a digitalizáció és digitális technológiai fejlődés globális tájképét,
benne Európával, bemutatja az EU jogvezérelt megközelítésének okait és következményeit,
különösen is kitérve a legújabb európai szabályozási fejleményekre.

EURÓPA HELYZETÉNEK ÁTTEKINTÉSE A GLOBÁLIS TECHNOLÓGIAI VERSENYBEN

Az ENSZ adatai szerint a globális adatalapú gazdaság magasan koncentrált, a legnagyobb
online platformok piaci kapitalizációja alapján az amerikai és kínai cégek együttesen 90%-ot
tesznek ki.⁶ A világ 50 vezető technológiai vállalatából csak négy európai.⁷ A felhőben tárolt
európai adatok 70%-át amerikai vállalatok kezelik,⁸ miközben a felhő jelentősége az AI és
a folyamatos adatbővülés igényeit figyelembe véve egyre nő. Az USA és Kína is (együtt 88%)
megelőzi az Európai Uniót (7%) a mesterséges intelligenciába mint a jövő technológiájába
való beruházás terén is.⁹ Az alapvető AI-modellek 73%-át az Egyesült Államokban, 15%-át
pedig Kínában fejlesztik ki.¹⁰ Az amerikai Google dominálja az EU-ban a keresőmotorok és
a mobiltelefonok operációs rendszereinek piacát, a Facebook pedig meghatározó a közös-
ségi média területén.¹¹ A világ mikrochipjeinek körülbelül 20%-át Európa fogyasztja, de csak
9%-ukat gyártják ott.¹² Európa digitális infrastruktúrájának és technológiáinak több mint
80%-a importból származik.¹³

¹ SHAFIQUE 2016: 4.

² WU 2020: 100.

³ The White House 2022: 6, 8, 32.

⁴ WU 2020: 101–102.

⁵ European Commission 2020a.

⁶ United Nations Conference on Trade and Development 2021.

⁷ BRIA–TIMMERS–GERNONE 2025: 12.

⁸ Cloud Market Gets its Mojo Back; AI Helps Push Q4 Increase in Cloud Spending to New Highs 2024.

⁹ MADIEGA–ILNICKI 2024.

¹⁰ MADIEGA–ILNICKI 2024.

¹¹ European Commission 2020b.

¹² BRIA–TIMMERS–GERNONE 2025: 11.

¹³ BRIA–TIMMERS–GERNONE 2025: 8. Lásd még European Parliament 2026.

Ha a mesterséges intelligencia és digitális gazdaság legfontosabb alapanyagát, az adatokat nézzük,¹⁴ akkor megállapítható, hogy az európai adatok 92%-át az USA-ban kezelik. A Draghi-jelentés szerint az „adatértékesztés” (azaz az EU-ból harmadik országokba továbbított adatok mennyisége) ma 90%-ra becsülhető.¹⁵ Ezekhez az európai adatokhoz az amerikai kormányzati szervezetek is hozzáférésük lehet.¹⁶ A 2018-ban elfogadott, az adatok törvényes külföldi felhasználását tisztázó amerikai törvény (CLOUD) ugyanis felhatalmazza az amerikai bűnüldöző szerveket, hogy hozzáférjenek az amerikai vállalatok által kezelt adatokhoz, függetlenül attól, hogy azok belföldön vagy külföldön vannak-e tárolva. Az Európai Bizottság (a továbbiakban: Bizottság) szerint túl sok európai vállalat küzd azért, hogy hozzáférjen a szükséges adatokhoz, míg a nagy külföldi technológiai vállalatok az európai adatokat használják fel üzleti tevékenységük előmozdítására.¹⁷ Az európai adatvagyon USA-ba vándorlása többek között az AI kifejlesztése és felhasználása terén folytatott nagy nemzetközi versenyfutásban is károsnak bizonyult.¹⁸ Érdekes, hogy ez az érv az amerikai adatlokalizációs előírásokban is megjelent.¹⁹ Az adatok ugyanis mennyiségi és minőségi szempontból is meghatározók az AI működése szempontjából.²⁰ A 2025-ös Adatuniós Stratégia szerint is

„[a]z EU-nak nagy mennyiségű, kiváló minőségű adatra van szüksége a versenyképességhez és az innováció előmozdításához. Ilyen adatok nélkül az EU nem tud erős mesterségesintelligencia-modelleket építeni [...] Az EU a mesterséges intelligencia fejlesztéséhez szükséges adatok hiányával, valamint a növekvő geopolitikai versennyel néz szembe, ahol az adatokat egyre inkább stratégiai eszköznek tekintik.”²¹

Így hát, ha az adat az új olaj,²² akkor természetesen, aki birtokolja, az jelentős hatalmat tudhat a magáénak.²³ Kína az adatvagyonát lényegében nemzeti stratégiai értéknek tekinti, teljes állami felügyelet érvényesül ezen a téren. Az ázsiai nagyhatalom megközelítése az adatszuverenitáson alapul, ezért előírja, hogy bizonyos adatkategóriákat Kínában kell tárolni.²⁴ Az érzékeny adatok bármilyen határokon átnyúló továbbítása kormányzati jóváhagyást

¹⁴ European Data Protection Supervisor 2016.

¹⁵ DRAGHI 2024a: 67.

¹⁶ Lásd STOLTON 2021; FLEMING 2025.

¹⁷ VON DER LEYEN 2024.

¹⁸ TÓTH 2020: 3–9; European Commission 2018.

¹⁹ PITTMAN et al. 2025.

²⁰ Az AI megbízható működése szempontjából kritikus, hogy az adatok teljes körűek és relevánsak legyenek, különben fennáll az emberi jogok sérülésének veszélye (diszkrimináció, egészség). Lásd European Commission 2020c.

²¹ European Commission 2025a.

²² Lásd The Economist 2017.

²³ Lásd CANDELON–REEVES 2017.

²⁴ Lásd Kína adatvédelmi intézkedéseit: Data Security Law (DSL), azaz Adatvédelmi törvény; Cybersecurity Law (CSL), azaz Kiberbiztonsági törvény, amely a kritikus információs infrastruktúra üzemeltetőire (*Critical Information Infrastructure Operators*, CIIOs) vonatkozik; Personal Information Protection Law (PIPL), azaz A személyes adatok védelméről szóló törvény.

igénnyel biztonsági értékelések, tanúsítások vagy szabványosított szerződések formájában.²⁵ Az USA – miközben szintén stratégiailag kezeli a maga adatvagyonát – nagyon hatékony az európai adatvagyon kiaknázásában, miként azt a Bizottság is a fentiek szerint elismerte. 2024. február 28-án Joe Biden elnök kiadta az 14117. számú végrehajtási rendeletet,²⁶ amely korlátozásokat vezetett be az amerikai személyes adatoknak a kijelölt „problémás országokba” (Kína – beleértve Hongkongot és Makaót –, Oroszország, Irán, Észak-Korea, Kuba, Venezuela) történő továbbítására vonatkozóan. Ezt a végrehajtói intézkedést követte az Igazságügyi Minisztérium 2024. decemberi szabályozása,²⁷ amely átfogó keretet hozott létre az érzékeny amerikai adatokhoz való külföldi hozzáférés által jelentett nemzetbiztonsági fenyegetés kezelésére. A 2025-ös Adatuniós Stratégia szeretné orvosolni a jelenlegi egyensúlytalanságokat, amelyek miatt az EU adatai megfelelő biztosítékok nélkül kerülnek külföldre.

Az Európai Unió 2020-ban elfogadott korábbi adatstratégiája is már kifejezetten elismeri, hogy „[j]elenleg a világ adatainak nagy részét néhány technológiai nagyvállalat birtokolja. Ez visszafoghatja az adatvezérelt vállalkozások megjelenését, növekedését és innovációját az EU-ban”.²⁸ Az uniós polgárok és vállalkozások adataihoz olyan harmadik országbeli joghatóságok férnek hozzá, amelyek nincsenek feltétlenül összhangban az EU adatvédelmi keretével.²⁹ Az Európai Bíróság 2020 júliusában hozott ítélete³⁰ is megerősíti ezeket az aggodalmakat. A technológiával rendelkező államok hazai technológiai iparágukat felhasználva befolyásolják és alakítják a kialakulóban lévő globális normákat, kihasználva az adatok és a digitális technológia nyújtotta erejüket a belső bürokráciájuk és a nemzetbiztonsági rendszereik támogatására.³¹ Ezt a következtetést Donald Trump elnök 2025-ös davos-i beszéde is megerősíti. Kritizálta az Európai Unió szabályozási intézkedéseit az olyan nagy amerikai technológiai vállalatok, mint az Apple, a Google és a Meta ellen. Az EU által kiszabott jelentős bírságokat az „adózás egyik formájának” nevezte, és azzal vádolta az EU-t, hogy „nagyon, nagyon igazságtalanul” bánik az amerikai techcégekkel.³² A párizsi AI-csúcstalálkozón (2025. február 11.) az amerikai alelnök, J.D. Vance kifejezetten figyelmeztette az európai vezetőket, hogy az EU-szerű szigorú szabályok visszafoghatják a befektetéseket és az innovációt a mesterséges intelligencia területén: „az AI-szektor túlzott szabályozása megölhet egy átalakulóban lévő iparágat, éppen akkor, amikor az felívelőben van”, és „növekedésbarát” (deregulációs) AI-politikát szorgalmazott. Szerinte „új ipari forradalom” „soha nem fog bekövetkezni, ha a túlzott szabályozás visszatartja az innovátorokat a szükséges kockázatok vállalásától”. Miután a Bizottság 2025. december 5-én 120 millió euró bírságot szabott ki Elon Musk vállalatára, az X-re a DSA megsértése miatt, Washington figyelmeztetett, hogy kereskedelmi eszközöket vethet be, beleértve az európai szolgáltatókra kiszabott díjakat vagy korlátozásokat is, tekintve, hogy az EU eljárásai diszkriminatív módon

²⁵ WALTER 2024.

²⁶ Federal Register 2024.

²⁷ Department of Justice 2024.

²⁸ European Commission 2020d.

²⁹ European Commission 2020d: 10.

³⁰ Bővebben lásd C-311/18. sz. Data Protection Commissioner kontra Facebook Ireland Limited és Maximillian Schrems ügyben 2020. július 16-án hozott ítélet (ECLI:EU:C:2020:559).

³¹ MCBRIDE 2025.

³² DOAN-STOLTON 2025.

vonatkoznak a nagy amerikai technológiai vállalatokra. Az USA Külügyminisztériuma pedig elkezdte alkalmazni az új vízumkorlátozási politikát (amelyet 2025 májusában jelentettek be), és öt európaít – köztük az EU korábbi digitális területért felelős biztosát, Thierry Bretont is – kitiltott, azzal vádolva őket, hogy nyomást gyakorolnak az amerikai technológiai vállalatokra, cenzúrázzák azokat. Ezt a lépést az Európai Parlament határozatban ítélte el.³³

Ebben az összefüggésben az európai digitális szabályozás (amely alapvetően védekező alaplásból fejlődik) a fokozódó nemzetközi kereskedelemi versenyben fegyvernek minősülhet.³⁴ (Lásd az EU-s szabályozás globális kisugárzó hatását, a *Brüsszel-hatást*.)³⁵ Nem kivételes az, ami történik, nevezetesen, hogy az EU szabályozása geopolitikai kontextusba kerül. Például az EU versenyszabályozását a második világháború után a győztes amerikaiak kényszerítették ki, miután a szövetségesek meggyőződése volt, hogy a pusztítás egyik fő erőforrását a központosított német gazdaság képezte, ezért a béketeremtés egyik fő iránya is ennek felszámolására irányult.³⁶ Később az ilyen előzmények után elfogadott európai versenyszabályozást az EU éppen az amerikai vállalatok monopolizálási törekvéseivel szemben használta fel.³⁷

EURÓPA SZABÁLYOZÁS-KÖZPONTÚ MEGKÖZELÍTÉSÉNEK OKAI ÉS KÖVETKEZMÉNYEI

Miként a bevezetőben erről már szó volt, a digitalizáció kihívása és a jog európai összefonódása egy többtényezős keplet eredménye.

Egyfelől a jog nemcsak módszer az EU számára, hanem az európai kulturális örökségen alapuló közös identitás alapvető összetevőjét is adja.³⁸ Vagyis bár az Európai Unió korai alapjai elsősorban gazdasági jellegűek voltak, az identitás kérdése mindig is jelen volt mind az európai integráció céljaként, mind pedig legitimációjaként.³⁹ A jog – a kontinensen betöltött történelmi-filozófiai szerepéből fakadóan – ez utóbbiban (nevezetesen az európai projekt identitásképzésében) kulcsszerepet játszott.⁴⁰ Ezt a jogi identitást konkrétan a digitalizációra vonatkoztatva lehet tetten érni, mivel az EU-ban a digitalizációs és digitális technológiai fejlődés jelentette kihívások szükségszerűen markáns jogi válaszokat is indukáltak.

³³ European Parliament 2026: 4. pont.

³⁴ MALINGRE 2025; ADRAGNA 2025.

³⁵ LESLIE 2023.

³⁶ TEPPER–HEARN 2018: 151.

³⁷ 1997-ben az EU először megtiltotta a Boeing és a McDonnell Douglas összefonódását, amire válaszul az USA protekcionizmussal vádolta az EU-t, hogy az Airbus védelmében avatkozott be. 2001-ben az EU pedig megtiltotta, hogy az amerikai General Electric felvásárolja a Honeywellt. A Microsofttal szembeni erőfölénnyel való visszaéléses ügyeket is másként kezelték az óceán két partján: az USA-ban a kormánnyal kötött megállapodással zárult az ügy, az EU-ban pedig összességében 1,6 milliárd euró bírságot szabtak ki a cégre a 2000-es években.

³⁸ MARTONYI 2019: 227.

³⁹ PŘIBÁŇ 2007: 115.

⁴⁰ TÓTH 2025: 234–235.

