# Rideg Gergely: A mesterséges intelligencia rendszerek, mint magas kockázatú rendszerek szabályozásának európai megközelítése a tanúsítványok és szabványok tükrében

## Bevezetés

Az utóbbi évek európai jogalkotói vizsgálódásait többek között a mesterséges intelligencia (továbbiakban úgy is mint MI) szabályozásának kockázat alapú megközelítése jellemzi. A magas fejlettségi szintet képviselő technológia gigantikus kockázati jóslatokat hívott elő számos diszciplína jeles képviselői részéről. A kockázati faktorok az alapvető emberi jogok széles spektrumával kapcsolatot mutatnak, felhívva ezzel a figyelmet az MI-alkalmazás esetleges veszélyeire[1]. Nem újkeletű a gépektől, gyorsaságtól, vagy hirtelen fejlődéstől való félelem, és ez indokolt és arányos óvatosságot kell, hogy követeljen mind az alkalmazók mind a szabályalkotók részéről.

A jelen tanulmányban arra keresem a választ, hogy a tanúsítási folyamat, és a szabvány mennyiben lehet eszköze a mesterséges intelligencia arányos és indokolt szabályozásának, alkalmazása korlátozásának. Melyek lehetnek azok a kihívások, amelyek e téren feltűnni látszanak és mit várunk el a jogalkotótól, és a jogalkalmazótól? Megfelelő garanciákat jelentenek-e a tanúsítási folyamatok a mesterséges intelligencia használata során? Milyen legyen a szabályozási hozzáállás? Milyen legyen a szabályozás, ha magas kockázatú mesterséges intelligenciával találkozik? Milyen a megbízható mesterséges intelligencia? Mitől lesz magas kockázatú egy MI-alkalmazás? Képes lehet a szabványok alkalmazása által a jogalkotó megfelelő mértékben porlasztani az MI-alkalmazások jelentette kockázatot?

### A választott kutatási módszer

A kérdésekre normatív vizsgálatok útján, rendszertani értelmezéssel (interpretatio systematica), és kontextuális elemzéssel keresem a választ. Az analízis használja továbbá az alkotmányos alapjogok szerinti értelmezést, és úgyszintén a jog mögötti etikai értékek szerinti értelmezést. A kutatás során a teleológiai értelmezés játszik fontos szerepet.

### Kutatási kérdések

A kutatás során azt is vizsgálom, hogy milyen legyen az a szabályozási attitűd, amely a mesterséges intelligencia rendszerek szabályozását jellemzi. A következőkben meglátjuk,

hogy az európai jogalkotó gondolkodásában hogyan alakul a szabályozás akkor, amikor a magas kockázatú mesterséges intelligenciával rendelkezik. Arra is választ kapunk, hogy milyen a megbízható mesterséges intelligencia.

A szabályozási sarokpontok Európában

Jelen tanulmányban érintőlegesen, a teljes igénye nélkül utalunk azokra az állomásokra, amelyek a mesterséges intelligencia európai regulációjának evolúcióját követték.

## Mérföldkövek az Európai Unióban

Az egyik fundamentális mérföldkő a 2018. április 25-én lefektetett MI-stratégia volt, amely részben az MI társadalmi-gazdasági aspektusait, részben a körülötte megjelenő beruházásokat vizsgálta. Egy további lépés a „A mesterséges intelligenciáról szóló összehangolt terv”[2] elkészítése volt, amely tartalmazta a közös célokat, és irányt mutatott az együttes erőfeszítésekhez. A Bizottság a témával foglalkozó magas szintű független szakértői csoportot is létrehozott 2018-ban, amely etikai iránymutatást adott ki a megbízható mesterséges intelligenciára vonatkozóan. A megbízhatóság általában lényeges az ismeretlen technológiák szabályozása kapcsán.[3] A munkacsoport hét kulcsfontosságú követelményt rögzített, melyek a) Emberi cselekvőképesség és emberi felügyelet; b) Műszaki stabilitás és biztonság; c) Adatvédelem és adatkezelés; d) Átláthatóság; e) Sokféleség, megkülönböztetésmentesség és méltányosság; f) Társadalmi és környezeti jólét; valamint g) Elszámoltathatóság.

