Az EU AI Act hazai implementációja: Jogi, kormányzási és biztonsági kockázatok a mesterséges intelligencia megfelelésében

Herman Zsuzsanna

Debreceni Egyetem, Debrecen, Magyarország
Levelező szerző, e-mail: drhermanzsuzsanna@gmail.com

Beérkezett: 2025. december 1.; elfogadva: 2026. január 5.

Összefoglalás

A tanulmány azt vizsgálja, miként illeszkedik az Európai Unió mesterséges intelligenciáról szóló rendelete (EU 2024/1689 – AI Act) és annak hazai végrehajtása, a 2025. évi LXXV. törvény a magyar jogi és intézményi környezetbe. A kutatás különös figyelmet fordít a kockázatalapú szabályozás logikájára, a *trustworthy AI* elvének érvényesülésére, valamint a *human-in-the-loop* követelmény gyakorlati megvalósítására. A vizsgálat kvalitatív jogelemzési és szabályozás-összehasonlító módszereket alkalmazott. Eredményei szerint Magyarország jelentős előrelépést tett a hatósági és infrastrukturális végrehajtás terén, azonban a szervezeti kultúra és az etikai érettség fejlettsége még nem éri el a kívánatos szintet. Ez a hiányosság biztonságpolitikai kockázatokat is hordoz, különösen a kritikus infrastruktúrák és a közszolgáltatások területén. A tanulmány javaslatokat fogalmaz meg az etikai irányelvek fejlesztésére, a szervezeti integritás erősítésére és az MI-compliance rendszerek mélyebb beágyazására a hazai kormányzási gyakorlatba.

Kulcsszavak: mesterséges intelligencia, AI Act, megfelelés, kormányzás, kockázatelemzés

Implementation of the EU AI Act in Hungary: Legal, governance and security risks in Artificial Intelligence compliance

Zsuzsanna Herman

University of Debrecen, Debrecen, Hungary

Summary

This paper explores how Regulation (EU) 2024/1689 on artificial intelligence (AI Act) is being implemented in Hungary and how the European Union's risk-based governance model is translated into the national legal and institutional landscape. It examines the intersection between legal compliance, organizational governance, and security-oriented risk management in the context of AI technologies. The central question concerns how the EU's trustworthy AI paradigm—grounded in legality, transparency, accountability, and human oversight—can be effectively operationalized within Hungarian administrative and organizational practice.

Methodologically, the study applies qualitative legal interpretation, comparative regulatory analysis, and document-based content examination. It draws on EU-level materials (AI Act, EDPB guidelines, OECD AI Principles), international standards (ISO/IEC 42001:2023), and national legal instruments such as Act LXXV of 2025 and Government Decree 344/2025 (X. 31.). This multi-layered approach allows for a comprehensive assessment of the emerging governance architecture surrounding AI regulation in Hungary.

The findings show that Hungary has made notable progress in establishing the institutional infrastructure required for AI oversight—creating the Hungarian Artificial Intelligence Council, introducing a regulatory sandbox, and designating competent authorities. These measures align the national framework with the EU's risk-based logic of classification, conformity assessment, documentation, and human control. Yet, the research also reveals that domestic

compliance practices remain largely formalistic and enforcement-driven. While the regulatory framework is strong, the internal culture of ethical awareness, proactive risk management, and transparency within organizations is still at an early stage of development.

A key contribution of this study is the identification of a structural imbalance between legal-institutional maturity and the ethical risk culture of organizations. This gap represents a latent security vulnerability: high-risk AI systems demand not only regulation and supervision but also continuous ethical reflection, built-in auditability, and ethics-by-design principles. Without strengthening human-in-the-loop mechanisms and clear accountability structures, the full implementation of the AI Act risks remaining procedural rather than substantive.

The paper concludes that enhancing Hungary's AI governance capacity requires a shift from formal compliance to value-based integrity governance. It recommends embedding AI compliance into organizational management systems, fostering interdisciplinary competence centers, supporting empirical research on AI governance, and cultivating a national AI culture that values transparency, accountability, and human-centric oversight. Strengthening these dimensions is essential not merely for regulatory alignment but for sustaining public trust, institutional integrity, and long-term societal security.

Keywords: artificial intelligence, AI Act, compliance, governance, risk analysis

Bevezetés

A mesterséges intelligencia (MI) a 21. század egyik legmeghatározóbb technológiai és társadalmi jelensége. Az elmúlt évtizedekben az MI fejlődése nem csupán technológiai áttöréseket hozott, hanem alapjaiban kérdőjelezte meg a jog, az etika és a felelősség hagyományos kereteit. Sokáig nem volt világos, mit is értünk pontosan „mesterséges intelligencia" alatt, és ez a bizonytalanság mind a gazdasági, mind a közszférában érezhető kockázatokat teremtett.

Erre a kihívásra válaszul az Európai Unió 2024-ben elfogadta a mesterséges intelligenciáról szóló (EU) 2024/1689 rendeletet, közismertebb nevén az *AI Act*et, amely a világ első átfogó, horizontális MI-szabályozási keretrendszere *(European Commission 2024)*. A rendelet célja kettős: egyrészt az MI-alkalmazások kockázatainak kezelése és az emberi alapjogok védelme, másrészt egy olyan bizalomra épülő, technológiai ökoszisztéma kialakítása, amely ösztönzi az innovációt *(European Commission 2024; Laux–Wachter–Mittelstadt 2024)*.

Már a jogszabály definíciós része is heves vitákat váltott ki. Ződi Zsolt rámutat, hogy az európai MI-rendelet (AI Act) fogalmi alapjai is vitathatók *(Ződi 2025)*. A rendelet definíciója – amely szerint az MI „gépi alapú rendszer, amely autonóm módon képes célorientált kimenetek előállítására" – egyszerre tűnik túl általánosnak és túl absztraktnak. Ződi szerint ez a kettősség komoly problémát okoz a jogalkalmazásban, mert nem világos, hol húzódik a határ a hagyományos algoritmus és a valóban „intelligens" rendszer között. Ez nemcsak elméleti kérdés: a gyakorlatban is bizonytalanságot okoz, hogy mely rendszerekre terjed ki a rendelet, és melyekre nem. A tanulmány egyik legfontosabb felismerése, hogy a szabályozás nem képes kezelni az MI-rendszerek folyamatos tanulását és adaptivitását. A „statikus" definíció miatt az AI Act kockázati logikája idővel elcsúszhat a valós technológiai működéstől. Ez a probléma a tagállami implementációban is megjelenhet: például egy adott rendszer besorolása – „magas" vagy „korlátozott" kockázatú – a technológia fejlődésével megváltozhat, anélkül, hogy a rendelet maga módosulna. Ződi szerint éppen ezért elkerülhetetlen lenne egy pontosabb, funkcionális megközelítés, amely különválasztja a valóban intelligens, adaptív rendszereket a hagyományos, szabályalapú algoritmusoktól *(Ződi 2025)*. Egy funkcionális értelmezést javasol: az MI-t nem pusztán technikai jegyei alapján kellene azonosítani, hanem annak döntéstámogató szerepe, tanulási képessége és társadalmi hatása szerint. Ezzel a nézőponttal az AI Act rugalmasabb, a gyakorlatban is értelmezhető keretté válhatna.

Ez a megközelítés összhangban áll az AI Act általános céljaival, de új megvilágításba helyezi az európai szabályozás lényegét. Az EU 2024-ben elfogadott AI Actje ugyanis nemcsak technológiai normákat határoz meg, hanem egy átfogó kormányzási és megfelelési rendszert is létrehoz, amely az etikus működés, az elszámoltathatóság és az átláthatóság elveire épül *(European Commission 2024; Cancela-Outeda 2024; Laux–Wachter–Mittelstadt 2024)*.

A szabályozás emellett a kockázatalapú besorolás logikáját követi, amely az MI-rendszereket négy kategóriába sorolja: elfogadhatatlan, magas, korlátozott és minimális kockázatú rendszerek. A magas kockázatú rendszerek, például biometrikus azonosítás vagy egészségügyi döntéstámogató algoritmusok esetében kötelező a megfelelőségi értékelés, az átláthatósági követelmények teljesítése, valamint az emberi felügyelet („human-in-the-loop") biztosítása *(Kappel 2024; Okoro 2024)*.

Európa tehát egy értékalapú digitalizációs modellt választott: az emberi méltóság, a biztonság és az átláthatóság védelmét helyezi előtérbe. Míg az Egyesült Államok inkább az innovációvezérelt, Kína pedig az államközpontú megközelítést követi, addig az Európai Unió a felelős és etikus technológiai fejlődést tekinti irányelvnek *(Birher et al. 2019)*.