Másfelől a digitalizáció és az azzal együtt járó, az azt kísérő technológiai fejlődés globális jelenségként geostratégiai kérdéssé is vált az államok között kibontakozó versenyben. Az EU részéről a digitalizációból fakadó kihívásokra adandó geostratégiai válasz – már csak a fentiek szerinti jogi identitásának köszönhetően is – szoros összefüggésbe került, szorosan összefonódott a jogi szabályozással, ugyanis az Európai Unió markáns szabályozási válasszal felel a digitalizáció globális kihívásaira is. Ahogy Di Marco és társai is megállapítják, az EU ereje történelmileg a szabályozási és normatív befolyásában rejlik, és hatékonysága azon képességétől függ, hogy alakítsa azokat a – technológiai, szabályozási és intézményi – kereteket, amelyekben keresztül a digitális rendszerek működnek.⁴¹ Tekintettel arra, hogy a digitális technológia frontján a fentiek értelmében globálisan kiszolgáltatott helyzetben van, a szabályozás az EU védekező reflexének eszközévé is vált a globális térben. Az EU digitális szabályozási cunamija ennek fényében már akár a védekező reflex „lázás” tünetének is tekinthető.

Harmadrészt ezzel szoros összefüggésben megfigyelhető egyfajta visszacsatolás is, nevezetesen, hogy a globális kihívásokra fentiek szerint születő európai szabályozási védekező reflex egyúttal az EU világméretű és nem megkerülhető piaca⁴² miatt az EU szabályozásának geoökonomiai erőt (Brüsszel-hatás) kölcsönöz.⁴³ Ennek köszönhetően viszont az EU-szabályozás – és benne többek között az EU AIA⁴⁴ – geopolitikai kontextusba kerül, és ennek jegyében minősülhet például vámnak is.⁴⁵

Fenti három tényező közül a második (a szabályozás mint az EU védekező reflexe a globális digitális technológiai versenyben) kapcsán érdemes kicsit részletesebben kitérni a szuverenitás és a digitalizáció összefüggéseire, illetve a jog/szabályozás szerepére bennük.

Európa legfőbb kihívása a technológiai függés csökkentése az USA-tól és Kínától.⁴⁶ A kritikus digitális infrastruktúra külső szolgáltatóktól való függőségének csökkentése érdekében határozott lépéseket kell tennie versenyképességének és stratégiai autonómiájának biztosítása érdekében.⁴⁷ Ezért az EU digitális technológiai szuverenitása kulcskérdés.⁴⁸ Általában az európai szuverenitás „az a képesség, hogy kapacitást, rezilienciát és biztonságot építsünk ki a stratégiai függőségek csökkentésével, a külföldi szereplőktől és egyetlen szolgáltatótól való függőség megelőzésével, valamint a kritikus technológiák és infrastruktúrák védelmével.”⁴⁹ A 2025-ös Adatuniós Stratégia szerint a szuverenitás védelme az EU ellenálló képességének védelmét is jelenti.⁵⁰

⁴¹ DI MARCO et al. 2025: 2.

⁴² „[B]ecause the EU is, at its core, a market, it may be best to conceive of the EU as a Market Power Europe (MPE).” DAMRO 2012: 682–683.

⁴³ MAHER 2024: 395–410.

⁴⁴ CAULCLUTT 2025.

⁴⁵ MALINGRE 2025.

⁴⁶ Lásd KOMAITIS–SHERMAN 2021; MADIEGA 2020; LARSEN 2022.

⁴⁷ BRIA–TIMMERS–GERNONE 2025: 13.

⁴⁸ POHLE–THIEL 2020; FLEMING 2025.

⁴⁹ European Parliament 2026: 1. pont.

⁵⁰ European Commission 2025a. Lásd The Economist 2017.

A digitális szuverenitás a digitális átállásnak mint folyamatnak stratégiai, önálló uralását jelenti, amikor adott állam a folyamatot saját államérdekei és értékei mentén⁵¹ kézben tartja, alakítja. Ennek lehet egyik eszköze a jog, de nem feltétlenül. Például, hogy az adatok stratégiai értéket képviselnek, a digitális készségek rendelkezésre állnak,⁵² a nemzeti vállalatok a digitális térben erősek – ezek digitális szuverenitási kérdések. A digitális szuverenitás szempontjából tehát az is jelentős, ha az európai uniós polgárok és vállalkozások adataihoz olyan harmadik országbeli joghatóságok férnek hozzá, amelyek nincsenek összhangban az EU adatvédelmi keretével.⁵³ Érdekes módon az Európai Parlament dokumentuma ezt fajta az adatkitettséget (európai adatok külföldi kizsákmányolását) nem említi, lehetségesen azért, mert a technológiai szuverenítésra koncentrál.⁵⁴

A digitális technológiai szuverenitás pedig azt jelenti, hogy maguk a technológiák működése és rendelkezésre állása biztosítja az állami autonómiát, illetve támogatja magát az értékvezérelt digitalizációs folyamatot. Például az adatokat kezelő technológiák (felhő, AI, adatközpontok) nemzeti kontroll alatt maradnak. Az, hogy az EU mennyire van ráutalva más országok digitális technológiáira, a digitális technológiai szuverenitás kérdése. Az EP szerint a technológiai szuverenitás

„az a képesség, hogy megtervezzük, kifejlesszük és kiterjesszük a gazdaságunk versenyképességéhez, polgáraink jólétéhez és az EU nyitott stratégiai autonómiájához szükséges digitális technológiákat a globalizált világban; ez magába foglalja az EU autonóm döntéshozatali képességének biztosítását, a megbízható, nem uniós országokkal és szervezetekkel való együttműködést, az ellátási láncok diverzifikálását és megerősítését, valamint a nyitottság és az interoperabilitás koncepciójának előmozdítását annak biztosítása érdekében, hogy Európa továbbra is vonzó befektetési központ maradjon”.⁵⁵

A technológiai szuverenítésnek tehát van néhány kulcsjellemzője: az EU arra vonatkozó képessége, hogy az uniós polgárok és az uniós vállalkozások jólétéhez szükséges kritikus technológiákat kifejlessze, védje, valamint a globalizált környezetben önálló cselekvésre és döntéshozatalra legyen képes.⁵⁶ Az Európai Parlament szerint az EU technológiai szuverenitása „nagyban függ attól, hogy Európa képes-e megteremteni azokat a piaci feltételeket, amelyek szükségesek ahhoz, hogy az európai vállalatok virágozhassanak és egymással versenyezzenek, ezáltal javítva termékeik minőségét”.⁵⁷ Ennek fényében technológiai szuverenitási kérdés az is, hogy a piaci feltételek lehetővé tegyék, hogy az európai cégek a technológia terén

⁵¹ Lásd European Commission 2020d: 3.

⁵² Council of the European Union 2024: 5.

⁵³ European Commission 2020d: 10; MADIEGA 2020: 1.

⁵⁴ Ellenben annak helytől független EU-szabályok szerint kezelését említi. Lásd European Parliament 2016: 21. pont.

⁵⁵ European Parliament 2026: 2. pont.

⁵⁶ RAMAHANDRY et al. 2021.

⁵⁷ European Parliament 2026: D) pont.

meghatározóvá váljanak.⁵⁸ Ezt én a fentiek szerint inkább digitális szuverenitási kérdésnek minősíteném, de mindez inkább a két kategória szoros összefüggését mutatja.

Az Európai Parlament szerint szuverenitási kérdés a digitális közinfrastruktúra (DPI) is,

„amely monopóliumok kialakulásához és külföldi szereplőktől való függőséghez vezetett; hangsúlyozza, hogy e hiányosság pótlására az EU-nak vezető szerepet kell vállalnia a DPI szilárd alapjainak megteremtésében azáltal, hogy félvezetőkből, csatlakozási megoldásokból, felhőalapú infrastruktúrából, szoftverekből, adatokból és mesterséges intelligenciából álló digitális technológiai rétegeket hoz létre”.⁵⁹

A digitális technológiai rétegen (félvezetők, adat, AI, felhő) kívül az EP szerint még van egy kritikus digitális infrastruktúra, amely magában foglalja a kábeleket (szárazföldi és tenger alatti), a mobilhálózatokat, a műholdas kommunikációs rendszereket, a spektrumot és a rádióberendezéseket, az érzékeny információkat tartalmazó felhőszervereket és az érzékeny információkat feldolgozó adatközpontokat.⁶⁰ A digitális infrastruktúra (beleértve az adatközpontokat, a felhőalapú platformokat, a félvezetőket, a szoftveres ökoszisztémákat és a mesterséges intelligenciát) piacait azonban néhány nem európai vállalat uralja (különösen a felhőalapú infrastruktúra, a félvezetők és az AI-platformok terén). Ez az erőegyensúly-hiány azonban gátolja Európa innovációs, versenyképességi és digitális gazdaságának ellenőrzési képességét.⁶¹ Az EU részéről nagyon markáns jelenség, hogy a digitális technológiai szuverenitás elérésében a jogra és szabályozásra támaszkodik.⁶²

Mások lehetnek a hangsúlyok az innovációs verseny frontján (USA–Kína), ahol például a szabályozásnak légiessnek kell lennie, mint azokban a régiókban, amelyeknek a kizsákmányolás ellen kell védekezniük.⁶³ Az amerikai hozzáállás alapján is látszik, hogy az innováció és a (jogilag) kötött pálya nehezen fér össze egymással.⁶⁴ Ez a jogi kényszerspálya már önmagában az innováció hiányának tünete, de másfelől felmerül, hogy annak további korlátja is. Érdekes módon a Draghi- és Letta-jelentések inkább ez utóbbival foglalkoznak, bár a Draghi-jelentésben vannak arra utaló jelek, hogy észlelték a maguk és az USA innovációs attitűdje között húzódó szakadékot, amelyet az EU jogi identitása okoz. A szabályozás költségét kezeletlenül a vállalatok maguk is beruházási költségként azonosítják,⁶⁵ amely hátrányosan érinti

⁵⁸ Lásd a szakirodalomban az EU digitális szabályozásának EU-cégek helyzetbe hozásával való összekapcsolását: „hope to redistribute technological and economic power from non-European to European companies”. YASAR 2025.

⁵⁹ European Parliament 2026: 13. pont.

⁶⁰ European Parliament 2026: 24. pont.

⁶¹ BRIA–TIMMERS–GERNONE 2025: 42.

⁶² MADIEGA 2020: 5; HULKÓ–KÁLMÁN–LAPSÁNSZKY 2025: 2.

⁶³ ELBAUM–SEGAL 2025.

⁶⁴ Lásd THIERER 2016.

⁶⁵ „Regulation is seen by more than 60% of EU companies as an obstacle to investment.” DRAGHI 2025: 18.

az EU nemzetközi versenyképességét.⁶⁶ Hozzá kell tenni azonban, hogy a megfelelési költségek egy része olyan szabályozásokból származik, amelyek elsősorban a nem európai vállalatokat érintik (például DMA, DSA, AIA). A Bizottság hatásvizsgálata arra a következtetésre jut, hogy az AI Act az összes AI-kiadást további 17%-kal megemeli. 2025-re az AI Act több mint 30 milliárd euróba fog kerülni az európai gazdaságnak.⁶⁷

A Draghi-jelentés⁶⁸ több okot is megemlít az erős európai technológiai szektor hiányára (az innovációk kereskedelmi hasznosításának kudarca,⁶⁹ a koordinált beruházások hiánya,⁷⁰ az európai kockázati tőke,⁷¹ illetve, hogy az európai K+F területén az első három legnagyobb szereplő autópári – ugyanez volt a helyzet az Egyesült Államokban a 2000-es évek elején, ahol ma az első három helyen technológiai szereplő található). Ezek az okok mind arra utalnak, hogy nem a vállalatok méretével van feltétlen probléma, hanem a kockázatt vállaló attitűddel. A Draghi-jelentés többek között méretproblémaként azonosítja az európai cégek versenyképességének hiányát. Ennél azonban sokkal fontosabb lehet az innovatív és kockázatt vállaló attitűd. Ezzel kapcsolatban persze felmerülhet, hogy a nagyobb verseny magasabb szintű innovációt hoz és növeli a termelékenységet.⁷² Viszont akkor az európai vállalatoknak innovatívabbnak kellene lenniük az amerikaiaknál, mert az öreg kontinens versenymutatói jobbak az USA-beliéknél, ami erősebb versenyre utal: Európában a profitfelárak jelentősen alacsonyabbak, mint az Egyesült Államokban,⁷³ ezenkívül itt nem tapasztalható az amott megfigyelt extrém piaci koncentráció.⁷⁴ Bár az európai verseny erősebb, mint az amerikai, a legnagyobb technológiai vállalatok között mégis kevés európai cég található. Talán éppen azért az, mert a kockázatt vállaló attitűd jellemzőbb az USA-ra, ami magyarázhatja az európai innovátorok tengerentúlra vándorlását. Nem véletlen, hogy a Szilícium-völgy meghatározó technológiai vezéregyéniségei európai (történetesen német) származásúak: Sam Altman, Peter Thiel.

⁶⁶ Nem véletlen, hogy a Budapesti nyilatkozat ezeknek a szabályozásból eredő terheknek a 25%-os csökkentését szorgalmazza. European Council 2024. Lásd továbbá European Commission 2025b; European Commission 2025c.

⁶⁷ „The Commission's impact assessment concludes that the [AI Act] will cause an additional 17% of overhead on all AI spending. By 2025, the [AI Act] will have cost the European economy more than €30 billion.” MUELLER 2021: 7. Idézi LAURER–REDA–YEUNG 2021.

⁶⁸ Angolul: *Draghi Report*. Széles körben hivatkozott megnevezése: *Draghi Report on EU competitiveness* (Draghi-jelentés az EU versenyképességéről). DRAGHI 2025; DRAGHI 2024b.

⁶⁹ DRAGHI 2024a.

⁷⁰ „In fact, there is no EU company with a market capitalisation over EUR 100 billion that has been set up from scratch in the last fifty years, while in the United States all six companies with a market capitalisation of more than €1 trillion have been created in that period.” DRAGHI 2025: 24.

⁷¹ Számos gyorsan növekvő uniós vállalat az amerikai kockázati tőkéből próbál finanszírozást szerezni, és az amerikai piacon kíván terjeszkedni. DRAGHI 2025: 29. Ennek oka, hogy az EU-ban az USA-hoz képest 80%-os hiány van a kockázati tőke terén. DRAGHI 2025: 25.