A munkacsoport rámutatott, hogy a megbízhatóság egyik szubsztanciája a bizalom. Az emberekben bizalom releváns, tudományosan megalapozott és hasznos információk alapján, széleskörű tájékoztatás útján tud kialakulni egy ismeretlen technológia iránt.

Az Európai Bizottság 2020. február 19. napján megjelent, a mesterséges intelligenciáról: a kiválóság és a bizalom európai megközelítéséről szóló Fehér könyvében (a továbbiakban úgy is mint Fehér könyv) az MI-alkalmazásokat illetően az alapvető jogokat, köztük az adatvédelmet, a magánélet védelmét és a megkülönböztetésmentességet érintő, valamint a biztonságot és a termékfelelősségi rendszer hatékony működését érintő kockázatokat elemezte.

Kifejtette, hogy az MI-alkalmazások termékekbe és szolgáltatások beépülve egyaránt kockázatot jelenthetnek. Mind a két esetben egyrészről a tervezési hibából eredő kockázat

járhat alapjogsértéssel, így például, ha olyan esettel találkozik az MI, amelyre hibásan beprogramozott választ ad, vagy pedig nem is kapott utasítást. Kockázatok eredhetnek abból is, ha az MI működésének alapjául nyers, kijavítás nélküli adatokat használnak fel. Az Európai Unió azt is felismerte, hogy bizonyos termékek és szolgáltatások esetében az MI éppen eszkaláló hatással van a termékben már egyébként is meglévő kockázatra, hiszen jóval nagyobb hatást képes gyakorolni a társadalomra az elvégzett munkafolyamatok száma és az érintettek száma végett.

Az MI szabályozás körében a jogbiztonságot megalapozó, garanciákkal rendelkező, ugyanakkor nem túlszabályozott, a gazdaságot támogató szabályozásra van szükség. Ebből kifolyólag objektív valószínűségi becslésekre, empirikus vizsgálatokra és nem sejtésekre alapozottan kell felmérni a kockázatot.[4]

Az Európai Parlament 2017. február 16-i állásfoglalása[5] a Bizottságnak szóló ajánlásokkal a robotikára vonatkozó polgári jogi szabályokról elkészült dokumentuma számos olyan alapvetést tartalmaz, amely a robotok, mint új technológiai entitások biztonságos működéséhez kapcsolódnak. Fontos megjegyezni, hogy ez az állásfoglalás is hangsúlyozza, hogy „a robotok valós élethelyzetekben történő tesztelése alapvető fontosságú az esetleges kockázatok, valamint a tisztán kísérleti laboratóriumi fázison túli technológiai fejlődésük feltárása és értékelése szempontjából”.

Az MI kapcsán a negatív események bekövetkeztének objektív valószínűségére vonatkozó becslések részben analógiákra alapulnak. Ismertek, dokumentáltak a számítógépes rendszerek egyes gyengepontjait kihasználó hacker-ek támadásai, amelyek jellemzően adatok (jelszavak, e-mail címek) megszerzésére irányulnak. Statisztikákkal alátámaszthatóan növekvő tendenciát mutat a cyber-bűncselekményeket elkövető csoportok száma. Ezeknek a csoportoknak az egyik fő célpontjai a később akár értékesíthető adatok.[6] Ismert továbbá a gyűlöletbeszéd elterjedése az online térben.[7]

A Fehér könyv által azonosított kockázatok mind az érintetti mind pedig a hatósági oldalon jelentkeznek, amely hatással van a jogbiztonságra, mivel az egyértelmű biztonsági intézkedések hiánya a jogbiztonság hiányához vezet, ugyanis egyértelmű rendelkezések hiányában a jogalkalmazók nem tudják, hogy hogyan járjanak el helyesen. Pontos szabályok nélkül a hatóságok és felügyeleti szervek is nehéz helyzetbe kerülnek, mert nem tudják, hogy mi alapján ellenőrizzenek.[8]