Magyarország az uniós kötelezettségeknek megfelelően 2025-ben elfogadta a 2025. évi LXXV. törvényt, amely az AI Act hazai végrehajtását és az MI-felügyeleti intézményrendszer kialakítását szolgálja. A törvény kijelölte a Nemzeti Akkreditáló Hatóságot (NAH) mint be-

jelentő hatóságot, valamint a vállalkozásfejlesztésért felelős minisztert mint piacfelügyeleti hatóságot, továbbá létrehozta a Magyar Mesterséges Intelligencia Tanácsot mint stratégiai koordinációs testületet (344/2025. [X. 31.] Korm. rendelet).

A magyar jogszabály ezzel megteremtette az első nemzeti AI-governance keretrendszert, amely összhangban áll az uniós szabályozással, ugyanakkor figyelembe veszi a magyar közigazgatási és vállalati sajátosságokat.

A kutatás időszerűségét két tényező adja: egyrészt az AI Act tagállami végrehajtása az uniós jogalkotás egyik legaktuálisabb feladata, másrészt az MI-irányításaktualitás és a megfelelés összekapcsolása új tudományos és kormányzási kérdéseket vet fel. A mesterséges intelligencia ma már nem pusztán technológiai kérdés, hanem társadalmi–intézményi, etikai és biztonságpolitikai kihívás is – működésének feltétele a bizalom, az elszámoltathatóság és az emberi felügyelet biztosítása *(Okoro 2024; European Data Protection Board 2024)*.

Vizsgálati anyag és módszer

A kutatás fő célja annak feltárása, hogyan illeszkedik az Európai Unió mesterséges intelligenciáról szóló rendelete (EU 2024/1689 – AI Act) a magyar jogi és intézményi környezetbe. A vizsgálat középpontjában három kulcsterület állt: a megfelelés (compliance), az irányítás (governance) és a biztonsági–kockázati követelmények kapcsolata.

A vizsgálat négy elemzési irányra épül: az AI Act elméleti és jogi alapjainak bemutatása, a nemzetközi megfelelési és szabványosítási keretek (OECD ISO/IEC 42001:2023) elemzése, a magyar jogi és intézményi adaptáció értékelése, végül pedig a három dimenzió szintézisét végeztem el, külön hangsúllyal a kockázatalapú és biztonsági megközelítésekre.

A kutatás módszertana kvalitatív és deduktív megközelítést követ. Alkalmazott módszerek: normatív jogelemzés, amely a rendelet és a kapcsolódó magyar jogszabályok értelmezésére irányult; összehasonlító szabályozásvizsgálat, amelyben az EU-s és a hazai végrehajtási mechanizmusok kerültek összevetésre; valamint tartalomelemzés, amely uniós szakpolitikai dokumentumok, nemzetközi standardok és lektorált tudományos források feldolgozásán alapult.

A vizsgálat a következő dokumentumok körére terjedt ki: EU AI Act és kapcsolódó uniós háttéranyagok *(European Commission 2024)*, OECD AI Principles (2023) és ISO/IEC 42001:2023 MI-irányítási szabvány. A magyar végrehajtási joganyagok: 2025. évi LXXV. törvény, 344/2025. (X. 31.) kormányrendelet, 1028/2025. (II. 24.) kormányhatározat, valamint Magyarország Mesterséges Intelligencia Stratégiája (2025–2030); végül a releváns nemzetközi és hazai szakirodalom (pl. *Laux–Wachter–Mittelstadt 2024; Cancela-Outeda 2024; Okoro 2024; Kappel 2024; Bederna 2025; European Data Protection Board 2024*).

A kutatás újdonságértéke abban áll, hogy az AI Actet nem kizárólag jogi normaként, hanem egy működő, integrált irányítási és megfelelési rendszerként vizsgálja, biztonsági–kockázati perspektívából is. Ez lehetővé teszi annak értékelését, hogy a hazai AI-governance mennyiben felel meg a szabályozási érettség követelményeinek, és hogy a szervezeti kockázati kultúra és etikai érettség hiányosságai milyen biztonságpolitikai kockázati rést teremtenek a magyar MI-megfelelési gyakorlatban.

Az EU AI Act főbb jogi és elméleti alapjai

A mesterséges intelligencia (MI) szabályozása napjainkra az európai uniós jog egyik legösszetettebb, ugyanakkor leginnovatívabb területévé vált. Az Európai Unió mesterséges intelligenciáról szóló, 2024/1689/EU rendelete – közismert nevén az AI Act – a világ első átfogó, horizontális szabályozási kerete, amelynek célja, hogy az MI-technológiák biztonságos, etikus és jogszerű módon működjenek az uniós belső piacon. A jogpolitikai törekvés kettős. Egyrészt az innováció és a mesterséges intelligencia gazdasági hasznosítása felé mutat, másrészt az alapvető jogok védelmét, a jogállamiság érvényesülését és a társadalmi bizalom megőrzését is szem előtt tartja *(Laux–Wachter–Mittelstadt 2024)*. Ez a kettősség adja az AI Act igazi karakterét: egyszerre ösztönöz fejlődést, miközben határt is szab annak.

Az AI Act az uniós szabályozási hagyományokhoz igazodva egy kockázatalapú modellt alkalmaz. A GDPR-ból is ismerős ez a logika. A rendelet négy kategóriát különít el: elfogadhatatlan, magas, korlátozott és minimális kockázatú rendszereket különböztet meg. Az első csoportba tartoznak például a társadalmi pontozási rendszerek és a megfigyelő algoritmusok, amelyek az emberi méltóságot sértik. A magas kockázatú rendszerek – mint a biometrikus azonosítás vagy az egészségügyi döntéstámogatás – viszont csak szigorú megfelelőségi értékelés után, megfelelő emberi felügyelet mellett működhetnek *(Cancela-Outeda 2024; Floridi–Holweg 2024)*.

A rendelet filozófiája a „Trustworthy AI" koncepcióra épül, amelyet az Európai Bizottság Mesterséges Intelligencia Szakértői Csoportja dolgozott ki az *Ethics Guidelines for Trustworthy AI* (2019) dokumentumban *(European Commission High-Level Expert Group on AI 2019)*. A bizalomra építő megközelítés három pillérre támaszkodik: a jogszerűségre, az etikus működésre és a technikai-üzemi robusztusságra. Ez a hármas elv a „humánközpontú" MI-felfogás alapja, amely az európai AI-governance szívében áll.

Az AI Act nem csupán tiltásokat sorol fel. Létrehoz egy európai irányítási architektúrát is, ahol az European Artificial Intelligence Office (AIO) koordinálja a tagállami hatóságok munkáját, biztosítva az egységes alkalmazást és a közös értelmezést *(Cantero Gamito–Marsden 2024)*.

A jogszabály újszerűsége részben abban rejlik, hogy a *ko-reguláció,* vagyis a társszabályozás elvét alkalmazza.

Ennek értelmében a folyamatokat nem kizárólag az állami és uniós hatóságok irányítják: a szabványosítási szervezetek – például a CEN-CENELEC, az ISO vagy az IEC – szintén kulcsszerepet játszanak a megfelelési követelmények meghatározásában. Az ISO/IEC 42001:2023 szabvány például a mesterséges intelligencia irányítási rendszerek nemzetközi normáit rögzíti, és várhatóan az AI Act gyakorlati végrehajtásának egyik sarokpontja lesz *(Wagner–Janssen 2024)*. A rendelet ezzel a *compliance by standardisation* megközelítést valósítja meg: a megfelelés a technológiai és etikai sztenderdek implementálásán keresztül jön létre *(Cantero Gamito–Marsden 2024)*.

A szabályozásnak természetesen erős adatvédelmi és etikai dimenziója is van. A GDPR és az AI Act közötti kapcsolat több szinten megfigyelhető: a jogalap, a célhoz kötöttség, az átláthatóság és az elszámoltathatóság elvei mindkét keretben azonos módon érvényesülnek *(European Data Protection Board 2024; Binns–Veale 2021; Tutt–Pasquale 2024)*. Az adatvédelem így nem önálló sziget, hanem a mesterséges intelligencia megfelelésének szerves része.