⁷² Azokon az online piacokon, ahol a kereskedelem átláthatóbb, és a verseny kieleztettebb, az inflációs ráta nem olyan magas, mint az offline piacokon. DEDOLA et al. 2023: 27.

⁷³ European Commission 2024.

⁷⁴ CAVALLERI et al. 2019.

AZ EU JELEN VÁLASZA A TOVÁBBI KIHÍVÁSOKRA: MÉG TÖBB SZABÁLYOZÁS

A tanulmány első fele azt vizsgálta, hogy az EU digitális szabályozása milyen olyan tágabb kontextusba illeszkedik, amellyel kölcsönhatásba kerül, és amely kölcsönhatásból következtéseket lehet levonni magának a szabályozásnak alakulására nézve. Ezt a kontextust a globális verseny és az EU jogi identitása adta, amelyből önmagában következett, hogy rövid távon nem prognosztizálható koncepcionális fordulat az EU digitális átálláshoz való jogvezérelt hozzáállásában a jogi identitás, a globális védekező reflex és az ebből adódó geoökonómiai erő érvényesítése miatt. Ezen elméleti következtetések gyakorlati tesztelésére kínálnak lehetőséget a legújabb európai digitális szabályozási kezdeményezések. Ezeket tekinti át alább a tanulmány, ami megerősíti, hogy az új szabályozási csomagok továbbra is a meglévő, erősen szabályozásvezérelt modellre építenek, és nem hoznak koncepcionális változást, minthogy nem is hozhatnak, hiszen a problémák forrása nem jogi vagy szabályozási jellegű. Úgy tűnik, az EU továbbra is a felülről (politikákkal, támogatásokkal, szabályozásokkal) vezérelt kapitalizmussal próbálja ellensúlyozni az alulról jövő kezdeményezések hiányát.

A Bizottság a Competitveness Compassban is nem kevesebb, hanem több szabályozási kezdeményezést jelentett be: European Innovation Act, EU Cloud and AI Development Act, Quantum Act, Digital Networks Act, European Biotech Act.⁷⁵ Ezzel párhuzamosan szintén jelen van a szabályozási teher csökkentésének igénye, a Budapesti nyilatkozattal⁷⁶ is összhangban (25%-kal kevesebb jelentéstételi teher). Az EU az AI felelősségi szabályozási javaslatát vissza is vonta,⁷⁷ 2025. november 19-én pedig a Bizottság bemutatta a „digitális egyszerűsítési csomagot”, amelynek legfontosabb jogalkotási elemét, a digitális omnibuszt kifejezetten a versenyképesség és az egyszerűsítés céljából dolgozták ki (becslésük szerint 2029-ig akár 5 milliárd euró adminisztratív költségmegtakarítás érhető el).⁷⁸ A csomag két digitális omnibuszt tartalmaz: az egyik egyszerűsítene a mesterséges intelligencia (AI) szabályozását (a továbbiakban: digitális AI-omnibuszjavaslat),⁷⁹ a másik pedig a kiberbiztonságra és az adatokra vonatkozó szabályokat (a továbbiakban: digitálisomnibusz-javaslat),⁸⁰ és ezt egészíti ki az adatuniós stratégia,⁸¹ amelynek célja a magas minőségű adatok az AI számára történő elérhetővé tétele. Közben az Európai Bizottság 2026. január 20-án új kiberbiztonsági csomagot is javasolt. Mindez azonban a szabályozással okozott nehézségek szabályozással való korrigálásának tűnik.⁸²

⁷⁵ European Commission 2025b; European Commission 2025c.

⁷⁶ European Council 2024.

⁷⁷ DATTA–HARTMANN 2025.

⁷⁸ European Commission 2025d.

⁷⁹ European Commission 2025e.

⁸⁰ European Commission 2025f.

⁸¹ European Commission 2025a.

⁸² „[C]hallenges of digitalisation can only be addressed within a comprehensive and coordinated regulatory framework.” MEZEI 2025: 5.

Az EU AI-szabályozásra vonatkozó versenyképességi és egyszerűsítési javaslatai

2025-ben az EU több szabályozási kezdeményezést is tett az európai AI-versenyképesség növelése érdekében. A Bizottság a már említett Adatuniós Stratégia mellett 2025-ben elfogadta a AI Continent Action Plan-t⁸³ és az Apply AI Strategy-t.⁸⁴

A Bizottság Mesterséges Intelligencia Kontinens Akcióterve (a továbbiakban: Akcióterv) prioritásként kezeli a nagy méretű számítási és felhőkapacitást, bővíti az AI-gyárak hálózatát (13 mesterségesintelligencia-gyárral, amelyeket nagyjából 10 milliárd euróval támogatnak), és javaslatot tesz AI-„gigagyárakra”, amelyeket (20 milliárd eurót mozgósítva) az InvestAI program támogat. A Bizottság jelzi, hogy elő fog készíteni egy felhő- és AI-fejlesztési törvényt, amelynek célja az EU adatközpont-kapacitásának megtöbbszörözése. Másrészt az Akcióterv fontos eleme olyan adatlaborok létrehozása, amelyek egyesítik és kezelik az AI-gyárak különféle forrásokból származó, nagy mennyiségű, jó minőségű adatait. Ehhez fog kapcsolódni az Adatuniós Stratégia. Harmadrészt kezelni kívánja azt a körülményt, hogy az EU-ban alacsony az AI elterjedése (az uniós vállalatok 13,5%-a használt csak mesterséges intelligenciát).

A Bizottság *Apply AI* stratégiája ágazati AI-stratégiaként pozicionálódik, és további lépést jelent Európa „AI-kontinenssé” tétele felé, azzal a céllal, hogy növelje a mesterséges intelligencia elterjedését és innovációját. A stratégia egy „első az AI” (*AI-first*) megközelítést alkalmaz, amely arra ösztönöz, hogy a mesterséges intelligenciát alapértelmezett problémamegoldási lehetőségként kezeljék, és ezt összekapcsolja egy olyan iparpolitikai orientációval, amely az európai megoldásokat helyezi előtérbe. Összesen tíz stratégiai ipari ágazatot (egészségügy/gyógyszeripar; mobilitás/autóipar; robotika, gyártás/építőipar; éghajlat/környezet; energia; mezőgazdasági és élelmiszeripar; védelem/biztonság/űrpar; elektronikus kommunikáció; kultúra/kreatív ipar/média) és a közsférát célozza meg.

A digitális AI-omnibusz keretében a Bizottság javasolja az EU-s AI-törvény egyes elemeinek kiigazítását, mivel az érdekelt felek 2025-ben jelezték, hogy a megfelelés kapcsán az illetékes hatóságok és megfelelőségértékelő testületek kijelölésének késedelve, valamint a harmonizált szabványok hiánya gondot okoz. Erre való tekintettel a Bizottság azt javasolja,⁸⁵ hogy a magas kockázatú AI-rendszer megfelelését kössék a szabványok rendelkezésre állásához:

- 6 hónappal azután lépnek hatályba, hogy a Bizottság hivatalosan megerősítette a III. mellékletben szereplő magas kockázatú rendszerekre vonatkozó szabványokat/iránymutatásokat, és
- 12 hónappal azután, hogy megerősítette az I. mellékletben szereplő magas kockázatú rendszerekre vonatkozó szabványokat/iránymutatásokat.

⁸³ European Commission 2025g.

⁸⁴ European Commission 2025h.

⁸⁵ Javaslat az Európai Parlament és a Tanács rendelete az (EU) 2024/1689 és az (EU) 2018/1139 rendeletnek a mesterséges intelligenciára vonatkozó harmonizált szabályok végrehajtásának egyszerűsítése tekintetében történő módosításáról (a mesterséges intelligenciáról szóló digitális omnibuszcsomag) (a továbbiakban: digitális AI-omnibuszjavaslat). European Commission 2025e. Az 1. cikk (31) bekezdése új d) pontot ad az AI Act 113. cikkéhez.

A késedelem elkerülése érdekében végső határidőket is kijelöltek: legkésőbb 2027. december 2-án a III. mellékletben szereplő rendszerek, 2028. augusztus 2-án pedig az I. mellékletben szereplő rendszerek esetében a szabályok akkor is alkalmazandók, ha nem kerül sor szabványok megerősítésére. A tanácsi és parlamenti megállapodás (PE-CONS 30/26) ezeket a dátumokat rögzíti csak, függetlenül a bizottsági döntésektől.

Másodszor, a Bizottság javasolja⁸⁶ az AI Act 11. cikk (1) bekezdése szerinti egyszerűsített megfelelési módszerek (standard bejelentési forma a technikai dokumentációra) kiterjesztését a kkv-król a kis- és közepes kapitalizációjú (SMC) vállalatokra.⁸⁷ Ezenkívül a gazdaságos kapacitást figyelembe kell venni a kkv-k/SMC-k szankcionálásakor, ami azt jelenti, hogy a végrehajtás során tekintettel lehet lenni a vállalkozás méretére és erőforrásaira.

A javaslat eltörli azt a közvetlen és általános kötelezettséget, miszerint az AI-szolgáltatók és -alkalmazók biztosítják, hogy személyzetük „megfelelő szintű AI-ismeretekkel” rendelkezzen, és helyette az Európai Bizottságot és a tagállamokat bízta meg, hogy ösztönözzék és támogassák a képzési programokat (például oktatási kezdeményezések, útmutatók vagy tanfolyamok finanszírozása révén).⁸⁸ Lényeges, hogy a magas kockázatú rendszerek üzemeltetőinek továbbra is megfelelő képzésben kell részesülniük. A tanácsi és parlamenti megállapodás (PE-CONS 30/26) megtartja a bizottsági/tagállami ösztönzést, de visszahozza a szolgáltatókra és a telepítőkre vonatkozó azon kötelezettséget, hogy intézkedéseket kell tenniük a személyzet mesterséges intelligencia-műveltségének támogatására, de nem kötelesek garantálni ennek egy konkrét szintjét.

A magas kockázatú AI-rendszerek szolgáltatói kötelesek forgalomba hozatal utáni ellenőrzést végezni, amelyre az AI Act eredetileg egységes, harmonizált monitoringterv-sablon használatát írta elő [AI Act 72. cikk (3) bekezdés], amelyet a javaslat eltörölne.⁸⁹ Ehelyett a szolgáltatók rugalmasan alakíthatják piaci bevezetés utáni monitoringintézkedéseiket. A tanácsi és parlamenti megállapodás (PE-CONS 30/26) bár a kötelező érvényű harmonizált sablon eltörlését fenntartja, de a monitoringtervet kötelező megfelelési tényezőként megőrzi.

Csökkennének a regisztrációs terhek, ha a III. melléklet szerinti felhasználás magas kockázatú területen történik, de csak szűk körű, illetve eljárási feladatokra használják, és a szolgáltató nem minősíti magas kockázatúnak [vélelem megdöntése az AI Act 6. cikk (3) bekezdése alapján; hatályos AI Act 6. cikk (4) bekezdés alapján ilyenkor is kötelező a regisztráció]. Tehát, ha egy AI-rendszer magas kockázatú területen működik, de a szolgáltató a 6. cikk (3) bekezdése szerinti mentesség alapján nem minősítette magas kockázatúnak, akkor a szolgáltatónak már nem kell regisztrálnia az EU adatbázisában. A szolgáltatónak továbbra is dokumentálnia kell kockázatertékelését, és készen kell állnia arra, hogy a hatóságoknak bizonyítsa: a rendszer valóban jogosult a mentességre. A tanácsi és parlamenti megállapodás (PE-CONS 30/26)

⁸⁶ A digitális AI-omnibuszjavaslat 1. cikk (8) és (9) bekezdése módosítja az AI Act 11. cikk (1) bekezdését és a 17. cikk (2) bekezdését. European Commission 2025e.

⁸⁷ 1000 főnél kevesebb alkalmazottal rendelkező.

⁸⁸ A digitális AI-omnibuszjavaslat 1. cikk (4) bekezdése az AI Act 4. cikkét („AI-ismeretek”) új rendelkezéssel helyettesíti. European Commission 2025e.

⁸⁹ A digitális AI-omnibuszjavaslat 1. cikk (24) bekezdése módosítja az AI Act 72. cikkének (3) bekezdését azért, hogy törli a Bizottság végrehajtási jogkörét, és helyette iránymutatást ír elő a forgalomba hozatal utáni monitoringtervvel vonatkozóan. European Commission 2025e.

visszaállítja a regisztrációt, de leegyszerűsíti azt, mert továbbra is fontos a piacfelügyelet és a nyilvános elszámoltathatóság szempontjából, de a VIII. melléklet tartalma egyszerűsödik.

A Bizottság javasolja a nagyon nagy online platformokba/keresőmotorokba beágyazott AI-ok AI-hivatal általi központosított felügyeletét (a már létező GPAI mellett), hogy csökkentsék a széttagolt felügyeletet.⁹⁰ A javaslat által AI Act-be építendő 75. cikk (1) bekezdés c) pontja létrehozna egy előzetes jóváhagyási tesztelési mechanizmust: a Bizottság a forgalomba hozatal előtt teszteli a magas kockázatú mesterségesintelligencia-rendszereket (ezzel a feladattal bejelentett szervezetet is megbízhat) a megfelelőség ellenőrzése érdekében.

A javaslat bevezeti az AI Act új 4a. cikkét,⁹¹ amely kifejezetten engedélyezi a személyes adatok különleges kategóriáinak (érzékeny adatok) feldolgozását az AI-rendszerekben előforduló torzítások felismerése, kijavítása és nyomon követése céljából. A jelenlegi AI Act szerint az érzékeny adatok (például faji, egészségügyi, politikai nézetekre vonatkozó adatok) AI-képzés/tesztelés céljára történő felhasználását a 10. cikk (5) bekezdése szigorúan korlátozza, amely csak akkor engedélyezett, ha az „szigorúan szükséges”, és a GDPR 9. cikkében foglalt feltételeknek megfelel. Az új 4a. cikk felváltaná ezt a rendelkezést és kiterjesztené a hatályát: bármely AI-rendszer szolgáltatója (és bármely magas kockázatú AI üzemeltetője) szükség esetén (nem csak „szigorúan szükséges” esetben) felhasználhatja érzékeny személyes adatokat az elfogultság vagy a tisztességtelen eredmények tesztelésére.⁹² Az ilyen feldolgozásnak továbbra is tartalmaznia kell megfelelő biztosítékokat – példának okáért ha nincs más alternatíva, azokat a legkorszerűbb adatvédelmi intézkedésekkel (például álnevesítés) kell védeni, azokat nem szabad továbbadni, és felhasználás után törölni is kell őket.