A Fehér könyvben a következő kockázati tényezők kerültek azonosításra:

a) Az MI különös jellemzői. A bonyolult algoritmusokon keresztül az is aggályos, hogy detektálni tudjuk, hol és ki követett el jogsértést.

b) Uniós jogszabályok alkalmazhatóságának korlátai az által például, hogy a termékbiztonsági jogszabályok termékekre vonatkoznak, és nem alkalmazhatók MI segítségével működő szolgáltatásokra.

c) Az MI-rendszerek életciklusuk során változhatnak, pl. szoftverfrissítésen keresztül.

d) Létezik egy bizonytalanság a felelősségnek az ellátási láncban részt vevő szereplők közötti megoszlása körében.

e) Magának a biztonság fogalmának a változása

A Fehér könyv alapvetően egy kockázatalapú megközelítést kívánt alkalmazni, illetve arányos beavatkozást javasolt, magas és nem magas kockázati szintű MI-alkalmazások között disztingvált.

A szabályozás konkrét kialakítása kapcsán az európai jogalkotó úgy látja, hogy a már meglévő rendeletekre, irányelvekre és állásfoglalásra lehet alapozni. Az MI-hez hasonló precedenseket lát például az adatvédelemmel kapcsolatosan már meglévő, az illegális online tartalom hatékony kezelésére irányuló intézkedésekről szóló bizottsági ajánlás tervezetében megjelenő kockázatértékelési megközelítésben.[9] Azzal együtt, hogy megállapítása szerint szükségesek újabb, a mesterséges intelligenciára szabott jogszabályok elkészítése, amelyeket aztán szabványokkal lehet tökéletesíteni. Izgalmas elképzelés, hiszen a szabványok Széll Sámuelt idézve tulajdonképpen „szakmai törvények”[10]. Vitathatatlan, hogy azok jól kezelik a műszaki, technikai megoldásokat, illetve, hogy a piaci szereplők gyorsabban reagálnak a változásokra, mint a jogalkotó.

A célirányos és arányos szabályozás kialakításához az európai koncepció szerint arra lesz szükség, hogy az adatok ellenőrzése, a tájékoztatás, az emberi felügyelete stb. a magas kockázatú MI-alkalmazások során a követelményekbe beépüljenek.

## A kialakuló MI-szabályozás első részeredményei

2020. október 20-án megjelent az Európai Parlament állásfoglalása[11] a Bizottságnak szóló ajánlásokkal a mesterséges intelligenciára vonatkozó polgári jogi felelősségi rendszerrel kapcsolatban, melyben kezdett formát ölteni az az elképzelés, amelyet a fent idézett

dokumentumok körvonalaztak.[12]

A javaslat magas kockázatú MI-rendszereket definiál, azzal, hogy meghatározza az MI-rendszereket, illetve a magas kockázatnak is definíciót ad.[13]

Az MI rohamosan fejlődő alkalmazása mellett az európai jogalkotó az egyik első olyan entitás a világon, amely átfogó szabályozási keretet vezet be ennek a paradigmaváltó technológiának egy meghatározott célra történő támogatására. Az MI átfogó szabályozását deklaráló javaslatot[14] a tanulmány írásakor az Európai Unió Tanácsa rendes jogalkotási eljárás keretében tárgyalja.[15] Ez a javaslat lényegében a magas kockázatú MI rendszerekre vonatkozó szabályokat tartalmazza. A magas kockázatú rendszerekbe történő besorolást a 6. cikk határozza meg, az egyes konkrét területeket pedig a III. melléklet sorolja fel. A magas kockázatot olyan esetekben tartja indokoltnak alkalmazni, amely az érintettek alapjogainak védelmével hozható kapcsolatba. A javaslat részletes tárgyalása nem tartozik jelen tanulmány körébe. Már több alkalommal említésre kerültek ugyanakkor a mesterséges intelligencia jelentette kockázatok. Helyesnek vélem, hogy pár mondatban kitérjünk arra, hogy pontosan mi az a kockázat, és miképpen mérjük közelítjük meg.