A felelősség kérdése külön fejezetet érdemelne. Az automatizált döntéshozatal és a humán felügyelet viszonya új, sokszor nehezen kezelhető kihívásokat hoz az uniós és tagállami gyakorlatban. Az AI Act ezért kimondja: minden olyan rendszerben, ahol emberi életet vagy alapjogot érintő döntés születik, kötelező a humán felügyelet. A „human-in-the-loop" megközelítés célja, hogy a gépi döntéshozatal soha ne váljon önjáróvá, és a folyamat átlátható, ellenőrizhető maradjon *(Okoro 2024; Selbst 2024)*. Ez az elv nemcsak technikai, hanem etikai biztosíték is.

Az AI Act mögött meghúzódó jogpolitikai gondolkodás végső soron az európai értékalapú digitalizáció vízióját tükrözi. Míg az Egyesült Államok inkább az innovációra, Kína pedig az állami irányításra építi modelljét, addig az Európai Unió a jogállamiság, az emberi méltóság és az átláthatóság hármas értékrendjét helyezi a középpontba *(Birher et al. 2019)*. Így az AI Act nem pusztán jogi norma, hanem kormányzási paradigma is – egy integrált modell, amelyben a megfelelés, az elszámoltathatóság és az etika egységes rendszerben érvényesül.

Az EU AI Act és a nemzetközi megfelelési keretek

Az EU AI Act nem elszigetelt jogi sziget az uniós jogrendszerben. Sokkal inkább a korábbi megfelelési és adatvédelmi keretek természetes továbbfejlesztése. A szabályozás – a GDPR-hoz hasonlóan – kockázatalapú megközelítésből indul ki: az MI-rendszerek használatával járó kockázatok azonosítása, értékelése és kezelése képezi a megfelelés magját *(Tutt–Pasquale 2024)*. A GDPR által megerősített elszámoltathatóság elve *(accountability)* az AI Actben már nemcsak a szervezetekre, hanem magukra a technológiai rendszerekre is kiterjed. Ennek eredményeként kialakul az *AI governance compliance* új, integrált fogalma *(Binns–Veale 2021)*. A mesterséges intelligenciával foglalkozó fejlesztők, üzemeltetők és felhasználók között ezzel új felelősségi viszonyok jönnek létre: az auditálás, a felügyelet és a jogorvoslat egymásra épülő rendszere *(Okoro 2024)*.

A kockázatalapú megfelelés ugyanakkor nem pusztán jogi kérdés. Legalább annyira szervezeti és technológiai is. Az ISO/IEC 42001:2023 szabvány – az MI-irányítási rendszerek első nemzetközi menedzsmentszabványa – az AI Act technikai párjaként értelmezhető. Meghatározza az MI-rendszerek fejlesztésének, működtetésének és felügyeletének alapvető követelményeit *(Bederna 2025)*. A szabvány a *compliance by design* elvet követi: a megfelelés nem utólagos ellenőrzés, hanem a fejlesztési folyamat beépített része.

Ez a gondolkodás a ko-reguláció logikáját tükrözi. Az AI Act szerint a jogalkotás és a szabványosítási szervezetek – például a CEN-CENELEC, az ISO vagy az IEC – egymást kiegészítő rendszert alkotnak *(Cantero Gamito–Marsden 2024)*. Az OECD AI Principles (2019) ehhez adja az etikai és társadalmi hátteret, amelyet az EU a rendelet preambulumában is megidéz. Különösen hangsúlyos az az alapelv, miszerint „az MI-nak az emberek és a társadalom javát kell szolgálnia". Az uniós modell tehát nem új értékrendet teremt, hanem a már létező nemzetközi normákat emeli kötelező jogi szintre.

A megfelelési rendszer egyik kulcsa, hogy az etikai elvek és a jogi normák szorosan összefonódnak benne. Laux, Wachter és Mittelstadt ezt a folyamatot „soft law to hard law" átalakulásként írják le: ami korábban ajánlás volt – például az átláthatóság vagy a humán felügyelet –, az az AI Actben már jogi kötelezettséggé vált *(Laux–Wachter–Mittelstadt 2024)*. A Trustworthy AI koncepció, amelyet a High-Level Expert Group on AI az *Ethics Guidelines for Trustworthy AI* dokumentumban rögzített *(European Commission HLEG 2019),* ma már kötelező megfelelési alapelv. A magyar jogi és intézményi környezet e tekintetben átmeneti állapotban van. A *Magyarország Mesterséges Intelligencia Stratégiája 2020–2030* már lefektette az etikus MI-irányítás alapelveit, de a részletes megfelelési struktúrák még formálódnak. Bederna rámutat arra, hogy az MI-megfelelés nem merül ki technikai követelményekben: az AI Act szerinti megfelelés integrált irányítási rendszert, kockázatmenedzsmentet, adatvédelmi és kiberbiztonsági kontrollokat, valamint etikai megfontolások szervezeti beágyazását is feltételezi *(Bederna 2025)*. Magyarországon – hasonlóan más új szabályozási területekhez – az AI Act alkalmazása kezdetben várhatóan erősebben kötődik majd a kötelező megfelelési követelmények teljesítéséhez, mint az önkéntes etikai vállalásokhoz.

Kappel ehhez kapcsolódva kiemeli, hogy az MI-alapú döntéstámogató rendszerek jogi és etikai kockázatainak kezelése új típusú megfelelési mechanizmusokat igényel *(Kappel 2024)*. A *human-in-the-loop* elv nemcsak technikai biztonsági feltétel, hanem compliance-alapelv is: biztosítja, hogy az emberi tényező ne tűnjön el a döntésho-

zatalból *(Okoro 2024; Selbst 2024)*. A humán kontroll kiterjed az automatizált döntések következményeinek értékelésére, az elfogultságok csökkentésére, valamint az adatvédelmi és társadalmi hatások nyomon követésére.

Mindezek alapján megállapítható, hogy az EU AI Act komplex, többszintű megfelelési ökoszisztémát hoz létre. Ebben a jogi, technológiai, szervezeti és etikai normák egymással összefonódva működnek. Az uniós modellhez való alkalmazkodás kettős kihívást jelent a magyar jogalkotás és az intézményrendszer számára: egyrészt a jogi követelmények pontos átvételét, másrészt a hazai AI-governance kultúra fokozatos kialakítását.

A hazai jogi és intézményi környezet

Az Európai Unió mesterséges intelligencia rendeletének (EU AI Act) magyarországi végrehajtása új szakaszba lépett a 2025. évi LXXV. törvény elfogadásával. A jogszabály – teljes címén „a mesterséges intelligenciáról szóló európai uniós rendelet végrehajtásáról és a mesterséges intelligencia hatósági felügyeletéről" – kijelöli a hazai intézményi struktúrát, meghatározza a felügyeleti hatóságok hatáskörét, és rögzíti a megfelelőségi feladatok elosztását.

A törvény célja kettős: egyfelől az EU AI Act végrehajtásának biztosítása a magyar jogrendben, másfelől olyan nemzeti felügyeleti és koordinációs mechanizmusok létrehozása, amelyek garantálják az MI-rendszerek jogszerű és etikus alkalmazását (2025. évi LXXV. törvény 1. §).

A részletes végrehajtási szabályokat a 344/2025. (X. 31.) kormányrendelet tartalmazza. Ez határozza meg az uniós rendelet hazai végrehajtásához szükséges intézményi és eljárási kereteket. A jogszabály nem alapított új hatóságot, hanem két, már működő szervezetet jelölt ki a feladatok ellátására. Az egyik a Nemzeti Akkreditáló Hatóság (NAH), amely a magas kockázatú MI-rendszerek megfelelőségértékelésének és kijelölésének hatósági feladatait látja el. A NAH feladatai közé tartozik a megfelelőségértékelő szervezetek kijelölése, tevékenységük ellenőrzése, valamint a megfelelőségi rendszer éves felülvizsgálata és jelentés készítése a Magyar Mesterséges Intelligencia Tanács számára. A másik kijelölt szerv a piacfelügyeleti hatóság, amelyet a vállalkozásfejlesztésért felelős miniszter irányít. Hatásköre a mesterséges intelligencia rendszerek piacfelügyeleti ellenőrzésére, a jogszerű működés vizsgálatára, valamint a közigazgatási bírságok kiszabására terjed ki. A hatóság működteti továbbá az MI-szabályozói tesztkörnyezetet, amely az innováció és a jogalkalmazási tapasztalatok integrált fejlesztését szolgálja. A rendelet előírja, hogy a két hatóság évente számoljon be a Magyar Mesterséges Intelligencia Tanácsnak az AI Act hazai alkalmazásának tapasztalatairól és a piacfelügyeleti tevékenység eredményeiről. Ezen túlmenően azonban érdemes megvizsgálni, mi indokolta éppen ennek a két szervezetnek a kijelölését. Jogpolitikai és szervezetrendszertani szempontból a döntés alkotmányos logikát követ. A NAH kijelölése a hatósági akkreditációs tapasztalatok és a nemzetközi szabványosítási kapcsolatok miatt volt indokolt – az MI-rendszerek megfelelősége ugyanis technikai és szabványalapú terület. A piacfelügyeleti funkció viszont a végrehajtó hatalomhoz illeszkedik, amelynek felelőssége a piaci működés jogszerűségének biztosítása.