Itt megemlítenéd, hogy a Digital Omnibus új GDPR 9. cikk (2) bekezdés k) pontot is javasol, amely lehetővé teszi a „maradék” különleges kategóriájú adat feldolgozását az AI-képzés során, amennyiben azok teljes törlése nem kivitelezhető, szigorú védelmi intézkedések mellett sem. Ez a GDPR-módosítás eltér az AI Act javasolt 4a. cikkétől: a képzési adatkészletekben található véletlenszerűen előforduló érzékeny adatokra vonatkozik, a 4a. cikk viszont az érzékeny adatok célzott feldolgozását teszi lehetővé, például a faji adatok szándékos felhasználását az AI elfogultságának ellenőrzésére a hiteljóváhagyások során.

⁹⁰ A digitális AI-omnibuszjavaslat 1. cikk (25) bekezdése által módosítandó AI Act 75. cikk (1) bekezdése egyértelműen kiterjesztené az AI Hivatal kizárólagos joghatóságát minden olyan AI-rendszerre, amely ugyanazon szolgáltató GPAI-modelljére épül (kivéve az ágazati jog hatálya alá tartozó termékekben találhatóakat), valamint a kijelölt nagyon nagy online platformok/keresőmotorok AI-rendszereire. European Commission 2025e.

⁹¹ A digitális AI-omnibuszjavaslat 1. cikk (5) bekezdése új 4a. cikket illeszt be az AI Act-be. European Commission 2025e.

⁹² Az AI Act 10. cikk (5) bekezdése lehetővé tette az érzékeny adatok feldolgozását „kizárólag az elfogultság figyelemmel kísérése, felismerése vagy korrekciója céljából”, de csak a magas kockázatú AI-rendszerek esetében. A javaslat törli a 10. cikk (5) bekezdését, és helyébe a 4a. cikket helyezi, amely kiterjeszti ezt a felhatalmazást, így bármely AI-rendszer szolgáltatója vagy üzemeltetője hivatkozhat a 4a. cikkre az érzékeny adatok feldolgozása érdekében, ha az valóban szükséges az elfogultság csökkentése céljából, és ha mind a hat feltétel (a–f) teljesül. A legfontosabb biztosítékok a következők: érzékeny adatok csak akkor használhatók, ha az elfogultság más (például szintetikus) adatokkal nem orvosolható, a legkorszerűbb adatvédelmi intézkedések (pszeudonimizálás, hozzáférés-ellenőrzés) alkalmazása, a harmadik felekkel való megosztás tilalma, valamint az elfogultság kijavítása után az adatok azonnali törlése. European Commission 2025e.

A tanácsi és parlamenti megállapodás (PE-CONS 30/26) visszatette továbbá azt a szűkítést, hogy a magas kockázatú AI-rendszerek szolgáltatói a személyes adatok különleges kategóriáit csak olyan mértékben dolgozhatják fel, amely „feltétlenül szükséges” az elfogultság észleléséhez és korrekciójához. Így a szöveg közelebb áll az eredeti (Bizottság által módosítani kívánt) szöveghez.

Az AI Act a sandboxszabályokat eredetileg nagyrészt a tagállamokra bízta, korlátozott uniós koordinációval, és csak az önálló, magas kockázatú rendszerek esetében engedélyezte a valós körülmények közötti tesztelést (RWT) (III. melléklet). A javaslat⁹³ kifejezetten lehetővé teszi az AI-hivatal számára, hogy uniós sandboxot működtessen az AI-rendszerek számára a saját kizárólagos hatáskörében (például rendszerkockázatú GPAI) – ez korábban nem állt fenn mint opció. A Bizottság azt is javasolja,⁹⁴ hogy bővítsék az AI-sandboxok és a valós körülmények közötti tesztelés (RWT) lehetőségeit. Korábban csak a III. mellékletben szereplő, magas kockázatú mesterséges intelligencia volt így tesztelhető; mostantól az I. mellékletben (például autópálya vagy egészségügy) szereplő AI is tesztelhető valós körülmények között a szolgáltatók által a piacra lépés előtt, egy terv alapján és a biztonsági jogszabályok sérelme nélkül. Az egyetlen kivétel, hogy az AI-törvény által teljes mértékben tiltott AI-rendszereket nem lehet kipróbálni még sandboxokban vagy kísérletekben sem.

A javaslat „egységes kérelem és egységes értékelés” eljárást vezet be azoknak a megfelelőségértékelő testületeknek, amelyek kettős kijelölést kérnek mind az AI Act, mind az I. mellékletben felsorolt vonatkozó ágazati termékjogszabályok alapján. A javaslat 1. cikk (10) bekezdésével kiegészített 28. cikk (8) bekezdése lehetővé teszi a bejelentett szervezetek számára, hogy egyszer nyújtsák be kérelmüket, feltéve, hogy az ágazati jogszabályok lehetővé teszik a közös értékeléseket. Az AI Act javasolt⁹⁵ 43. cikk (3) bekezdése egyértelművé teszi, hogy ha egy magas kockázatú AI-rendszert integrálnak egy ágazati jogszabályok hatálya alá tartozó termékbe, akkor a meglévő termékmegfelelőségi értékelés elegendő, és az AI Act követelményeit külön eljárás nélkül beépítik.

A tanácsi és parlamenti megállapodás (PE-CONS 30/26) új tiltott gyakorlatokat vezet be az olyan AI-rendszerekkel kapcsolatban, amelyek azonosítható személyek kifejezett hozzájárulása nélkül realizisztikus szexuális vagy intim anyagot állítanak elő vagy manipulálnak. A szintetikus tartalmak jelölésének határidejét is előrehozták 2026. december 2-ára.

Fentiek fényében az látszik, hogy a társjogalkotók kevésbé voltak a Bizottsághoz képest radikálisak az egyszerűsítés terén, és módosításokat eszközöltek ott, ahol szerintük az egyszerűsítés a jogbizonytalanságot, az elszámoltathatóságot vagy a jogvédelmek enyhítését kockáztatja (például AI-műveltség, regisztrációs kötelezettség, érzékeny adatfeldolgozás, monitoringterv).

⁹³ A digitális AI-omnibuszjavaslat 1. cikk (17) bekezdés a) pontja módosítja az AI Act 57. cikkét: beilleszt egy új (3a) bekezdést, amely felhatalmazza az AI Hivatalt, hogy EU-szintű AI szabályozási sandboxot hozzon létre az általa felügyelt bizonyos AI-rendszerek számára. European Commission 2025e.

⁹⁴ A digitális AI-omnibuszjavaslat 1. cikk (19) bekezdése módosítja az AI Act 60. cikk (1)–(2) bekezdését, hogy kiterjessze a valós körülmények közötti tesztelést (RWT). European Commission 2025e.

⁹⁵ Digitális AI-omnibuszjavaslat, 1. cikk (13) bekezdés. European Commission 2025e.

A digitálisomnibusz-javaslat

A hatályos uniós jogszabályok szerint a kiberbiztonsági incidenssel érintett szervezeteknek több keret alapján is jelentéstételi kötelezettségük lehet (például NIS2 irányelv,⁹⁶ GDPR,⁹⁷ 2002/58/EK irányelv⁹⁸). A digitálisomnibusz-javaslat ezért létrehozna az összes ilyen incidensbejelentéshez egy *egységes belépési pontot* biztosító digitális platformot (egyablakos ügyintézési pont, amelyet az ENISA⁹⁹ fog kifejleszteni).¹⁰⁰ A szervezetek ezen a portálon keresztül egyetlen jelentést nyújthatnak be, hogy egyszerre több jogszabály szerinti kötelezettségüket is teljesítsék („report once, share many”).¹⁰¹ Ezt az egyes jogszabályok előírásainak megfelelően továbbítanák az összes érintett nemzeti hatóságnak (CSIRT-ek, szabályozó hatóságok, adatvédelmi hatóságok stb.). A Bizottság arra számít, hogy ezáltal a legtöbb szervezet számára körülbelül felére csökken a teher.¹⁰² Az egyablakos ügyintézési pont tehát nem ruházna új hatásköröket az ENISA-ra, az csupán biztonságos csatornaként szolgálna, bebiztosítaná azt. A nemzeti hatóságok továbbra is teljes mértékben felelősek maradnának a hatáskörükbe tartozó incidensek fogadásáért és kezeléséért.

Az omnibuszjavaslat módosítaná a GDPR-t is. Két további jogalap kerülne be a 9. cikk (2) bekezdésében szereplő kivételek (az érzékeny adatok, például biometrikus adatok, egészségügyi adatok stb. feldolgozása alóli mentesség) listájára, méghozzá új k) pontként: szigorú feltételek

⁹⁶ Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1792 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS2 irányelv). European Parliament – European Council 2022: (80)–(134) bekezdés.

⁹⁷ European Parliament – European Council 2016: (1)–(88) bekezdés.

⁹⁸ European Parliament – European Council 2002: (37)–(47) bekezdés.

⁹⁹ *European Union Agency for Cybersecurity*, vagyis az Európai Unió Kiberbiztonsági Ügynökség.

¹⁰⁰ A NIS2 irányelv új 23a. cikkel egészül ki, amely felhatalmazza az ENISA-t az EU-szintű bejelentési platform létrehozására és fenntartására, megfelelő biztonsági és interoperabilitási funkciókkal. European Commission 2025f: 6. cikk 1. bekezdés.

¹⁰¹ A NIS2 23. cikkének (1) bekezdése úgy módosul, hogy az alapvető/fontos szervezetek az incidenseket a 23a. cikk alapján létrehozott egyablakos ügyintézési ponton keresztül jelentse. [European Commission 2025f: 6. cikk 2. bekezdés a) pont.] A 23. cikkhez új (12) bekezdést adnak hozzá, amely tisztázza, hogy ha egy gyártó már jelentette a „súlyos incidenst” a kiberrezilienciáról szóló (EU) 2024/2847 rendelet (CRA) alapján, akkor az a jelentés megfelel a NIS2 incidensbejelentési követelményeinek. [European Commission 2025f: 6. cikk 2. bekezdés b) pont.] A GDPR 33. cikkének (1) bekezdése úgy módosulna, hogy a bejelentés csak akkor legyen kötelező, ha az incidens „valószínűleg magas kockázatot” jelent a természetes személyek jogaira és szabadságaira nézve (megfelelően a 34. cikk szerinti, az érintettek tájékoztatására vonatkozó küszöbértéknek). Ezzel a küszöbérték *bármilyen kockázatról magas kockázatra* emelkedik, ami csökkenti a triviális jelentések számát, és a határidő 72 órától 96 órára nő. [European Commission 2025f: 3. cikk 8. bekezdés a) pont] Az omnibuszjavaslat hatályon kívül helyezné a távközlési ágazat vonatkozásában alkalmazandó 2002/58/EK irányelv 4. cikkét, amely előírta a távközlési szolgáltatók számára a kommunikáció biztonságának védelmét és az adatvédelmi incidensek bejelentését. Mivel a távközlési szolgáltatók a NIS2 irányelv alapján „alapvető fontosságú szervezetek” is, így a hatályon kívül helyezés megszünteti a távközlésre vonatkozó duplikált jelentési kötelezettséget, mivel ezek a szolgáltatók a NIS2 szerint egyetlen bejelentési ponton keresztül jelentenek biztonsági incidenseket. Fontos megjegyezni, hogy az e-adatvédelmi irányelv általános titoktartási szabályai továbbra is érvényben maradnak: csak az átfedő biztonsági bejelentési kötelezettséget szüntetik meg. [European Commission 2025f: preambulum (48) bekezdés.]

¹⁰² European Commission 2025i.

mellett az úgynevezett *maradék különleges kategóriájú adatok* feldolgozása AI-rendszer vagy AI-modell fejlesztésével és működtetésével összefüggésben végzett adatkezelés során. Ez a kivétel olyan eseteket érint, amikor a megfelelő szervezeti és technikai intézkedések ellenére az adatkezelő az AI tanításához, teszteléséhez vagy validálásához használt adatkészletekben, illetve az AI-rendszerben vagy AI-modellben a személyes adatok különleges kategóriáit azonosítja. Ilyen esetekben köteles eltávolítani a szóban forgó adatokat. Azonban ha az eltávolításuk aránytalanul nagy erőfeszítést igényel, az adatkezelő köteles minden esetben indokolatlan késedelem nélkül hatékonyan megvédeni ezeket attól, hogy kimenetek előállítására használják fel, felfedjék vagy más módon harmadik felek rendelkezésére bocsássák őket. Új 1) pontként szerepelne tehát, hogy biometrikus adatok feldolgozása kizárólag az érintett személyazonosságának megerősítése céljából történhet, feltéve, hogy mind ezek, mind az ellenőrzési eszközök az érintett személy kizárólagos ellenőrzése alatt maradnak (például a felhasználó ujjlenyomata vagy az arcszkennelése, amelyet saját eszközének vagy fiókjának feloldásához használ).

A GDPR 22. cikke szerinti érintettre nézve joghatással járó vagy őt hasonlóképpen jelentős mértékben érintő döntés csak akkor alapulhat kizárólag automatizált adatkezelésen – ideértve a profilalkotást is –, ha bizonyos feltételek teljesülnek (például szerződés megkötésének szükségessége). Vita alakult ki a „a szerződés megkötéséhez vagy teljesítéséhez szükséges” fordulat jelentéséről. A javaslat ezért módosítaná a 22. cikket, hogy egyértelművé tegye: az érintettel kötött szerződés keretében az automatizált döntéshozatali rendszer használata akkor is kielégítheti a „szükségesség” feltételét, ha elméletileg egy ember is meghozhatná a döntést. Más szavakkal: az számít, hogy az automatizálás a *szerződéses* szolgáltatás nyújtásának része, ahhoz szükséges.