## Kockázatértékelés

Mit is értünk kockázat alatt? A kockázat valamely (negatív) esemény bekövetkezése gyakoriságának (valószínűségének) és az esemény (negatív) következményei mértékének a szorzatát jelenti. A gyakoriság és a súlyosság előzetes megítélésében ugyanakkor jelentős az eltérés a társadalmi érzékelés és a tudományos valószínűség alapján kialakított előre becslés értékelése között.[16] A mesterséges intelligencia által okozott negatív esemény lehet kisebb, egy kisebb csoportot érő adatvédelmi incidens, de lehet akár tömegszerencsétlenség, amely egy önvezető autó döntése miatt következik be. Ezek a negatív externáliák igen jelentősek a tekintetben, hogy hogyan kezeljük a mesterséges intelligenciát mint a szabályozás tárgyát. Nicolas Petit a mesterséges intelligencia által okozott externáliák három csoportját állította fel. A legenyhébbtől a legsúlyosabbig egyszer a helyi hatások, vagy diszkrét externáliák, amelyek csak az egyének szintjén jelentkeznek, ritkábbak. A második csoport a rendszerszintű hatások, amelyek lokalizáltak, kiszámíthatók. A harmadik csoport végül a történelmi jelentőségű externáliák, amelyek megjósolhatatlanok és végzetesek.[17] Látható, hogy e helyütt a mesterséges intelligencia rendszerek csoportosítása más szempontú. A gyenge és erős mesterséges intelligencia csoportosítások mellett ez a fajta elkülönítés alkalmas lehet arra, hogy a szabályozás még komplexebb legyen és így helyesen szolgálja a szabályozási célt.

Valamilyen szintű kockázatot természetesen mindenképpen vállalni kell egy versenyképes gazdaságban. Fontos ugyanakkor, hogy a kockázatot a különböző tudományágak eltérő értelmezéssel kezelik.[18] A szabályozás létrehozásakor ezeket közös nevezőre kell hozni.

## Az Európai Unióban kikristályosodó magas kockázat

Mi alapján kerülhet meghatározásra, hogy egy MI-alkalmazás magas kockázattal jár? Az európai jogalkotó egyrészről abból indul ki, hogy abban az esetben kerülhet megállapításra, amennyiben alapvető jogokat sérthet az alkalmazás. A Javaslat szabályai alapvetően ezen az elven alapulnak. Akár egy embernek is a méltóságát sértő, adatait jogosulatlanul felhasználó MI alkalmazás ezzel a kockázattal jár. Nem elhanyagolható körülmény továbbá, hogy könnyen rengeteg embert érinthet a mesterséges intelligencia kicsi meghibásodása. Az MI működése különösen nagy szakmai tudást igényel, a működése bizonyos esetekben átláthatatlan laikus, köznapi felhasználó számára.[19]

A hivatkozott állásfoglalásban az európai jogalkotó a magas kockázatú MI-rendszerekre vonatkozó objektív felelősség alkalmazását tartja megfelelőnek. „(1) Egy magas kockázatú MI-rendszer üzemeltetője objektív felelősséggel tartozik minden olyan sérelemért vagy kárért, amelyet a szóban forgó MI-rendszer által vezérelt fizikális vagy virtuális tevékenység, eszköz vagy folyamat okozott.”[20]

A kockázatközösségi konstrukció alkalmazása is tetten érhető az állásfoglalásban, amikor azt írja, hogy egy magas kockázatú MI-rendszer frontend-üzemeltetőjének gondoskodnia kell arról, hogy az MI-rendszer működésére rendelkezzen elegendő fedezetet biztosító felelősségbiztosítással.[21]

A mesterséges intelligencia felelősségi szabályozását illetően a vizsgált szakirodalmak többféle megoldást is elfogadhatnak találnak. Jelen tanulmány keretében nincs lehetőség ezek részletes elemzésére, itt sokkal inkább arra keresem a választ, hogy milyen elv vezérli az európai jogalkotót a szabályozás létrehozásakor.