A két intézmény együttműködése kettős hatású: egyrészt decentralizálja a felügyeletet, másrészt erősíti az intézményi átláthatóságot, hiszen az egyik a technikai, a másik a gazdasági–piaci aspektusokat felügyeli. Ez a konstrukció illeszkedik a magyar közigazgatási rendszer horizontális hatásmegosztásához és az európai kormányzási mintákhoz is.

A Magyar Mesterséges Intelligencia Tanács a kormány mesterségesintelligencia-stratégiájának szakmai koordinátora. Nemcsak beszámolókat fogad, hanem iránymutatásokat és ajánlásokat is készít, valamint összehangolja a kutatási és szabályozási tevékenységeket. Tagjai között megtalálhatók a főbb állami szervek (pl. NAIH, GVH, MNB), az akadémiai intézmények, gazdasági szereplők, valamint a Digitális Jólét Program (DJP) és a Nemzeti Mesterséges Intelligencia Koalíció, amelyek a szakpolitikai ökoszisztéma civil és szakmai pillérét képviselik *(Magyar Közlöny 2025/152)*.

Ez az intézményi modell egy nemzeti AI-governance architektúrát valósít meg, amely a kockázatalapú szabályozásra és az emberi felügyelet követelményére épül. A felügyelet középpontjában a magas kockázatú MI-rendszerek állnak: például az egészségügyi, közlekedési, pénzügyi vagy közigazgatási alkalmazások. A jogalkotó itt különös figyelmet fordított az átláthatóságra, az adatkezelésre és az emberi felügyelet fenntartására.

A 2025. évi LXXV. törvény nem csupán intézményi reform, hanem a hazai megfelelési kultúra erősítésének egyik első állomása. A törvény előírja, hogy a közszféra és a vállalati MI-rendszerek üzemeltetői kötelesek létrehozni belső megfelelőségi mechanizmusokat. A megbízható és átlátható működést dokumentált kockázatkezelési és kontrollfolyamatokkal kell biztosítani. Ez összhangban áll azzal a megfelelési logikával, amelyben az AI-irányítási rendszer együttműködik a minőségirányítási, információbiztonsági és adatkezelési rendszerekkel *(Bederna 2025)*. A fentiekből látható, hogy a hazai AI-governance nem egységes, centralizált intézményként működik, hanem három funkcionális szintet lefedő rendszerként, amely különböző szereplők együttműködésén alapul.

Ez a struktúra biztosítja a nemzeti jogalkotás és az uniós szabályozás összhangját, miközben illeszkedik a magyar közigazgatás és az innovációs kormányzás hagyományaihoz.

1. Stratégiai irányítási szint. A stratégiai döntéshozatal és a szakpolitikai koordináció központi eleme a Magyar Mesterséges Intelligencia Tanács, Digitális Jólét Program, Innovációs és Technológiai Minisztérium. Feladatuk a szakpolitikai koordináció, az MI-stratégia

végrehajtásának támogatása és az uniós megfelelés folyamatos biztosítása. A DJP által kidolgozott Mesterséges Intelligencia Stratégia (2020) a nemzeti irányítási keret alapja.
2. Felügyeleti és végrehajtási szint. Ez a szint biztosítja az AI Act operatív végrehajtását.
   – A Nemzeti Akkreditáló Hatóság (NAH) működik MI-bejelentő hatóságként: a nagy kockázatú MI-rendszerek megfelelőségértékelését végző szervezetek kijelöléséért és felügyeletéért felel.
   – Az MI piacfelügyeleti hatóság feladatait a vállalkozásfejlesztésért felelős miniszter látja el. Ez a hatóság vizsgálja az MI-rendszerek megfelelését, piacfelügyeleti eljárásokat folytat, közigazgatási bírságokat szabhat ki, és működteti az MI-szabályozói tesztkörnyezetet (2025. évi LXXV. tv. 10. §), amely lehetőséget biztosít az innováció és a szabályozási tapasztalat együttes fejlesztésére.
3. Szakmai önszabályozás és társadalmi együttműködés. A szakmai és önszabályozási mechanizmusokat a Nemzeti Mesterséges Intelligencia Koalíció, a Magyar Szabványügyi Testület, az egyetemi etikai bizottságok és kutatóintézetek biztosítják. Ezek a szervezetek a Tanáccsal és a kormányzati szereplőkkel együttműködve dolgoznak a mesterséges intelligencia felelős alkalmazásának etikai, biztonsági és oktatási keretein. A koalíció – amely 2018-ban jött létre több mint háromszázötven taggal – a magyar AI-stratégia megvalósításának szakmai motorja, és közvetlenül kapcsolódik az OECD, az EU AI Office és az ISO/IEC 42001:2023 szabványrendszer irányelveihez.

Elmondható, hogy a magyar AI-governance rendszer egy hálózatos, funkcionálisan differenciált modell, amelynek erőssége a különböző hatósági, szakmai és társadalmi szereplők együttműködésében rejlik. A rendszer kifejezetten a kockázatalapú szabályozásra, az emberi felügyelet („human-in-the-loop") elvére és az átlátható, auditálható működésre épül, megfelelve az AI Act által megfogalmazott uniós elvárásoknak. A modell sikere attól függ, hogy a jogi megfelelésen túl mennyire sikerül elmélyíteni az etikus, felelősségteljes és transzparens AI-használat kultúráját a köz- és magánszférában.

Összességében a 2025. évi LXXV. törvény és a 344/2025. kormányrendelet a hazai AI-governance struktúra alapjait teremtette meg. A jövő kihívása nemcsak a jogi követelmények átültetése lesz, hanem az is, hogy az átláthatóság, a humán kontroll és az etikus AI-használat kultúrája valóban beépüljön a szervezeti működésbe.

Az EU AI Act hazai végrehajtásának aktuális fejleményei (2025)

A Magyar Kormány a 2025. évi LXXV. törvény felhatalmazása, valamint a 344/2025. (X. 31.) kormányrendelet alapján hozta létre a Magyar Mesterséges Intelligencia Tanácsot, amely stratégiai iránymutatást ad az MI-fejlesztések nemzeti szintű koordinálásához *(Országgyűlés Hivatala 2025)*. A Tanács munkáját a Mesterséges Intelligencia Hivatal támogatja, amelyet az 1028/2025. (VI. 21.) kormányrendelet hozott létre. A Hivatal felel a szakpolitikai és szabályozási végrehajtásért, különösen az MI-rendszerek kockázati besorolása és a megfelelőségértékelési mechanizmusok területén. A nemzeti szabályozás egyik legfontosabb innovációja a „regulatory sandbox", vagyis a szabályozói tesztkörnyezet. Az 1301/2024. (IX. 30.) kormányhatározat alapján ez a keret lehetőséget ad arra, hogy az új MI-fejlesztések korlátozott, felügyelt környezetben kerüljenek kipróbálásra. Így a jogalkotó egyszerre támogatja az innovációt és őrzi meg az etikai, valamint adatvédelmi megfelelést *(Infojegyzet 2025)*. Ezzel Magyarország az uniós tagállamok élvonalába került a mesterséges intelligencia területén, mivel a szabályozói sandbox az egyik leginnovatívabb kockázatkezelési megoldás, amelyet korábban csak Spanyolország és Finnország alkalmazott a gyakorlatban. Spanyolországban az *AI Sandbox* (2023) az adatvédelem és a pénzügyi technológiák összehangolt kockázatkezelési rendszerére épült. A spanyol megközelítés előnye, hogy az innovációt erősen intézményi felügyelet mellett engedi kibontakozni – ezt a logikát a magyar rendszer is átvette, különösen az előzetes megfelelőségértékelés és a dokumentációs követelmények tekintetében. Finnország viszont a *pilot projektek decentralizált modelljét* alkalmazta, amelyben a kutatóintézetek, az egyetemek és a közintézmények közösen tesztelik az MI-rendszerek megfelelését. Ezáltal a modell rugalmasabb, de nagyobb felelősséget ró az üzemeltetőkre. A magyar szabályozás a két megközelítés ötvözését választotta: központi irányítás mellett enged innovációt, de megköveteli a felügyeletet és az etikai kontrollt. Ez a hibrid megoldás közelíti Magyarországot a „regulációs élvonalhoz", miközben csökkenti az újszerű bevezetés „gyermekbetegségeit".