A javaslat a 2002/58/EK irányelvből (távközlési adatvédelmi irányelv) a GDPR-ba helyezné át az úgynevezett *cookie-k* jóváhagyására vonatkozó követelményeket. A GDPR-ba új 88a. cikk kerülne, amely előírná a felhasználó hozzájárulását a személyes adatok felhasználói eszközön (végberendezésen) történő tárolásához vagy az azokhoz való hozzáféréshez. A jelenlegi távközlési adatvédelmi irányelv 5. cikk (3) bekezdés értelmében a felhasználó eszközén történő információtárolás vagy -hozzáférés (például cookie-k, nyomkövetők formájában) általában a felhasználó hozzájárulását igényli, kivéve, ha az a közzétételéhez műszakilag, vagy a felhasználó által kért szolgáltatáshoz feltétlenül szükséges. Az omnibuszcsomag modernizálná az EU cookie-szabályait, hogy a felhasználók valódi ellenőrzést kapjanak, és csökkenjen a felesleges felugró ablakok terhe. A megközelítés három fő elemből áll:

- a hozzájárulás megjelenítésének egyszerűsítése (egyszerű választási lehetőségek, beleértve az *Összes elutasítása* opciót egy kattintással) [digitálisomnibusz-javaslat 88a. cikk (4) bekezdés a) pont];
- a felhasználói központi beállítások engedélyezése (hozzájárulás vagy elutasítás) a böngésző vagy az eszköz beállításain keresztül a 88b. cikk (1) bekezdése szerint:¹⁰³ az adatkezelőknek biztosítaniuk kell, hogy webhelyeik elolvassák és feldolgozzák mind a hozzájárulásra, mind a tiltakozásra vonatkozó jelzéseket [beleértve a felhasználó tiltakozási jogát a GDPR 21. cikk (2) bekezdése szerint]; a 88b. cikk (6) bekezdése kötelezettséget ró

¹⁰³ A 88b. cikk automatizált jelzések tiszteletben tartására vonatkozó követelményei nem vonatkoznak a média-szolgáltatókra, amikor azok tartalmukat szolgáltatják. European Commission 2025f.

- a nagy (nem KKV) webböngésző-szolgáltatókra: lehetővé kell tenniük a felhasználók számára, hogy ezeket a hozzájárulási döntéseket géppel olvasható formában továbbítsák;
- bizonyos ártalmatlan vagy alacsony kockázatú felhasználások mentesítése a hozzájárulás követelménye alól a javasolt 88b. cikk (3) bekezdés alapján:
 - a hálózaton történő adatátvitel technikai szükségessége,
 - a felhasználó által kifejezetten kért szolgáltatás,
 - összesített statisztikák készítése a webhely használatáról,
 - a szolgáltatás vagy a felhasználó eszköze biztonságának fenntartása vagy helyreállítása esetén.

A GDPR javasolt 88a. cikk (4) bekezdése két korlátozást vezet be a „sötét minták” megelőzése érdekében: ha a felhasználó hozzájárulását adta, az adatkezelő nem kérheti újra ugyanazon célból a hozzájárulást, amíg amaz érvényben van; ha a felhasználó elutasította, az adatkezelő legalább 6 hónapig nem kérheti újra a hozzájárulását ugyanazon célból.

Az Európai Bizottság digitálisomnibusz-javaslatá új 88c. cikket vezetne be a GDPR-ba, hogy megoldja a személyes adatok feldolgozásával kapcsolatos jogi bizonytalanságot az AI-rendszerek és AI-modellek fejlesztése és üzemeltetése terén. A rendelkezés a GDPR jogszerű érdek jogalapjának [6. cikk (1) bekezdés f) pont] célzott pontosításaként, nem pedig új, önálló jogalapként lett megfogalmazva, és kimondja, hogy amennyiben az adatkezelés „az AI-rendszer” (az AI-törvény meghatározása szerint) vagy az AI-modell „fejlesztése és működtetése” során az adatkezelő érdekei szempontjából szükséges, az ilyen adatkezelés lehetséges a jogos érdekek alapján, a szokásos mérlegelési teszt és a fokozott biztosítékok figyelembevételével. Tehát megerősíti a GDPR „jogos érdekek” szerkezetét azzal, hogy kifejezetten megismétli: az adatkezelés csak akkor megengedett, ha az adatkezelő érdekei nem ütköznek az érintett érdekeivel vagy alapvető jogával és szabadságával,¹⁰⁴ kiemelve – ahogyan azt a 6. cikk (1) bekezdés f) pontja is teszi – a gyermekeket érintő adatkezelés különleges érzékenységet. Bevezet egy nem kimerítő biztonsági célú intézkedéssorozatot, amely magában foglalja

- az adatok minimalizálását a források kiválasztásában és a képzésben/tesztelésben,
- a modellekben/rendszerekben maradékosan megőrzött adatok nyilvánosságra hozatala elleni védelmet,
- a fokozott átláthatóságot, valamint
- az ilyen adatkezelés elleni „feltétel nélküli tiltakozási jogot”.

¹⁰⁴ Az adatkezelőknek mérlegelniük kell, hogy az AI-jal kapcsolatos érdek előnyös-e az érintettek és a társadalom számára (például előítéletek felismerése/eltávolítása és biztonságosabb, pontosabb eredmények), és értékelniük kell az észszerű elvárásokat, a fokozott átláthatóságot és a kockázatokat. European Commission 2025f: preambulum (30)–(33) bekezdés.

Ez utóbbi elem normatív szempontból jelentős, mivel a GDPR 21. cikk (1) bekezdésében foglalt általános tiltakozási jog feltételekhez kötött, amely ezáltal kiterjesztődne a mesterséges intelligencia fejlesztésének/működésének kontextusára is.¹⁰⁵

Az EU az elmúlt években több jogszabályt is elfogadott az adatmegosztás és a tisztességes digitális gazdaság elősegítése érdekében.¹⁰⁶ A digitálisomnibusz-javaslat egységesítené és egyszerűsítené ezeket a jogszabályokat, és azok legfontosabb rendelkezéseit beépítené a Data Act-be, hogy egyetlen koherens keretrendszer hozzon létre – lényegében összevonnák az említett négy európai adatjogszabályt. Ezenkívül a platformok és vállalkozások közötti kapcsolatokra vonatkozó rendelet (2019/1150/EU,¹⁰⁷ P2B rendelet) – bár a tisztességes platformgyakorlatokra összpontosít, és nem szigorúan az „adatokra” – a javaslat 10. cikk (1) bekezdése alapján szintén hatályát vesztené (kivéve bizonyos cikkeket, amelyek 2032 végéig hatályban maradnak).¹⁰⁸ A Bizottság indoklása szerint a P2B-szabályokat nagyrészt felváltotta a szigorúbb DMA. A Data Act (2023/2854 rendelet)¹⁰⁹ célzott módosításai:

- „Szivárgás elleni” védelem az üzleti titkok számára: a Data Act II. fejezete kötelezi az IoT-eszközök gyártóit és a kapcsolódó szolgáltatások nyújtóit, hogy (a felhasználó kérésére) megosszák az adatokat a felhasználóval vagy harmadik felekkel. A javasolt 4. cikk (8) bekezdése az adatkezelőknek jogot biztosít arra, hogy megtagadják az üzleti titkok felhasználóval való megosztását, ha fennáll a titkok jogellenes felhasználásának vagy nyilvánosságra hozatalának magas kockázata, különösen harmadik országok felé, amelyek uniós jog által előírtnál gyengébb vagy azzal nem egyenértékű védelmet nyújtanak.
- Felhőszolgáltató-váltási kötelezettségek (KKV/SMC-mentesség): a Data Act VI. fejezete átfogó követelményeket támaszt a felhőszolgáltatókkal szemben, hogy az ügyfelek átválthassanak egy másik szolgáltatóra (adatok és szolgáltatások hordozhatósága), valamint fokozatosan megszünteti a kilépési díjakat. Az omnibuszjavaslat célzott mentességet vezetne be a Data Act javasolt 31. cikk (1a) és (1b) bekezdései által: a kkv-k/SMC-k vagy testreszabottan nyújtott felhőszolgáltatások esetében, ha a szolgáltatási szerződést a Data Act alkalmazása előtt (2025. szeptember 12. előtt) írták alá, az ilyen szolgáltatók mentesülnek a szolgáltatóváltás megkönnyítésére vonatkozó követelmények alól. Tehát ez a mentesség korlátozott, csak a kkv/SMC szolgáltatók már meglévő szerződéseire vagy a magasan testreszabott megoldásokra vonatkozik, és a jövőben nem szünteti meg a hordozhatósági szabályokat.

¹⁰⁵ Ezt a javaslatot bírálata érte, mert a „feltétel nélküli tiltakozási jog” megvalósítása nehéz lehet, ha az érintettek nem tudják, hogy szerepelnek a képzési adatkészletekben. European Digital Rights 2025: 1–2; NOYB 2025: 68–72.

¹⁰⁶ A Data Actet (2023/2854/EU rendelet); az adatkormányzási rendeletet (DGA, 2022/868 rendelet); a nem személyes adatok szabad áramlásáról szóló rendeletet (2018/1807/EU rendelet) és a nyílt adatokról szóló irányelvet (2019/1024/EU irányelv).

¹⁰⁷ European Parliament – European Council 2019.

¹⁰⁸ A 10. cikk (2) bekezdése alapján az (EU): 2. cikk (1) bekezdés („üzleti felhasználó” fogalmának meghatározása), 2. cikk (2) bekezdés („online közvetítői szolgáltatások” fogalmának meghatározása), 2. cikk (5) bekezdés („online keresőmotor” fogalmának meghatározása), 4. cikk (korlátozás, felfüggesztés és megszüntetés), 11. cikk (belső panaszkezelési rendszer), 15. cikk (végrehajtás). European Commission 2025f.

¹⁰⁹ European Parliament – European Council 2023.

Az Adatuniós Stratégia

Az Európai Bizottság adatuniós stratégiája¹¹⁰ három prioritás köré csoportosítja az uniós fellépést:

- a mesterséges intelligencia számára elérhető, kiváló minőségű adatokhoz való hozzáférés előmozdítása, nevezetesen olyan adatlaboratóriumok¹¹¹ elindításával, amelyek összekapcsolják a közös európai adattereket az AI-ökoszisztémákkal, és biztonságos hozzáférést és megfelelést támogató szolgáltatásokat nyújtanak (beleértve az adatvédelmet megőrző eszközöket, mint például az álnevesítés és a szintetikus adatok generálása), miközben folytatják az ágazati adatterek bevezetését, amelyet egy folyamatban lévő, körülbelül 100 millió eurós uniós beruházás támogat;
- az adatvédelmi szabályok egyszerűsítése: adatokhoz való hozzáférésre/felhasználásra vonatkozó mintaszerződési feltételek, felhőszolgáltatásokra vonatkozó standard szerződéses kikötések, iránymutatások és egy erre a célra létrehozott jogi ügyfélszolgálat; továbbá
- az EU adatszuverenitásának védelme a nemzetközi adatszivárással szemben. Ez utóbbi kapcsán a Bizottság stratégia iránymutatásokat (2026 második negyedév) hirdet meg az EU-szervezetek/adatok harmadik országok általi kezelésének/méltányosságának értékelésére.

A Bizottság ezenkívül adatuniós stratégiájában bejelenti egy adatszivárgás elleni eszközkészlet létrehozását, amelynek célja, hogy ellensúlyozza azokat az indokolatlan harmadik országbeli gyakorlatokat, amelyek az EU nem személyes adatainak áramlását érintik, ideértve a lokalizációs követelményeket, a piaci kizárást és a gyenge vagy elégtelen biztosítékokat, valamint a kapcsolódó adatszivárgási kockázatokat. A stratégia ezt a kezdeményezést az EU adatszuverenitásának tágabb célkitűzésébe ágyazza, amelynek meghatározása szerint az Unióban és külföldön meg kell őrizni az adatokhoz való hozzáférést, az azok felhasználása és védelme feletti ellenőrzést, miközben tisztességes és biztonságos feltételek mellett lehetővé kell tenni a határokon átnyúló adatcserét megbízható partnerekkel. A Bizottság jelzi, hogy az eszköztár támaszkodhat az Unió olyan eszközeire, mint a kereskedelmi végrehajtási rendelet és a kényszerítés elleni eszköz, illetve további intézkedések is megfontolhatók.

¹¹⁰ European Commission 2025a.

¹¹¹ Ezek az adatkutató laboratóriumok speciális létesítmények vagy sandboxok, ahol a vállalatok (különösen a start-upok, illetve a kkv-k) és a kutatók biztonságos környezetben, közösen hozzáférhetnek nagy, sokszínű adatkészletekhez és kísérletezhetnek velük. Az európai *közös adatterületek* (ágazati adatmegosztási infrastruktúrák) alakuló hálózatába integrálva a laboratóriumok áthidalhatják a nyers adatok rendelkezésre állása és a mesterséges intelligencia fejlesztési igényei közötti szakadékot.

Az új kiberbiztonsági csomag

Az Európai Bizottság 2026. január 20-án új kiberbiztonsági csomagot javasolt. A javaslat magában foglalja a Cybersecurity Act 2-t¹¹² (CSA2 javaslat) és a NIS2 irányelv módosítását.¹¹³

A javaslat összesen négy főbb célkitűzést tartalmaz:

- az EU-s információs és kommunikációs technológiák (IKT) ellátási láncai biztonságának javítása;
- az európai kiberbiztonsági tanúsítási keret egyszerűsítése és fejlesztése;
- a kiberbiztonsági szabályok betartásának megkönnyítése (NIS2 irányelv módosítása);
- az Európai Unió Kiberbiztonsági Ügynökség (ENISA) szerepének megerősítése a tagállamok és az EU támogatásában a kiberbiztonsági fenyegetések kezelése terén.