## Precaution principle, vagyis az elővigyázatosság elve

A precaution principle egy kockázatértékelő szabályozási hozzáállás. Ez alapján a tiltás csak akkor indokolt, ha a tudományos szempontok szerint azonosított magas kockázat más szabályozási eszközzel megnyugtatóan (biztonságosan) nem küszöbölhető ki. Az elővigyázatosság elvének felhasználása tehát három előzetes feltétel együttes teljesülésekor indokolt: a) feltehetően káros hatások meghatározásra kerültek, a rendelkezésre álló

tudományos adatok értékelése megtörtént, a tudományos bizonytalanság mértéke meghatározható.[22] Az ilyen szabályozás megfelelő fékeket és garanciákat képes beépíteni a szabályozási rendszerbe.

Álláspontom szerint tehát az elővigyázatosság elve az a helyes irányvonal, amelyt egy ismeretlen technológia szabályozásánál figyelembe kell venni.

## A mesterséges intelligencia szabályozás rétegei

Mintegy alapvetésként megállapíthatjuk, hogy az Európai Unió mesterséges intelligencia szabályozása az eddig megvizsgált és rendelkezésre álló információk szerint több rétegből épül majd fel.

Egyrészről a már meglévő szabályokra kíván építeni, így a termékfelelősség[23] és egyéb felelősségi rendszerek területén megoldhatónak látja utaló szabályokkal behozni a meglévő megoldásokat az új technológiák, így az MI által teremtett helyzetekre.

Fontosak ugyanakkor az új, a kifejezetten a mesterséges intelligencia által generált helyzetekre hozott szabályok és megoldások. Ilyen például a mesterséges intelligencia jogszabály (Artificial Intellgience Act)

A jelen dolgozat a továbbiakban azzal a harmadik réteggel foglalkozik, amely a különböző technológiai felhasználások helyes, biztonsági garanciákat tartalmazó részletszabályait hivatott deklarálni. Ezek a szabványok és a tanúsítványok.

### Szabványok és tanúsítványok

A szabványok és a tanúsítványok, a tanúsítási rendszer alkalmas lehet mind azoknak a kockázatoknak a kezelésére, amelyeket a jogalkotónak sikerült már azonosítania. Ezt pedig sikerülhet oly módon kezelni, hogy ne kelljen mindeközben teljesen új joganyagot létrehozni.

A szabványok alkalmazása, a tanúsítványok megszerzése hordoz magában egy fajta önszabályozást a piaci szereplők részéről. Nem beszélve természetesen most arról, amikor a jogalkotó teszi kötelezővé egyes szabványok alkalmazását. Ahogyan arra Karácsony Gergely rámutat, itt egy verseny-oldali megközelítés is szerepet játszik, hiszen a piaci szereplők a vásárlók, a szolgáltatást igénybe vevők bizalmának elnyerése érdekében biztonságossá és a felhasználók számára elfogadhatóvá kívánják majd tenni a termékeiket és az

üzletpolitikájukat, termelési folyamatukat.[24]

Ezzel lehetővé válik a gyorsabb, és egyértelműbb implementálás, amely növeli a jogbiztonságot. A jogalkalmazók hamarabb kapnak választ a kérdéseikre, kalkulálni tudnak az MI-használattal járó költségekkel.

A szabványok és a tanúsítványok arról árulkodnak, hogy a mérnöki tudományos munkák ugyanúgy figyelembe veszik és tekintettel vannak a jogi munkákra, mint fordítva.