A végrehajtás során kormánybiztos felügyeli az MI-hatósági rendszer kiépítését. Ez a pozíció nem pusztán koordinatív, hanem jogpolitikai súlyú: a kormánybiztos feladata a kockázatalapú felügyeleti modellek és a compliance-orientált vizsgálati eljárások bevezetése. Az új szabályozási logika szorosan kapcsolódik a megfelelés (compliance) érettségi szintjeihez. A vállalatoknak és a közintézményeknek bizonyítaniuk kell, hogy MI-rendszereik megfelelnek az AI Act 9–15. cikkeiben rögzített átláthatósági, dokumentációs és auditálási követelményeknek *(Európai Parlament és Tanács 2024)*.

A magyar AI-végrehajtási rendszer nem csupán technológiai projekt. A szabályozásba beépültek az integritásalapú kormányzás elemei is: etikus működés, felelősségi láncok tisztázása és kockázatalapú auditálás. Mindez azt jelenti, hogy az implementáció nemcsak adatvédelmi vagy technológiai kérdés, hanem etikai és szervezeti integritási kihívás. A Mesterséges Intelligencia Hivatal feladatköre ennek megfelelően bővült: nemcsak a jogi megfelelést ellenőrzi, hanem a felelősségi láncokat, az

etikai megfelelést és az auditálási gyakorlatokat is figyelemmel kíséri. A magyar megközelítés ezáltal egyre közelebb kerül a *governance-driven compliance* modellhez, amelyet a nemzetközi szakirodalom is meghatározó trendként azonosít *(Laux–Wachter–Mittelstadt 2024; Okoro 2024)*. A modell lényege, hogy a megfelelés és az etika nem külön funkciók, hanem az MI-rendszerek működésének integrált, folyamatos ellenőrzési keretei. A magyar kormányzati gyakorlat ennek megfelelően a hagyományos közigazgatási ellenőrzést kiegészíti a szervezeti kultúra és az etikus döntéshozatal fejlesztésével.

A hazai végrehajtási modell sikerét több tényező határozza meg. Egyrészt az intézményi megfelelés és az átláthatóság biztosítása, másrészt annak képessége, hogy a szabályozás mögött valós etikai kultúra épüljön ki mind a közszférában, mind a vállalati környezetben. A jelenlegi fejlemények abba az irányba mutatnak, hogy a humán felügyelet, az átláthatóság és a kockázatalapú auditálás a magyar AI-governance központi pilléreivé válhatnak.

Magyarország ezzel – Spanyolország és Finnország tapasztalataiból tanulva – nemcsak követi, hanem részben formálja is az uniós szabályozási irányokat. A hazai implementáció ezért nem pusztán adaptáció, hanem kísérleti laboratórium, ahol az etika, a jog és az innováció közös platformon találkozik.

Ugyanakkor fontos látni, hogy a magyar modell – bármennyire is előremutató – több ponton további finomhangolásra szorul. Az egyik ilyen terület a szabályozói sandbox gyakorlati működése. Bár a kísérleti környezet csökkenti a fejlesztési kockázatokat, túlzott adminisztratív terhet is jelenthet a kisebb fejlesztők számára, akik nem rendelkeznek belső jogi vagy megfelelőségi apparátussal. Ennek orvoslására érdemes lenne egyszerűsített megfelelőségi csatornákat kialakítani, különösen az oktatási és a KKV-szektor számára. Másrészt a kockázati kategorizálás és a humán felügyelet gyakorlati érvényesítése jelenleg még nem kellően egységes. A hatósági iránymutatások és a piaci szereplők közötti kommunikáció erősítése nélkül a megfelelés gyakran formális maradhat.

Végül a magyar AI-governance hosszú távú sikerét az fogja meghatározni, hogy képes-e proaktív kockázatkezelési kultúrát kialakítani – olyat, amely nem csupán reagál a problémákra, hanem előre azonosítja és kezeli azokat. Ehhez nemcsak jogi, hanem etikai és intézményi innováció is szükséges.

Elemzés és értelmezés

Az Európai Unió mesterséges intelligenciáról szóló 2024/1689-es rendelete (EU AI Act) és annak magyarországi adaptációja, a 2025. évi LXXV. törvény nem csupán új szektorális szabályozást hozott létre, hanem egy olyan kormányzási és megfelelési paradigmaváltást, amely a mesterséges intelligenciát technológiai objektumból társadalmi–institucionális kockázati tényezővé minősíti át. A két jogszabály közös elve a „kockázatalapú megfelelés" (risk-based compliance), amely a technológiai, jogi, adatvédelmi és etikai kockázatok integrált értékelését teszi a szabályozási logika középpontjává *(Tutt–Pasquale 2024)*.

A nemzetközi megfelelési keretrendszer – különösen az ISO/IEC 42001:2023 szabvány – azt mutatja, hogy az MI-szabályozás földrajzi és intézményi környezetektől függetlenül hasonló mintázatokat követ: kockázatértékelés, átláthatósági kötelezettségek, technikai–etikai kontrollok, emberi felügyelet, auditálhatóság. Ez a struktúra jelenik meg mind az AI Actben, mind a magyar végrehajtási szabályozásban *(Cantero Gamito–Marsden 2024)*.

A hazai jogalkotás ugyanakkor sajátos hangsúlyokat hordoz. Míg az EU AI Act kiemelten támogatja a *transparency by design* és az *ethics by design* megközelítéseket, addig Magyarországon inkább a hatósági kontroll, az ellenőrzési jogosítványok és a piacfelügyeleti auditálás dominálnak. A Magyar Mesterséges Intelligencia Tanács létrehozása fontos koordinációs lépés, de a szakirodalom szerint *(Birher et al. 2019)* a magyar kormányzási struktúrában az önszabályozó és etikai dimenziók jelenleg kevésbé erősek, mint a formális megfelelési mechanizmusok.

A hazai szervezetek MI-megfelelési gyakorlata – különösen a közszférában – még erőteljesen „külső megfelelés alapú" (reactive compliance). Jelenleg a szabályozási kényszer az elsődleges motiváló tényező, nem pedig a belső, értékalapú integritás vagy az önkéntes etikai vállalások. Ezt a trendet támasztja alá Bederna és Papp elemzése is, amelyek szerint az MI-alkalmazások elszámoltathatósága, átláthatósága és etikai felügyelete erősen függ a szervezeti kultúrától *(Bederna 2025; Papp 2025)*.

A „human-in-the-loop" elv *(Okoro 2024; Selbst 2024)* központi jelentőségű mind az EU-s, mind a magyar szabályozásban. Ez a követelmény két funkciót lát el. Az egyik a garanciális szerep: ez biztosítja az emberi felügyeletet, hogy a kritikus döntések feletti kontroll ne kerülhessen át teljesen az automatizált rendszerhez. A másik a compliance-funkció, amely a humán kontroll auditnyomvonalának elsődleges megfelelőségi mechanizmusaként szolgál a high-risk kategóriákban. Kappel szerint a vezetői döntéstámogató MI-rendszerek olyan új típusú kockázatokat hoznak létre – például a döntési felelősség elmosódását, az automatizált torzítások erősödését vagy a túlzott technológiai bizalmat –, amelyek a korábbi compliance-rendszerekben nem voltak jelen *(Kappel 2024)*. Ez szükségessé teszi a kontroll- és az integritásmechanizmusok újragondolását. A trustworthy AI koncepció – amelyet a High-Level Expert Group 2019-es irányelve fektetett le – mára az EU jogi keretrendszerének kötelező elemévé vált *(European Commission HLEG 2019; Laux–Wachter–Mittelstadt 2024)*. A magyar jogalkotás ezt részben beemelte a nemzeti szabályozásba, de a szakirodalom szerint *(Birher et al. 2019)* a normatív beágyazottság és a társadalmi legitimáció csak akkor lesz teljes, ha az etikai elvek nemcsak a jogszabá-

lyokban, hanem a szervezeti kultúrában és napi gyakorlatban is érvényesülnek.