Az IKT-ellátási láncok biztonságának erősítése az EU-ban

Az új kiberbiztonsági törvény célja az Európai Unió információs és kommunikációs technológiai ellátási láncában jelentkező, harmadik országbeli beszállítókhoz kapcsolódó kockázatok csökkentése. A Bizottság szerint a jelenlegi geopolitikai környezetben az ellátási lánc biztonságának ki kell terjednie a beszállítókkal összefüggő stratégiai kockázatok kezelésére is. A javaslat tehát kiegészíti a NIS2 irányelv általános kiberbiztonsági kockázatkezelési követelményeit és a termékekre összpontosító kiberreziliencia-törvényt azáltal, hogy *nem technikai jellegű*¹¹⁴ *beszállítói kockázatokkal* (például geopolitikai befolyás) is foglalkozik.¹¹⁵ Az új keret a NIS2 irányelv szerinti kiemelten kritikus és az egyéb kritikus ágazatokban felmerülő nem technikai kockázatokat fogja kezelni.

A javaslat 99. cikke bevezeti az uniós szintű koordinált biztonsági kockázatértékeléseket, ami lehetővé teszi a Bizottság (vagy legalább három tagállam) számára annak kezdeményezését, hogy a NIS együttműködési csoport alapesetben 6 hónapon belül azonosításra javasoljon az ellátási láncon belüli kulcsfontosságú IKT-eszközöket, és javaslatot tegyen kockázatcsökkentő intézkedésekre. A 99. cikk (3) bekezdése létrehoz egy sürgősségi eljárást: amennyiben a Bizottság úgy ítéli meg, hogy az IKT-ellátási láncot érintő jelentős kiberfenyegetés gyors intézkedést igényel a belső piac védelme érdekében, sürgősen konzultálnia kell a tagállamokkal a kockázatcsökkentő intézkedések (a 103. cikkben meghatározottak szerinti) bevezetéséről, továbbá kockázatértékelést kell végeznie, amely szintén azonosítja a legfontosabb eszközöket,

¹¹² European Commission 2026a. A továbbiakban: The Cybersecurity Act 2.

¹¹³ European Commission 2026b. A továbbiakban: NIS2 módosítási javaslat.

¹¹⁴ Annak a valószínűsége, hogy a szállító harmadik ország gyakorolhat olyan hatást, amely a nyújtott szolgáltatás kiesését vagy zavarát okozhatja, vagy veszélyeztetheti a szervezet által gyártott terméket, vagy adatlopáshoz vezethet, többek között kémkedés vagy bevételtermelés céljából. The Cybersecurity Act 2. cikk (42) bekezdés.

¹¹⁵ A The Cybersecurity Act 2. 98. cikk (2) bekezdése rögzíti, hogy ez a mechanizmus nem hivatott felváltani 1. a kiberreziliencia-törvény (2024/2847/EU rendelet) termékszintű kötelezettségeit és 2. a tagállamok által a NIS2 átitételésekor végrehajtott szervezetszintű kockázatkezelési kötelezettségeket, azok továbbra is párhuzamosan alkalmazandók.

a fenyegetést jelentő szereplőket és a sebezhetőségeket, valamint kockázatcsökkentő intézkedésekre is javaslatot tesz.

Amennyiben a 99. cikk szerinti eljárás vagy más forrás alapján felmerül, hogy egy harmadik ország súlyos és strukturális nem technikai kockázatot jelent az IKT-ellátási láncokra, a 100. cikkben javasolt eljárás keretében a Bizottság ellenőrzi az adott ország által jelentett kockázatot, figyelembe véve olyan elemeket, mint a jogi vagy gyakorlati kényszer a sebezhetőségek állami hatóságok felé történő közzétételére; a hatékony jogorvoslatok és demokratikus felügyelet hiánya; az adott országból működő szereplőkkel kapcsolatos rosszindulatú kibertevékenységek bizonyítéka; valamint az ország együttműködési hajlandóságának vagy képességének hiánya. A 100. cikk (4) bekezdése konkrét következményeket fűz az ilyen harmadik országban letelepedett vagy általa ellenőrzött magas kockázatú beszállító fogalmához: a javaslat így kizárná őket az egyes szabványosítási és specifikációs folyamatokban való részvételből, az EU-s kiberbiztonsági tanúsításból, az akkreditált megfelelőség ellenőrzési tevékenységből, a közbeszerzésekből.

A NIS együttműködési csoport által végzett uniós szintű koordinált biztonsági kockázátértékelés vagy a 99. cikk (3) bekezdése szerinti sürgősségi eljárás eredményeként:

- a 102. cikk felhatalmazza a Bizottságot (végrehajtási aktus útján), hogy meghatározza, mely eszközök minősülnek „kulcsfontosságú IKT-eszközöknek” a NIS2 irányelv I. és II. mellékletében felsorolt típusú szervezetek által gyártott termékek vagy nyújtott szolgáltatások tekintetében; a cikk felsorolja a kijelöléshez irányadó kritériumokat is (például alapvető/érzékeny funkciók; súlyos zavarok vagy adatszivárgás lehetősége; koncentrációs függőség; értékelési eredmények);
- a 103. cikk felsorolja a kockázatcsökkentő eszközöket, köztük (legfőképpen) azt a lehetőséget, hogy a Bizottság végrehajtási aktussal tilalmat rendeljen el a 102. cikkben meghatározott kulcsfontosságú IKT-eszközökben a magas kockázatú beszállítók IKT-alkatrészeinek használatára/telepítésére/integrálására vonatkozólag, átmeneti és fokozatos kivezetési időszakokkal együtt; a cikk emellett szélesebb körű kockázatcsökkentési lehetőségeket is biztosít (átláthatósági követelmények; bizonyos adatátvitel és a távoli feldolgozás korlátozása; műszaki ellenőrzések; működési ellenőrzés/kiszervezés korlátozása; szerződéses korlátozások; átvilágítási követelmények; diverzifikációs intézkedések).

A 104. cikk előírja, hogy a Bizottság (végrehajtási aktusok útján) állítsa össze a magas kockázatú beszállítók listáját a 103. cikk szerinti tilalmak tekintetében. A 100. cikkben meghatározott harmadik országgal kapcsolatban álló szervezet mentességet kérhet bizonyos tilalmak alól (beleértve a kulcsfontosságú IKT-eszközök alkatrészeinek szállítására és a vonatkozó közbeszerzésekben való részvételre vonatkozó korlátozásokat), feltéve, hogy bizonyítja a kockázat hatékony mérséklését.

A 110. cikk a megbízható ellátási lánc logikáját alkalmazza a mobil, vezetékes és műholdas elektronikus hírközlési hálózatokra azáltal, hogy a II. mellékletben meghatározza azok legfontosabb IKT-eszközeit, és előírja a magas kockázatú beszállítóktól származó alkatrészek fokozatos kivonását. A mobilhálózatok esetében legfeljebb 36 hónapos kivezetési időszakot határoz meg (a vonatkozó magas kockázatú beszállítók listájának közzétételétől számítva). A 111. cikk értelmében az említett hálózatok szolgáltatói nem használhatnak, telepíthetnek

vagy integrálhatnak magas kockázatú beszállítóktól származó IKT-alkatrészeket a II. mellékletben meghatározott kulcsfontosságú IKT-eszközök üzemeltetése során.

Az európai kiberbiztonsági tanúsítási keret egyszerűsítése és fejlesztése

A felülvizsgált kiberbiztonsági törvény biztosítaná, hogy az EU fogyasztóihoz eljutó termékek és szolgáltatások biztonságát hatékonyabb módon teszteljék. Ez a megújított európai kiberbiztonsági tanúsítási keretrendszer (ECCF) révén valósulna meg. Az ECCF lehetővé teszi az európai kiberbiztonsági tanúsítási sémák (szabálykönyvek) alapértelmezés szerint 12 hónapon belüli kidolgozását. Az ENISA által kezelt tanúsítási sémák gyakorlati, de önkéntes eszközzé válnának a vállalkozások számára. Lehetővé tennék a vállalkozások számára, hogy igazolják az uniós jogszabályoknak való megfelelést, csökkentve ezzel a megfelelési terheket és a költségeket. Az IKT-termékeken, szolgáltatásokon, folyamatokon és felügyelt biztonsági szolgáltatásokon túl a vállalatok és szervezetek tanúsíthatják kiberbiztonsági helyzetüket, hogy megfeleljenek a piaci igényeknek.

Alapértelmezés szerint a tanúsítás önkéntes (kivéve, ha az uniós vagy a nemzeti jog egy adott kontextusban kötelezővé teszi) [71. cikk (3) bekezdés], és a keret alapján kiadott tanúsítványokat, EU-megfelelőségi nyilatkozatokat automatikusan el kell ismerni minden tagállamban [71. cikk (4) bekezdés].

A sémák kidolgozása az ENISA-hoz benyújtott bizottsági kérelemmel indul (73. cikk). Az ENISA ezután strukturált folyamat keretében jelölt sémát készít elő, amelyhez a tagállamok az Európai Kiberbiztonsági Tanúsítási Csoporton (az ECCG-n) keresztül is hozzájárulnak, és amely végül a Bizottság végrehajtási aktusban történő elfogadásához vezet (74. cikk). Az ENISA támogatja a sémák karbantartását (75. cikk), azokat a Bizottság értékelheti, felülvizsgálhatja vagy akár vissza is vonhatja (76. cikk). Az ENISA nyilvános weboldalon biztosítja a sémák leírását.

A sémáknak meghatározott biztonsági célokat kell kitűzniük (például biztonságos tervezés / alapértelmezett biztonság, a titkosság/integritás/elérhetőség védelme, a sebezhetőség kezelése, naplózás/monitorozás, rugalmasság) (80. cikk). A séma tartalmazhat szabványosított elemeket (81. cikk), és meg kell határoznia a biztonsági szinteket: *alapvető/jelentős/magas* (82. cikk). Ezeknek a szinteknek arányosnak kell lenniük a kockázattal (az események valószínűsége/hatása; rendeltetésszerű használat; működési környezet) [82. cikk (1) bekezdés].

- *Alapvető*: az értékelés legalább a műszaki dokumentáció áttekintését tartalmazza [82. cikk (5) bekezdés].
- *Jelentős*: szigorúbb ellenőrzéseket (például nyilvánosan ismert sebezhetőségek hiánya + tesztelés) ad hozzá az ismert kockázatok és a korlátozott képességekkel/erőforrásokkal rendelkező támadók forgatókönyveinek minimalizálása érdekében [82. cikk (6) bekezdés].
- *Magas*: a „legkorszerűbb” támadásokra irányul, amelyeket nagy képességű szereplők hajtanak végre; magában foglalja (legalább) a nyilvánosan ismert sebezhetőségek hiányát + a legkorszerűbb tesztelést + az ellenállás értékelését (például ahol releváns, penetrációs tesztelés) [82. cikk (7) bekezdés].

Adott séma keretei között adható ki az európai kiberbiztonsági tanúsítvány, és az a séma által biztosított bármely biztosítási szintre vonatkozhat [82. cikk (2) bekezdés]. Ha egy IKT-termék, -szolgáltatás, -folyamat, illetve általa felügyelt biztonsági szolgáltatás vagy egy szervezet kiberbiztonsági helyzete egy séma keretében tanúsítást kap, akkor feltételezik, hogy megfelel a sémakövetelményeknek [85. cikk (1) bekezdés]. Alacsonyabb kockázatú felhasználási esetekben a rendszerek lehetővé tehetik a megfeleléség önértékelését, amely EU-megfelelőségi nyilatkozathoz vezet [82. cikk (2) bekezdés és 83. cikk (2) bekezdés].

Amennyiben egy másik uniós jogi aktus így rendelkezik, az ECCF-tanúsítvány megfeleléségi vélelmet keletkeztethet a vonatkozó jogi követelményekkel kapcsolatban (78. cikk). Például a CRA előírja, hogy ha egy termék (és a gyártói folyamatok) rendelkezik EU-megfelelőségi nyilatkozattal vagy tanúsítvánnyal, amelyet a 2019/881/EU rendelet (azaz az ECCF séma) szabályoz, akkor úgy tekintendő, hogy „megfelel” a CRA I. melléklete követelményeinek, amennyiben a tanúsítvány/nyilatkozat kiterjed ezekre a követelményekre [CRA 27. cikk (8) bekezdés].

A további tanúsítványokat általában az akkreditált megfeleléséértékelő szervezetek (CAB-ek) állítják ki [85. cikk (2) bekezdés], de a *magas* biztosítási szint esetében a kiadás szigorúbb feltételhez van kötve: nemzeti tanúsító hatóságok végzik [85. cikk (4)–(5) bekezdés].

*Az NIS2 irányelv módosítása*¹¹⁶

A javaslat kiegészíti a „méretüktől függetlenül” a NIS2 hatálya alá eső szervezeteket:

- az európai digitálisidentitás-tárcák és az európai üzleti tárcák szolgáltatóival,¹¹⁷ amelyek digitális infrastruktúra szolgáltatóknak fognak majd minősülni;
- a stratégiai kettős felhasználású infrastruktúra tulajdonosainak/kezelőinek/üzemeltetőinek minősülő szervezetekkel.¹¹⁸

Viszont a mikro- és kis DNS-szolgáltatókat kiveszi a javaslat a „méretétől független” hatály alá tartozó szervezetek köréből.¹¹⁹

Az I. mellékletben szereplő szervezetek esetében felemelnék az alapvető szervezetek küszöbértékét: csak az I. mellékletben szereplő, a kis- és közép vállalkozásokra vonatkozó küszöbértékeket meghaladó szervezetek minősülnek „alapvetőnek”.¹²⁰ Ezáltal az I. mellékletben szereplő szervezetek „alapvető fontosságú” kategóriából „fontos” kategóriába való áthelyezése csökkenti a felügyeleti intenzitást, hiszen így ezek nem előzetes, hanem csak utólagos megfelelési kötelezettség alá esnek.

A tagállamok előírhatják a szervezetek számára, hogy szerezzenek kiberbiztonsági tanúsítványt a CSA2 alapján elfogadott európai kiberbiztonsági tanúsítási rendszer keretében.¹²¹

¹¹⁶ NIS2 módosítási javaslat.

¹¹⁷ Lásd NIS2 módosítási javaslat 1. cikk (1) bekezdés a) pont.

¹¹⁸ NIS2 módosítási javaslat 1. cikk (2) bekezdés b) pont.

¹¹⁹ Lásd NIS2 módosítási javaslat 1. cikk (1) bekezdés a) pont i. alpont.