Az összehasonlító elemzés alapján az AI Act és a magyar jog közös metszete a *governance-driven compliance*, amelyben a megfelelés nem csupán jogi kötelezettség, hanem az MI-rendszerek felelős működésének kormányzási alapelve, amely a szervezeti integritást, az etikus működést és az átláthatóságot összehangolt mechanizmusként kezeli. A magyar modell sikeressége azon múlik, hogy ezek a mechanizmusok mennyiben tudnak proaktív etikai kultúrává alakulni, túl a puszta szabályozói megfelelésen.

Összességében megállapítható, hogy bár a magyar szabályozás összhangban áll az uniós kockázatalapú modell elveivel, a gyakorlatban több kihívás is azonosítható. A megfelelőségi auditok jelenleg túlnyomórészt formai ellenőrzésre épülnek, miközben az etikai és humán szempontok beépítése még nem egységes. Az egyik lehetséges irány a *compliance maturity model* bevezetése lenne, amely lehetővé tenné, hogy az MI-rendszerek megfelelőségi szintjei az érettség és az etikai teljesítmény alapján differenciálhatók legyenek. Emellett szükség lenne egy egységes, nyilvános kockázatértékelési protokollra, amely segítené a vállalati és a közszférabeli szereplőket az AI Act gyakorlati alkalmazásában.

A mesterséges intelligencia biztonsági és kockázatelemzési aspektusai – a „high-risk governance" modell értékelése

A mesterséges intelligencia biztonsági és kockázati dimenziói az elmúlt években a nemzetközi szakirodalom egyik legizgalmasabb kutatási területévé váltak. A diskurzus egyre kevésbé technológiai, egyre inkább intézményi és biztonságpolitikai kérdésként közelíti meg az MI-t. A legtöbb szerző arra figyelmeztet, hogy a mesterséges intelligencia nem pusztán új ipari technológia, hanem kritikus infrastruktúra jellegű rendszer, amely képes befolyásolni a társadalmi stabilitást, az információs biztonságot és a jogrendet (lásd pl. *Brundage et al. 2023; Heinrich–Heinecke–Krüger 2023*).

Az EU AI Act erre a felismerésre reagálva nemcsak kockázatokat kategorizál, hanem azokhoz normatív kormányzási logikát is rendel.

A nemzetközi biztonsági diskurzus fő irányai

A nemzetközi szakirodalom három fő kockázati területet azonosít.

1. Elsőként a *technikai és rendszerszintű kockázatok* jelentkeznek. Idesorolhatók az algoritmikus hibák, a modellrobusztusság hiányosságai, az elfogultság (bias) vagy az *adversarial* támadások, amikor a rendszert megtévesztő inputokkal próbálják manipulálni *(Yu et al. 2022)*. A kockázat ebben az esetben mérhető és kontrollálható – ám csak addig, amíg a szervezet ismeri a modell határait. A probléma az, hogy sok fejlesztő „fekete dobozként" kezeli saját rendszerét.
2. Másodikként az *intézményi és irányítási kockázatok* jelennek meg. Ezek nem a technológiából, hanem az irányítás hiányosságaiból erednek. Ha nincs kompetens felügyeleti szervezet, vagy a felelősségi láncok elmosódnak, akkor a „high-risk" rendszerek auditálása formális aktussá válik *(OECD 2023)*.
3. Harmadikként a *társadalmi és biztonságpolitikai kockázatok* emelhetők ki. Az algoritmikus döntések átláthatatlansága, a tömeges megfigyelés lehetősége és a jogbiztonsági aggályok – különösen a rendészeti vagy igazságügyi MI-rendszerekben – mélyen beavatkoznak az alapvető jogok terébe *(Laux–Wachter–Mittelstadt 2024)*.

Ez a három réteg együtt magyarázza, miért kezelik a mesterséges intelligenciát egyre inkább kritikus infrastruktúra jellegű technológiaként, amelynek védelme nem szűkíthető le informatikabiztonsági kérdésekre.

A kockázatalapú megközelítés biztonsági jelentősége az EU AI Actben

Az EU AI Act kockázatalapú struktúrája – amely az MI-rendszereket elfogadhatatlan, magas, korlátozott és minimális kockázatú kategóriákba sorolja – első ránézésre jogtechnikai konstrukciónak tűnhet, a biztonsági tudomány szempontjából azonban irányítási és kockázatpolitikai modellként is értelmezhető *(Cantero Gamito–Marsden 2024)*.

A magas kockázatú rendszerekre előírt kötelezettségek, például a folyamatos kockázatmenedzsment-rendszer, az adatminőség- és modelldokumentáció, a robusztussági és biztonsági tesztek, az emberi felügyelet és a beavatkozási pontok, a naplózás és az auditálhatóság együttesen biztonsági kontrollrendszert alkotnak. Heinrich, Heinecke és Krüger ezt a logikát a klasszikus *security-by-design* és *defense-in-depth* megközelítés kiterjesztéseként értelmezi az MI-rendszerekre: a biztonság nem utólagos javítás, hanem a teljes életciklusba beépített kontroll *(Heinrich–Heinecke–Krüger 2023)*. Álláspontom szerint a jogi keret itt még mindig konzervatív: bár a rendelet hangsúlyozza a „biztonság mint folyamat" elvet, a gyakorlati alkalmazás sok helyen statikus megfelelési listává válik. Ennek korrekciója érdekében a biztonsági tanúsítások mellé érdemes lenne bevezetni dinamikus kockázatkezelési protokollokat, hasonlóan a pénzügyi szektorban alkalmazott „stress-test" modellekhez.

Az emberi felügyelet mint biztonsági garancia

Az AI Act egyik legerősebb újítása, hogy az emberi felügyeletet biztonsági garanciaként kezeli. A *human-in-the-loop* és *human-on-the-loop* modellek célja, hogy a döntési folyamat kritikus pontjain az emberi kontroll ne

tűnjön el az automatizmus mögött *(Okoro 2024; Selbst 2024)*.

A szakirodalom rámutat, hogy az automatizált döntésekkel kapcsolatos legnagyobb kockázat nem a hibás predikció önmagában, hanem az, amikor a döntéshozók „rábízzák magukat" a rendszerre (automation bias): amikor a felelősség „elmosódik" az ember és a gép között, és amikor nincs kialakult eljárás a hibás döntések felismerésére és korrigálására *(Kappel 2024)*.

Biztonságpolitikai szempontból ez különösen kritikus a rendészeti, határigazgatási, pénzügyi szektorbeli és igazságszolgáltatási MI-rendszereknél, ahol a hibás döntések jogbiztonsági és társadalmi stabilitási kockázatot hordoznak. Az emberi felügyelet ezért nem pusztán „etikai extra", hanem a rendszer biztonságának egyik központi pillére. A magyar implementációban ennek kezelésére a szabályozói sandbox adhat keretet, de csak akkor, ha az emberi tényezőt nem csupán „felügyeletként", hanem aktív tanuló szereplőként értelmezzük. Ezzel a sandbox nemcsak a technológia, hanem az emberi döntéshozatal biztonsági laboratóriuma is lehetne.

Magyar biztonsági kontextus: a szabályozói sandbox és a piacfelügyelet szerepe

A magyar jogi és intézményi környezetben a biztonsági és kockázati aspektusokat elsősorban a 2025. évi LXXV. törvény, a 344/2025. (X. 31.) kormányrendelet, valamint a szabályozói tesztkörnyezet (regulatory sandbox) hivatottak kezelni *(Magyar Közlöny 2025/143; Infojegyzet 2025)*. A sandbox előnye, hogy a kísérleti környezetben azonosíthatók a technikai és etikai kockázatok, még mielőtt a rendszer széles körű alkalmazásba kerülne.

Ez a megoldás nem magyar sajátosság. A spanyol és a finn példák bizonyították, hogy az ilyen tesztkörnyezetek csökkentik a „rendszersokkot", amelyet a szabályozatlan MI-bevezetések okozhatnak. Magyarország azonban – helyesen – erősebb piacfelügyeleti modellt választott. Ennek előnye, hogy központosított, így jobban biztosítja a biztonsági szint homogenitását. Hátránya viszont, hogy a szervezetek nem tanulnak meg önállóan kockázatot kezelni.

A jövőben érdemes lenne az állami felügyelet mellé önszabályozó etikai kódexeket és kötelező *risk learning* tréningeket bevezetni az MI-fejlesztők és -üzemeltetők számára. Ez segíthetné, hogy a biztonság ne csak szabályozási követelmény, hanem szervezeti reflex legyen.