¹²⁰ A NIS2 módosítási javaslat 1. cikk (2) bekezdés a) pont i. alpontja alapján.

¹²¹ Lásd a NIS2 módosítási javaslat 1. cikk (9) bekezdése alapján.

Az ilyen módon tanúsított szervezeteket az illetékes hatóságok nem vethetik alá további felületei intézkedéseknek.

Ransomware-támadás esetén a javaslat szerint a váltságdíj-követeléssel/-fizetéssel kapcsolatos információkat kérésre át kellene adni.¹²²

Az ENISA megerősítése

Az ENISA megbízatását megerősítik, hogy az jobban megfeleljen az EU operatívabb kiberbiztonsági modelljének: több szolgáltatásnyújtás és koordináció, kevesebb tisztán tanácsadói tevékenység. A Cybersecurity Act 2 csomag intézményi pilléreként hatályon kívül kerül a (EU) 2019/881 rendelet. Az ENISA alapvető célját úgy fogalmazza meg, hogy magas szintű kiberbiztonságot, kiberrezilienciát és bizalmat biztosítson az Unió egész területén¹²³ és az EU szakértelmének „referenciapontjaként” működjön,¹²⁴ miközben az ügynökséget kifejezetten a belső piac fragmentációjának csökkentésére pozicionálja.¹²⁵ Az ENISA a tagállamokkal és az uniós szervekkel folytatott operatív együttműködés központjává válik, beleértve a CSIRT-hálózat és az EU-CyCLONe titkársági feladatait is [10. cikk (2)–(3) bekezdés]. Köteles korai riasztásokat kiadni (12. cikk). Feladata továbbá az incidensekkel kapcsolatos közvetlen támogatási képességek biztosítása: az EU kiberbiztonsági tartalék működtetése és igazgatása [13. cikk (1) bekezdés], az incidensek felülvizsgálatának/értékelésének támogatása [13. cikk (2) bekezdés], valamint egy ransomware-segélyszolgálat működtetése a NIS2 alapvető/fontos szervezeteinek számára [13. cikk (3) bekezdés]. Az ENISA-nak továbbá konkrét operatív eszközöket kell biztosítania – elsősorban uniós szintű platformokat, ideértve a CRA/NIS2 egyseges jelentési platformját (15. cikk) és az Unió sebezhetőségkezelési szolgáltatási kapacitását (16. cikk) –, miközben továbbra is ösztönöznie kell az uniós tanúsítási ökoszisztémát (17. cikk).

KÖVETKEZTETÉSEK

Az Európai Bizottság a Draghi-jelentés nyomán a szabályozási terhelés csökkentése, valamint az innováció és a versenyképesség növelése címén átfogó szabályozási intézkedéseket jelentett be 2025 végén és 2026 elején. Ezekben az intézkedésekben közös, hogy a meglévő, erősen szabályozás-központú és -orientációjú rendszeren belül mozognak, a rendszer említett szempontok szerinti finomhangolásait jelentik a rendszer egészére vonatkozó koncepcionális változtatások nélkül. Az 1. táblázat áttekintést nyújt a digitális és az AI-omnibusz-, valamint a kibercsomagok alapján.

¹²² NIS2 módosítási javaslat 1. cikk (8) bekezdés.

¹²³ Lásd The Cybersecurity Act 2 3. cikk (1) bekezdés.

¹²⁴ Lásd The Cybersecurity Act 2 3. cikk (2) bekezdés.

¹²⁵ Lásd The Cybersecurity Act 2 3. cikk (3) bekezdés.

1. táblázat: Az EU digitális technológiai szabályozási intézkedéseinek összefoglalása (2025–2026)

KKV-terhek csökkentése	– A NIS2 irányelvben emelnék az alapvető szervezetek küszöbértékét: csak az I. mellékletben szereplő, a kis- és középvállalkozásokra vonatkozó küszöbértékeket meghaladó szervezetek minősülnek <i>alapvetőnek</i> – Időleges mentesség a felhőszolgáltató-váltás (Data Act) kötelezettsége alól a kkv-k/SMC-k esetében
Bürokráciai terhek csökkentése	– Eltörlik az EU AI Act megfelelő szintű AI-ismeretekre vonatkozó előírását – Az EU AI Act piaci bevezetés utáni monitoring nincs standard formához kötve, hanem szabadon alakítható – Magas kockázatú AI-minősítés vélelmének megdöntésekor egyszerűbb regisztráció. – Nagyon nagy online platformokba/keresőmotorokba beágyazott AI-ok EU-s AI-hivatal általi központosított felügyelete – Egyablakos bejelentési pont a kiberincidensek jelzésére a CSA2 szerint
Megfelelés könnyítése	– A magas kockázatú AI-rendszer megfelelését konkrét dátumokhoz kötik – Az ENISA által kezelt tanúsítási sémák lehetővé teszik a vállalkozások számára, hogy igazolják az uniós jogszabályoknak való megfelelést
Innováció támogatása	– Engedélyezik a személyes adatok különleges kategóriáinak (érzékeny adatok) feldolgozását az AI-rendszerekben előforduló torzítások felismerése, kijavítása és nyomon követése céljából – Digitális omnibusz: az új GDPR 9. cikk (2) bekezdés k) pontot javasol, amely lehetővé teszi a „maradék” különleges kategóriájú adat feldolgozását az AI-képzés során, amennyiben azok teljes törlése szigorú védelmi intézkedések mellett sem kivitelezhető – Valós körülmények közötti tesztelés (RWT) lehetőségének bővítése – GDPR-érdekelv megerősítése az AI-modell fejlesztéshez kapcsolódó adatkezelés kapcsán
Szuverenitás erősítése	– Az EU adatszuverenitásának védelme a nemzetközi adatelszívással szemben (EU Adatstratégia) – Az Európai Unió információs és kommunikációs technológiai ellátási láncában jelentkező, harmadik országbeli beszállítókhoz kapcsolódó kockázatok csökkentése
Felhasználói terhek csökkentése	A felhasználó hozzáféréseinek automatizálása a személyes adatok felhasználói eszközön (végberendezésen) történő tárolásához

Forrás: a szerző szerkesztése

Látható, hogy a fenti javaslatok a létező szabályozási kereten belüli könnyítéseket tartalmaznak, illetve igyekeznek növelni a stratégiai önállóságot, biztonságot. Az alapvető koncepcióváltást (a szabályozásvezérelt attitűddel való szakítást) azonban nyilvánvalóan akadályozza, hogy az EU nem egységes, homogén államalakulat. Erre példa a CSA2 javaslat, amely a digitális technológiai szuverenitás védelmében megteremti az EU-szintű geopolitikai jellegű kockázatkezelést, de nagyon lassan és körülményesen tudja a számtalan érdek egyeztetésének követelménye miatt. Így a CSA2 javaslat 98. cikk (3) bekezdése¹²⁶ alapján továbbra is a tagállamok kezében marad a gyors védekezés lehetősége. A másik akadály azzal kapcsolatos, hogy a piaci lehetőségek és a szabályozás kapcsolatát illetően az EU-ban továbbra is utóbbi szerepe a meghatározó, míg az innováció és versenyképesség szempontjából fordítva: a szabályozásnak

¹²⁶ „Nem zárja ki, hogy a tagállamok az IKT-ellátási láncokban magasabb szintű kiberbiztonságot biztosító rendelkezéseket fogadjanak el vagy tartsanak fenn.”

a piaci folyamatokat követő, és nem azokat megalkotó/kitaláló pozícióban kellene lennie¹²⁷ (lásd EU-s szabályozásvezérelt kapitalizmus).¹²⁸ Az AI-ra vonatkozó amerikai cselekvési terv (2025. július)¹²⁹ például nyíltan „alulról felfelé” építkezik: felszólal a magánszektor gátló felesleges szabályozási akadályok ellen, és a szövetségi intézkedéseket a magánszektor által vezérelt innováció feltételeként pozicionálja – ezt kifejezetten szembeállítva azzal, amit *terhes szabályozásnak* nevez. Az EU-modell kritikussai azzal érvelnek, hogy az ex ante szabályozás tiltó megfelelési terheket ró, lelassítja az AI-kutatáshoz elengedhetetlen iteratív fejlesztési ciklusokat, és hátrányos helyzetbe hozza az európai startupokat a megengedőbb joghatóságokban működő versenytársakkal szemben.¹³⁰ Mivel a törvényhozók nem tudják előre látni a mesterséges intelligenciához hasonló technológiák fejlődési pályáját, a szigorú megfelelési követelmények a tehetségeket és a tőkét az innovációbarátabb környezetbe terelik.¹³¹

A második akadály kapcsán említhető még az EU redisztribúciós szabályozási megközelítése, amellyel a digitális technológiai hatalomhoz viszonyul,¹³² és amely a nagy digitális technológiai cégek ökoszisztémájának feltörése, az eszközeihez való hozzáférés előírása által próbál piaci lehetőségeket teremteni. Ez nyilván az innováció hiányának tünete is, amennyiben a szabályozás az innovatív európai vállalatok hiányában, védekezésből kényszerül arra, hogy a globális digitális technológiai cégeket szabályozási keretek közé szorítsa. Szabályozási kapitalizmusként az EU digitális szabályozásában kifejezetten az audit jellegű kötelezettségek (ön- és harmadik feles értékelése, mint például a NIS2 vagy CRA) szabályozási előírásán keresztül érhető tetten újfajta piacok (szabályozási) létrehozása.

Meg kell említeni egy harmadik koncepcionális akadályt is, ez pedig a biztonságra törekvés. Ez a szempont nehezen választható el az innovációhiánytól, hiszen a szabályozási védekezés jellegét és terjedelmét (amely biztonsági szempontként merül fel) nyilván a külföldi cégek térnyerése, és ezzel összefüggésben a szuverenitási szempontok is befolyásolják. A biztonság pedig köztudottan költséges és semmiképpen sem olyan tényező, amelyet elegendő volna piaci logikára építeni.

FELHASZNÁLT IRODALOM

- ADRAGNA, Anthony (2025): Trump Threatens More Tariffs after EU Fines Google €2.95B. *Politico*, 2025. május 9. Online: www.politico.com/news/2025/09/05/trump-threatens-more-tariffs-after-eu-fines-google-00547922
- BRIA, Francesca – TIMMERS, Paul – GERNONE, Fausto (2025): *EuroStack – A European Alternative for Digital Sovereignty*. Gütersloh: Bertelsmann Stiftung. Online: <https://doi.org/10.11586/2025006>

¹²⁷ Lásd THIERER 2016.

¹²⁸ LEVI-FAUR 2005: 12–32.

¹²⁹ The White House 2025.

¹³⁰ COLLAO 2024: 153–158.

¹³¹ KRETSCHMER et al. 2023.

¹³² Lásd YASAR 2025.

- C-311/18. sz. Data Protection Commissioner kontra Facebook Ireland Limited és Maximilian Schrems ügyben 2020. július 16-án hozott ítélet [ECLI:EU:C:2020:559]. Online: https://infocuria.curia.europa.eu/tabs/jurisprudence?lang=EN&sort=DOC_DATE-DESC&search-Term=%2522ECLI%253AEU%253AC%253A2020%253A559%2522
- CANDELON, François – REEVES, Martin (2017): The New Digital World: Hegemony or Harmony? BCG Henderson Institute, 2017. november 14. Online: www.bcg.com/publications/2017/strategy-globalization-new-digital-world-hegemony-harmony
- CAULCLUTT, Clea (2025): JD Vance Warns Europe to Go Easy on Tech Regulation in Major AI Speech. *Politico*, 2025. február 11. Online: www.politico.eu/article/vp-jd-vance-calls-europe-row-back-tech-regulation-ai-action-summit
- CAVALLERI, Maria Chiara et al. (2019): *Concentration, Market Power and Dynamism in the Euro Area: ECB Working Paper Series, No 2253*. Frankfurt am Main: European Central Bank.
- Cloud Market Gets its Mojo Back; AI Helps Push Q4 Increase in Cloud Spending to New Highs (2024). *Synergy Now TechInsights*, 2024. február 1. Online: www.srgresearch.com/articles/cloud-market-gets-its-mojo-back-q4-increase-in-cloud-spending-reaches-new-highs
- COLLAO, Vanessa Villanueva (2024): Navigating the Transatlantic AI Landscape: The EU Artificial Intelligence Act and its Ripple Effect on the US. *MediaLaws: Rivista di diritto dei media*, 8(1), 153–158.
- Council of the European Union (2024): *Council Conclusions on the Future of Cybersecurity: Implement and Protect Together*. 10133/24 jelzetű EU-dokumentum, 2024. május 21. Online: <https://data.consilium.europa.eu/doc/document/ST-10133-2024-INIT/en/pdf>
- DAMRO, Chad (2012): Market Power Europe. *Journal of European Public Policy*, 19(5), 682–699. Online: <https://doi.org/10.1080/13501763.2011.646779>
- DATTA, Anupriya – HARTMANN, Théophile (2025): Commission Withdraws AI Liability Directive After Vance Attack on Regulation. *Euractiv*, 2025. február 11. Online: www.euractiv.com/news/commission-withdraws-ai-liability-directive-after-vance-attack-on-regulation
- DEDOLA, Luca et al. (2023): *Digitalisation and the Economy: ECB Working Paper Series, No. 2809*. Frankfurt am Main: European Central Bank.
- Department of Justice (2024): *Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons*. Online: www.justice.gov/nsd/media/1382521/dl
- DI MARCO, Diletta et al. (2025): *Open but Not Powerless: Towards a Common Understanding of EU Digital Sovereignty*. Ispra: European Commission.
- DOAN, Lynn – STOLTON, Samuel (2025): Trump Blasts EU Regulators for Targeting Apple, Google, Meta. *Bloomberg*, 2025. január 23. Online: www.bloomberg.com/news/articles/2025-01-23/trump-blasts-eu-regulators-for-targeting-apple-google-meta
- DRAGHI, Mario (2024a): *Address by Mr. Draghi: Presentation of the Report on the Future of European Competitiveness (European Parliament, Strasbourg, 17 September 2024)*. Online: https://commission.europa.eu/document/download/fcbc7ada-213b-4679-83f7-69a4c2127a25_en?filename=Address+by+Mario+Draghi+at+the+Presentation+of+the+report+on+the+future+of+European+competitiveness.pdf&prefLang=en&utm