Biztonságpolitikai következtetés: az MI-kockázatok „négy csomópontja"

A nemzetközi és hazai elemzések alapján négy csomópont azonosítható, amely meghatározza egy MI-rendszer biztonsági érettségét.

1. Technológiai biztonság: robusztus, tesztelt, támadásoknak ellenálló modellek.
2. Intézményi felügyelet: működő, szakmailag kompetens auditmechanizmus.
3. Etikai és jogi garanciák: emberi felügyelet, alapjogvédelem, átláthatóság.
4. Szervezeti kockázati kultúra: proaktív, integritásalapú döntéshozatal.

A tanulmány megállapítása szerint Magyarország az első három csomópontban érdemi előrelépést tett a szabályozás szintjén, ugyanakkor a negyedik – a szervezeti kockázati kultúra és az etikai érettség – terén még jelentős fejlődési potenciál mutatkozik. Ez a „kockázati rés" elsősorban nem jogi, hanem vezetéstudományi és kulturális probléma: hogyan alakítható ki olyan szervezeti környezet, ahol a biztonság nem kényszer, hanem közös felelősség.

A kutatás eredményei arra utalnak, hogy a jövő AI-stratégiáinak sikerét nem a szabályozás szigorúsága, hanem a tanulószervezeti modellek elterjedése fogja meghatározni. A mesterséges intelligencia nemcsak új kockázatokat, hanem újfajta biztonságpolitikai gondolkodást is követel – olyat, amelyben a felelősség, az etika és a technológiai innováció egy rendszerként működik.

Következtetések és ajánlások

Az Európai Unió mesterséges intelligenciáról szóló rendelete (Regulation (EU) 2024/1689 – AI Act) és annak magyarországi adaptációja, a 2025. évi LXXV. törvény nem pusztán egy új jogi keretrendszert hozott létre, hanem egyfajta szabályozási fordulatot is. Ez a fordulat abban áll, hogy az MI többé nem technológiai kérdés, hanem társadalmi és kormányzási felelősség tárgya. A mesterséges intelligencia alkalmazása ma már a jog, az etika és a szervezeti működés metszéspontján dől el. Az AI Act éppen ezt a hármasságot kívánja intézményesíteni a *trustworthy AI* elvére építve *(Laux–Wachter–Mittelstadt 2024)*. A magyar jogalkotás időben és tartalmilag is illeszkedett ebbe a folyamatba, azonban a megfelelés kultúrája és a governance–compliance összhangja még kialakulóban van.

A kutatás megállapította, hogy míg az EU AI Act a soft law eszközök, a nemzetközi szabványosítás (pl. ISO/IEC 42001:2023) és az etikus innováció elveit hangsúlyozza, addig a magyar végrehajtás jelenleg inkább hard law-orientált, vagyis hatósági kontrollra, formális megfelelésre és piacfelügyeleti auditokra épül. A két megközelítés céljai azonosak, de eszköztáruk hangsúlyai eltérnek, ami különösen a szervezeti szintű megfelelés és az etikai kultúra területén jelent kihívást.

Az etikai–intézményi fejlesztés iránya: az értékalapú MI-kultúra erősítése

A tanulmány eredményei alapján három kulcsfontosságú stratégiai irány körvonalazódik a hazai AI-governance továbbfejlesztéséhez.

Az első stratégiai irány az etikai és intézményi fejlesztés elmélyítése. Az MI-szabályozás akkor működik, ha az etikai elvek nemcsak deklarációként, hanem működési normaként jelennek meg. A trustworthy AI koncepció *(European Commission HLEG 2019)* világossá teszi: a megbízhatóság nem technikai minősítés, hanem emberi döntésminőség kérdése.

Bederna (2025) szerint az MI-kockázatkezelésben az irányítás kritikus szerepet játszik, mivel olyan folyamatok és dokumentációk kialakítását igényli, amelyek a kockázatok felismerését, értékelését és mérséklését szolgálják. A kutatás alapján a *reactive compliance* helyett a *proactive integrity governance* modellje felé kell elmozdulni – vagyis egy olyan környezet felé, ahol az etikus döntés nem külső kényszer, hanem szervezeti reflex.

Ennek érdekében elengedhetetlen az *ethics by design* elv alkalmazása, amely az etikai szempontokat a fejlesztési folyamat elejétől integrálja. Fontos lépés lenne továbbá az átlátható felelősségi láncok és az etikai auditok beépítése az MI-projektekbe. Ahogyan Papp fogalmaz: „Az etika nem kiegészítése, hanem alapfeltétele a megfelelésnek" *(Papp 2025)* – és ez a tétel különösen érvényes a mesterséges intelligencia korában.

Az MI-compliance beágyazása a szervezeti irányítási rendszerekbe

A második stratégiai irány az MI-compliance rendszerszintű integrálása a szervezeti működésbe. A mesterséges intelligencia ugyanis nem csupán technikai eszköz, hanem döntési infrastruktúra, amely – közvetve vagy közvetlenül – emberi felelősséget és társadalmi kockázatot hordoz.

Bederna (2025) elemzése alapján a magas kockázatú MI-rendszerek megfelelősége kockázatkezelési, dokumentációs, emberi felügyeleti, valamint kiberbiztonsági és adatvédelmi követelmények együttes teljesítéséhez kötődik. Ez jogilag biztonságos, de innovációs szempontból korlátozott. A hosszú távon fenntartható modell a compliance és a governance összekapcsolása, ahol a szervezetek nemcsak „végrehajtják" a jogot, hanem értelmezik is.

A *human-in-the-loop* elv kulcsszerepet játszik ebben *(Okoro 2024; Kappel 2024)*. A humán kontroll nem formai követelmény, hanem folyamatos biztonsági és etikai szűrő, amely képes mérsékelni az automatizált döntéshozatal kockázatait. Saját kutatói álláspontom szerint ezen a ponton a magyar rendszer egyik fő kihívása a „pszeudo-emberi" kontroll: a humán felügyelet gyakran csak dokumentált, nem valós. A jövőbeli szabályozásnak éppen ezt a gyakorlatot kell áttörnie – akár digitális naplózással, akár valós idejű auditmechanizmusokkal.

A tudományos és szakpolitikai szinergiák megerősítése

A harmadik irány a tudomány és a szakpolitika közötti kapcsolat újragondolása. Az MI-kormányzás multidiszciplináris tér: a jogtudomány, a közgazdaságtan, az informatika és az etika kölcsönhatásában képes fenntartható modelleket létrehozni.

A kutatás tapasztalatai szerint a magyar AI-governance fejlesztése csak akkor lehet hatékony, ha a tudományos szféra valós szerepet kap a szabályozás értékelésében és tervezésében. Ennek egyik eszköze lehet az empirikus megfelelési kutatások kiterjesztése – például az MI-rendszerek gyakorlati auditjainak és döntési torzításainak vizsgálata. Emellett szükség lenne multidiszciplináris doktori programokra és kutatóközpontokra, amelyek az MI-etika, a jog és a biztonságpolitika metszetében dolgoznak. Ez nem csupán tudományos kérdés, hanem politikai érettség kérdése is: a kormányzási innováció nem hozható létre kizárólag minisztériumi keretek között, csak együttműködő, tanuló ökoszisztémában.

A szervezeti kockázati kultúra és az etikai érettség mint a jövő kulcsa

A tanulmány egyik kulcsmegállapítása, hogy Magyarország a biztonság és a megfelelés négy eleméből (technológiai biztonság, intézményi felügyelet, etikai-jogi garanciák és szervezeti kockázati kultúra) az első három területen érdemi előrelépést tett, ugyanakkor a negyedik, a szervezeti kockázati kultúra és az etikai érettség terén még jelentős fejlesztési potenciál mutatkozik. Ez a különbség hozza létre azt a biztonságpolitikai kockázati rést, amelyre a jövőben a hazai AI-stratégiának, a közszféra intézményeinek és a vállalati szereplőknek egyaránt reagálniuk kell. Ez a megállapítás különösen releváns a kritikus infrastruktúrák, a közszolgáltatások és a rendészeti alkalmazások esetében, ahol a szervezeti érettség közvetlenül befolyásolja a társadalmi biztonságot és a közbizalmat. Ezen a téren a legfontosabb fejlesztési irány az etikai érettség mérése és ösztönzése. A „compliance maturity model" bevezetése – amely a szervezeteket nem csupán jogi, hanem etikai teljesítmény alapján értékeli – hozzájárulhatna a valódi kulturális áttöréshez. Ez a megközelítés már sikeresen működik a pénzügyi szektorban, és alkalmazható lenne a mesterséges intelligencia területén is.