- DRAGHI, Mario (2024b): *The Future of European Competitiveness, Part B: In-Depth Analysis and Recommendations*. Luxembourg: Publications Office of the European Union.
- DRAGHI, Mario (2025): *The Future of European Competitiveness, Part A: A Competitiveness Strategy for Europe*. Luxembourg: Publications Office of the European Union. Online: <https://doi.org/10.2872/9356120>
- ELBAUM, Sebastian – SEGAL, Adam (2025): What If China Wins the AI Race? *Foreign Affairs*, 2025. június 13. Online: www.foreignaffairs.com/united-states/what-if-china-wins-ai-race
- European Commission (2018): *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Artificial Intelligence for Europe*. COM(2018) 237 final, 2018. április 25. Online: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52018DC0237>
- European Commission (2020a): *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Shaping Europe's Digital Future*. COM(2020) 67 final, 2020. február 19. Online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020DC0067>
- European Commission (2020b): *Inception Impact Assessment on the Digital Services Act Package: Ex Ante Regulatory Instrument for Large Online Platforms with Significant Network Effects Acting as Gate-Keepers in the European Union's Internal Market*. Ares (2020) 2877647, 2020. június 2. Online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=int-com:Ares%282020%292877647>
- European Commission (2020c): *White Paper On Artificial Intelligence – A European Approach to Excellence and Trust*. COM(2020) 65 final, 2020. február 19. Online: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52020DC0065>
- European Commission (2020d): *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data*. COM(2020) 66 final, 2020. február 19. Online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020DC0066>
- European Commission (2024): *Protecting Competition in a Changing World: Evidence on the Evolution of Competition in the EU During the Past Years*. Brussels: Publications Office of the European Union. Online: <https://doi.org/10.2763/089949>
- European Commission (2025a): *Communication from the Commission to the European Parliament and the Council: Data Union Strategy – Unlocking Data for AI*. COM(2025) 835 final, 2025. november 19. Online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025DC0835>
- European Commission (2025b): *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions. A Competitiveness Compass for the EU*. COM(2025) 30 final, 2025. január 29. Online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025DC0030>
- European Commission (2025c): *European Commission Presents Its Compass to Boost Europe's Competitiveness in the Next Five Years*. *European Commission*, 2025. január 30. Online: https://ec.europa.eu/commission/presscorner/detail/en/ac_25_385

- European Commission (2025d): *Simpler EU Digital Rules and New Digital Wallets to Save Billions for Businesses and Boost Innovation*. European Commission, 2025. november 19. Online: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2718
- European Commission (2025e): *Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI)*. COM(2025) 836 final, 2025. november 19. Online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025PC0836>
- European Commission (2025f): *Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus)*. COM(2025) 837 final, 2025. november 19. Online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025PC0837>
- European Commission (2025g): *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: AI Continent Action Plan*. COM(2025) 165 final, 2025. április 9. Online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025DC0165>
- European Commission (2025h): *Communication from the Commission to the European Parliament and the Council: Apply AI Strategy*. COM(2025) 723 final, 2025. október 8. Online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025DC0723>
- European Commission (2025i): *Digital Package*. European Commission, 2025. november 25. Online: <https://digital-strategy.ec.europa.eu/en/faqs/digital-package#:~:text=Hence%2C%20we%20are%20introducing%20a,the%20reporting%20effort%20in%20half>
- European Commission (2026a): *Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European Cybersecurity Certification Framework, and ICT Supply Chain Security and Repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2)*. COM(2026) 11 final, 2026. január 20. Online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52026PC0011>
- European Commission (2026b): *Proposal for a Directive of the European Parliament and of the Council amending directive (EU) 2022/2555 as regards simplification measures and alignment with the [Proposal for the Cybersecurity Act 2]*. COM(2026) 13 final, 2026. január 20. Online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52026PC0013>
- European Council (2024): *Budapest Declaration on the New European Competitiveness Deal*. European Council, 2024. november 8. Online: www.consilium.europa.eu/en/press/press-releases/2024/11/08/the-budapest-declaration
- European Data Protection Supervisor (2016): *Opinion 8/2016: EDPS Opinion on Coherent Enforcement of Fundamental Rights in the Age of Big Data*. Online: www.edps.europa.eu/data-protection/our-work/publications/opinions/big-data_en

- European Digital Rights (2025): *Why the Digital Omnibus Puts GDPR and ePrivacy at Risk*. Online: https://edri.org/wp-content/uploads/2025/11/202511-Eexplaining-GDPR_epri-privacy-Digital-Omnibus.pdf
- European Parliament – European Council (2002): *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*. 32002L0058 jelzetű EU-dokumentum, 2002. július 12. Online: <http://data.europa.eu/eli/dir/2002/58/oj>
- European Parliament – European Council (2016): *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. 32016R0679 jelzetű EU-dokumentum, 2016. április 27. Online: <http://data.europa.eu/eli/reg/2016/679/oj>
- European Parliament – European Council (2019): *Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services*. 32019R1150 jelzetű EU-dokumentum, 2019. június 20. Online: <http://data.europa.eu/eli/reg/2019/1150/oj>
- European Parliament – European Council (2022): *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*. 32022L2555 jelzetű EU-dokumentum, 2022. december 14. Online: <http://data.europa.eu/eli/dir/2022/2555/oj>
- European Parliament – European Council (2023): *Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act)*. 32023R2854 jelzetű EU-dokumentum, 2023. december 13. Online: <https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng>
- European Parliament (2026): *European Parliament Resolution of 22 January 2026 on European Technological Sovereignty and Digital Infrastructure*. P10 TA(2026)0022 jelzetű EU-dokumentum, 2026. január 22. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202603697
- Federal Register (2024): *Preventing Access to Americans’ Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern*. *Federal Register*, 2024. február 28. Online: www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related
- FLEMING, Sean (2025): *What Is Digital Sovereignty and How Are Countries Approaching It?* *World Economic Forum*, 2025. január 10. Online: www.weforum.org/stories/2025/01/europe-digital-sovereignty
- HULKÓ, Gábor – KÁLMÁN, János – LAPSÁNSZKY, András (2025): *The Politics of Digital Sovereignty and the European Union’s Legislation: Navigating Crises*. *Frontiers in Political Science*, 7, 1–9. Online: <https://doi.org/10.3389/fpos.2025.1548562>

- KOMAITIS, Konstantinos – SHERMAN, Justin (2021): US and EU Tech Strategy Aren't as Aligned as You Think. *Brookings*, 2021. május 11. Online: www.brookings.edu/articles/us-and-eu-tech-strategy-arent-as-aligned-as-you-think
- KRETSCHMER, Martin et al. (2023): Europe and the Global Race to Regulate AI: Why the EU Should Focus On Data Quality and Liability Rules. *Verfassungsblog*, 2023. november 10. Online: <https://verfassungsblog.de/europe-and-the-global-race-to-regulate-ai>
- LARSEN, Benjamin Cedric (2022): The Geopolitics of AI and the Rise of Digital Sovereignty. *Brookings*, 2022. december 8. Online: www.brookings.edu/articles/the-geopolitics-of-ai-and-the-rise-of-digital-sovereignty
- LAURER, Moritz – RENDA, Andrea – YEUNG, Timothy (2021): Clarifying the Costs for the EU's AI Act. *CEPS*, 2021. szeptember 24. Online: www.ceps.eu/clarifying-the-costs-for-the-eus-ai-act
- LESLIE, Will (2023): Brussels Effect? Convergence and Divergence on Platform Regulation In Transatlantic Competition Policy. *TechREG Chronicle**, 3(4), 49–53.
- LEVI-FAUR, David (2005): The Global Diffusion of Regulatory Capitalism. *Annals of the American Academy of Political and Social Science*, 598(1), 12–32. Online: <https://doi.org/10.1177/0002716204272371>
- MADIEGA, Tambiama (2020): *Digital Sovereignty for Europe*. Brussels: European Parliamentary Research Service.
- MADIEGA, Tambiama – ILNICKI, Rafał (2024): AI Investment: EU and Global Indicators. *European Parliamentary Research Service*, 2024. április 4. Online: <https://epthinktank.eu/2024/04/04/ai-investment-eu-and-global-indicators>
- MAHER, Richard (2024): European Perspectives on Geoeconomics. In AGGARWAL, Vinod K. – CHEUNG, Tai Ming (szerk.): *The Oxford Handbook of Geoeconomics and Economic Statecraft*. Oxford: Oxford University Press, 395–410. Online: <https://doi.org/10.1093/oxfordhb/9780197673546.013.29>
- MALINGRE, Virginie (2025): European Digital Regulation Comes Under Attack from Trump, Musk and Zuckerberg. *Le Monde*, 2025. január 13. Online: www.lemonde.fr/en/economy/article/2025/01/13/european-digital-regulation-comes-under-attack-from-trump-musk-and-zuckerberg_6737001_19.html?srsltid=AfmBOorU1y5WAKyhr5bQiRSf7-3FB0jc-mdO4tYOf3Ap5gu1KkNiSpU7
- MARTONYI, János (2019): Law and Identity in the European Integration. *Hungarian Journal of Legal Studies*, 60(3), 227–235. Online: <https://doi.org/10.1556/2052.2019.00014>
- MCBRIDE, Keegan (2025): The Rise of Tech-Enabled States. *The Republic*, 2025. április 1. Online: <https://therepublicjournal.com/essays/the-rise-of-tech-enabled-states>
- MEZEI, Kitti (2025): Governing Digital Ecosystems in the EU: A Coordinated Regulatory Approach. *DOT.PL*, 2(1), 1–14. Online: <https://doi.org/10.60097/DOTPL/215839>
- MUELLER, Benjamin (2021): *How Much Will the Artificial Intelligence Act Cost Europe?* Online: <https://datainnovation.org/2021/07/how-much-will-the-artificial-intelligence-act-cost-europe>
- NOYB (2025): *Digital Omnibus: First Analysis of Select GDPR and ePrivacy Proposals by the Commission*. Vienna: NOYB – European Center for Digital Rights.

- PITTMAN, Paul et al. (2025): DOJ Issues Final Rule Prohibiting and Restricting Transfers of Bulk Sensitive Personal Data. *White & Case*, 2025. február 27. Online: www.whitecase.com/insight-alert/doj-issues-final-rule-prohibiting-and-restricting-transfers-bulk-sensitive-personal
- POHLE, Julia – THIEL, Thorsten (2020): Digital Sovereignty. *Internet Policy Review*, 9(4). Online: <https://doi.org/10.14763/2020.4.1532>
- PŘIBÁŇ, Jiří (2007): *Legal Symbolism: On Law, Time and European Identity*. Aldershot: Ashgate.
- RAMAHANDRY, Tiana et al. (2021): Key Enabling Technologies for Europe's Technological Sovereignty. Brussels: European Parliamentary Research Service.
- SHAFIQUE, Muhammad (2016): *Essays on the Role of Knowledge, R&D, and Technology-Based Firms in the Evolution of Socio-Techno-Economic System*. PhD-disszertáció. Universitaire Pers Maastricht. Online: <https://doi.org/10.26481/dis.20160419ms>
- STOLTON, Samuel (2021): LEAK: Commission in Bid for EU Data Sovereignty with Digital Decade Targets. *Euractiv*, 2021. március 8. Online: www.euractiv.com/news/leak-commission-in-bid-for-eu-data-sovereignty-with-digital-decade-targets
- TEPPER, Jonathan – HEARN, Denise (2018): *The Myth of Capitalism: Monopolies and the Death of Competition*. Hoboken, NJ: Wiley.
- The Economist (2017): The World's Most Valuable Resource Is No Longer Oil, but Data: The Data Economy Demands a New Approach to Antitrust Rules. *The Economist*, 2017. május 6. Online: www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data
- The White House (2022): *National Security Strategy*. Washington, DC: The White House.
- The White House (2025): *Winning the Race: America's AI Action Plan*. Washington, DC: The White House.
- THIERER, Adam (2016): *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom*. Arlington, VA: George Mason University Mercatus Center.
- TÓTH András (2020): A mesterséges intelligencia szabályozásának paradoxonja és egyes jogi vonatkozásainak alapvető kérdései. *Infokommunikáció és Jog*, 16(73), 3–14.
- TÓTH András (2025): Versenyjog és Magyarország az Európai Unióban. In GÁRDOS-OROSZ Fruzsina – OSZTOVITS András – VARJU Márton (szerk.): *Az európai jog szerepe a magyar jogfejlődésben 2004–2024: Személyes esszék Magyarország európai uniós tagságának első húsz évéről*. Budapest: Osiris, 233–256.
- United Nations Conference on Trade and Development (2021): *Digital Economy Report 2021: Cross-Border Data Flows and Development: For Whom the Data Flow*. New York: United Nations Publications.
- VON DER LEYEN, Ursula (2024): *Europe's Choice: Political Guidelines for the Next European Commission 2024–2029*. Strasbourg: European Commission.
- WALTER, Andre (2024): EU and China to Tackle Challenges of Cross-Border Transfer of Non-Personal Data. *Pinsent Masons*, 2024. augusztus 30. Online: www.pinsentmasons.com/out-law/news/eu-china-tackle-challenges-cross-border-transfer-non-personal-data

WU, Xiangning (2020): Technology, Power, and Uncontrolled Great Power Strategic Competition Between China and the United States. *China International Strategy Review*, 2, 99–119. Online: <https://doi.org/10.1007/s42533-020-00040-0>

YAŞAR, Ayşe Gizem (2025): Regulating the Digital Economy in the EU: The Hope of Redistribution. *LSE Legal Studies Working Paper*, 19(ksz): 34. Online: <https://doi.org/10.2139/ssrn.5893147>

Tóth András egyetemi docens, a Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar Digitális és Technológia Jogi Tanszékének vezetője. 2010 óta a Gazdasági Versenyhivatal elnökhelyettese, a Versenytanács elnöke. A *European Competition and Regulatory Law Review* szerkesztőbizottsági tagja. A Central European Lawyers Initiative és a Jáki Szaniszló Társaság elnöke.