A kutatás eredményei azt mutatják, hogy a compliance és a governance konvergenciája nem csupán jogi, hanem kulturális és szervezeti kihívás is. A magyar szabályozás hosszú távú hatékonysága attól függ, sikerül-e az AI-irányítási modelleket a szervezeti integritás és a társadalmi felelősségvállalás szintjén is beágyazni.

Láthattuk, hogy az EU AI Act és a magyar implementáció egy olyan hibrid mesterségesintelligencia-szabályozási ökoszisztémát hoz létre, amely a versenyképesség, a biztonság, a transzparencia és az etika céljait egyaránt szolgálja. A következő évtized kulcskérdése már nem a jogszabályi keretek megléte, hanem azok élő, felelős és értékalapú működtetése, amely jogászok, közgazdászok, technológiai szakemberek és döntéshozók közös felelőssége. A mesterséges intelligencia szabályozása egy új típu-

sú állam–technológia–etika viszonyt hoz létre. A jog ma már nem egyszerűen reagál a technológiai fejlődésre, hanem *partnerévé válik*. A szabályozás nem lezárt folyamat, hanem folyamatos társadalmi tanulás. És ha van tanulság, amelyet ebből a kutatásból levonhatunk, az talán az, hogy a mesterséges intelligencia korszakában az igazi kockázat nem maga a gép, hanem az emberi döntés hiánya.

Összegzés

Az EU AI Act és a magyar implementáció egy új, hibrid MI-szabályozási ökoszisztéma alapjait fektette le, amely egyszerre szolgálja a versenyképességet, a biztonságot, a transzparenciát és az etikai felelősséget. A jövő kulcskérdése nem a jogszabályok megléte, hanem azok érett, értékalapú működtetése lesz – egy olyan rendszeré, amelyben a mesterséges intelligencia nemcsak a fejlődést, hanem a bizalom és az emberi felelősség új kultúráját is megerősíti.

Irodalomjegyzék

2025. évi LXXV. törvény a mesterséges intelligenciáról szóló európai uniós rendelet végrehajtásáról. Magyar Közlöny, 2025/143. https://magyarkozlony.hu

344/2025. (X. 31.) Korm. rendelet az Európai Unió mesterséges intelligenciáról szóló rendeletének végrehajtásáról. Magyar Közlöny. https://magyarkozlony.hu

1028/2025. (VI. 21.) Korm. rendelet a Mesterséges Intelligencia Hivatal létrehozásáról. https://njt.hu/jogszabaly/2025-1028-30-22.0

1301/2024. (IX. 30.) Korm. határozat a mesterséges intelligencia fejlesztését támogató szabályozói tesztkörnyezet kialakításáról. https://njt.hu/jogszabaly/2024-1301-30-22

Bederna Zs. (2025) A mesterségesintelligencia-rendszerek megfelelősége. Hadmérnök, Vol. 19. No. 3. pp. 119–135. https://doi.org/10.32567/hm.2024.3.8

Binns, R. & Veale, M. (2021) Is that your final decision? Multi-stage profiling, selective effects, and Article 22 of the GDPR. Computer Law & Security Review, Vol. 41. Article No. 105577. https://doi.org/10.1016/j.clsr.2021.105577

Birher N., Fábryné Keszler N., Kulifay B. & Regős F. (2019) A mesterséges intelligencia alkalmazásának társadalmi hatásai a normaalkotásra, jogi és erkölcsi szempontok alapján. Humán Innovációs Szemle, Vol. 10. No. 1. pp. 4–16.

Brundage, M. et al. (2023) Frontier AI safety and policy: Managing emerging risks to public safety. AI Policy Forum. https://doi.org/10.48550/arXiv.2306.06012

Cancela-Outeda, P. (2024) The European Union Artificial Intelligence Act: Risk-based regulation for trustworthy AI. European Journal of Risk Regulation, Vol. 15. No. 2. pp. 245–267. https://doi.org/10.1017/err.2024.18

Cantero Gamito, M. & Marsden, C. T. (2024) Artificial intelligence co-regulation? The role of standards in the EU AI Act. International Journal of Law and Information Technology, Vol. 32. No. 2. https://doi.org/10.1093/ijlit/eaae011

Digitális Jólét Program (2020) Magyarország Mesterséges Intelligencia Stratégiája 2020–2030. https://digitalisjoletprogram.hu/hu/mi-strategia

Európai Parlament és a Tanács (2024) Regulation (EU) 2024/1689 of the European Parliament and of the Council on Artificial Intelligence (AI Act). Official Journal of the European Union, L 1689. pp. 1–148. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689

European Commission High-Level Expert Group on Artificial Intelligence (2019) Ethics Guidelines for Trustworthy AI. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

European Data Protection Board (EDPB) (2024) Guidelines on the interplay between the AI Act and the GDPR. https://edpb.europa.eu

Floridi, L. & Holweg, M. (2024) AI regulation as risk regulation: The logic of the EU AI Act. AI & Society. https://doi.org/10.1007/s00146-024-01729-6

Heinrich, T., Heinecke, F. & Krüger, F. (2023) Security-by-Design for Machine Learning Systems. IEEE Security & Privacy, Vol. 21. No. 4. pp. 47–57. https://doi.org/10.1109/MSEC.2023.3273374

Infojegyzet (2025) Az Európai Unió mesterséges intelligencia rendeletének végrehajtása. Országgyűlés Hivatala. Infojegyzet 2025/29. https://www.parlament.hu/documents/10181/1458893/Infojegyzet_2025_29_EU_MI_rendelet.pdf

Kappel, G. (2024). Mesterséges intelligencia alapú döntéstámogató és döntéshozó rendszerek kockázatai a vállalatok vezetői szintű döntéshozatalában: Szakirodalmi áttekintés. Pro Futuro, 14(1), 152–177. https://doi.org/10.26521/profuturo/2024/1/15166

Kormányzati határozatok (2024–2025) 1301/2024. (IX. 30.), 1028/2025. (VI. 21.), 1149/2025. (VII. 9.) kormányhatározatok a mesterséges intelligencia hazai szabályozásáról. Magyar Közlöny, 2024–2025. évi lapszámok. https://magyarkozlony.hu

Laux, J., Wachter, S. & Mittelstadt, B. (2024) Trustworthy Artificial Intelligence in the European Union: A legal and governance analysis of the AI Act. Computer Law & Security Review, Vol. 55. Article No. 105879. https://doi.org/10.1016/j.clsr.2024.105879

OECD (2023) OECD Artificial Intelligence Principles. OECD Publishing, Paris. https://oecd.ai/en/ai-principles

OECD (2024) AI Policy Observatory – Hungary Country Report. https://oecd.ai

Okoro, C. (2024) Ethical governance of Artificial Intelligence: The human oversight imperative under the EU AI Act. International Data Privacy Law, Vol. 14. No. 1. pp. 23–41. https://doi.org/10.1093/idpl/ipad015

Országgyűlés Hivatala (2025) Az EU MI Act végrehajtásának nemzeti keretei. Az Európai Unió mesterséges intelligencia rendeletének végrehajtása Magyarországon. Infojegyzet 2025/29. https://www.parlament.hu/infolapok

Papp R. (2025) A mesterséges intelligencia etikai kihívásai. Jogelméleti Szemle, Vol. 26. No. 1. pp. 51–72.

Selbst, A. D. (2024) The limits of human oversight in AI governance. AI and Ethics, Vol. 4. pp. 45–67. https://doi.org/10.1007/s43681-024-00412-7

Tutt, A. & Pasquale, F. (2024) The AI Act and data protection law: Intersections and tensions. International Data Privacy Law, Vol. 14. No. 2. pp. 113–129. https://doi.org/10.1093/idpl/ipad022

Wagner, B. & Janssen, M. (2024) Standardisation and certification challenges under the EU AI Act. Computer Law & Security Review, Vol. 53. Article No. 105900. https://doi.org/10.1016/j.clsr.2024.105900

Yu, T. et al. (2022) Adversarial robustness of AI systems: A survey. ACM Computing Surveys, Vol. 55. No. 12. pp. 1–38. https://doi.org/10.1145/3522785

Ződi Zs. (2025) A mesterséges intelligencia definíciójának problémái (és egy lehetséges megoldása) az európai MI-rendeletben. Gazdaság és Jog, Vol. 33. No. 3–4. pp. 8–13.