A tanúsítvány egy eljárás eredményeként létrejövő dokumentum, amely hitelt érdemlően igazolja, hogy valami megtörtént, vagy valami/valaki egyes jellemzőkkel rendelkezik.

## A szabványok

Tényként rögzíthetjük, hogy a szabványok használata által jelentős hatékonyságot tudnak a piaci szereplők elérni, így közvetve a gazdaság egyik fontos mozgatóelemét jelentik.[25] Általánosságban, Európai Uniós dimenzióban elmondhatjuk, hogy a szabványok és a szabványosítás az uniós egységes piac létrehozásának is egy fundamentuma. A nemzeti műszaki előírások helyébe lépő európai szabványok hozzájárulnak a technikai akadályok felszámolásához. A szabványok által lehetőség nyílik a piacra jutást könnyíteni a piaci szereplők számára, és nem csupán uniós, de nemzetközi együttműködést is elősegítenek. A szabványok elhozhatják a jobb kapcsolatokat a beszállítókkal és az ügyfelekkel, ami a fogyasztók biztonságának javulásából ered. Az Európai Unió meglátása szerint a szabványok lehetőséget tudnak biztosítani arra is, hogy az európai kkv szektort versenyképesebbé tegye.[26] A Bizottság rámutatott, hogy a szabványok csökkentik azt az időt, amely alatt az új technológia piacra tud kerülni, továbbá megkönnyítik az innovációt az által, hogy lehetővé teszik a vállalkozások számára, hogy a szabványban foglalt eredményekre támaszkodjanak és építsenek.

Érdemes megemlíteni azt, hogy a szabványok milyen hatással vannak a gazdasági versenyre, amely, mint ismeretes, az innovációnak és a fejlődésnek a motorja. A szabvány alkalmazása ugyanis, ha bizonyos vállalkozások számára nem lehetséges a szabványmegállapítási folyamatok eredményeinek megismerése, úgy versenyellenes eredményekhez vezet. A szabvány akkor nem korlátozza a versenyt, ha az bizonyos feltételekre épül. Így fontos, hogy a szabvány elfogadási eljárása átlátható, tisztességes, ésszerű és megkülönböztetésmentes legyen. Tehát mindenki egyenlő feltételekkel hozzájuthasson.[27]

A szabványok és a verseny kapcsolatát azért tartom fontosnak kiemelni, mert a verseny e

tekintetben a mesterséges intelligencia olyan irányú fejlesztéséhez vezet, amely maximálisan a fogyasztók érdekeit, biztonságát szolgálja.

A szabványokkal kapcsolatosan pár alapfogalmat tartok fontosnak tisztázni. E tanulmányban alapvetően a magyar szabványokkal kapcsolatos fogalmakat veszem alapul, és ehhez kapcsolódóan csatolok nemzetközi kitekintést. Mindenekelőtt a szabvány maga egy „elismert szervezet által alkotott vagy jóváhagyott, közmegegyezéssel elfogadott olyan műszaki (technikai) dokumentum, amely tevékenységre vagy azok eredményére vonatkozik, és olyan általános és ismételten alkalmazható szabályokat, útmutatókat vagy jellemzőket tartalmaz, amelyek alkalmazásával a rendező hatás az adott feltételek között a legkedvezőbb.”[28]

Szabványosítás alatt olyan tevékenységet értünk, „amely általános és ismételten alkalmazható megoldásokat ad fennálló vagy várható problémákra azzal a céllal, hogy a rendező hatás az adott feltételek között a legkedvezőbb legyen.”[29]

A szabványügyi szerv „olyan szabványosító szerv, amelyet nemzeti, regionális vagy nemzetközi szinten elismertek, és amelynek fő funkciója – alapszabályzatából adódóan – a közösség számára hozzáférhető szabványok kidolgozása és jóváhagyása vagy elfogadása.”[30]

Európai szabványügyi szervezetek az Európai Szabványügyi Bizottság (CEN), az Európai Elektrotechnikai Szabványügyi Bizottság (CENELEC), az Európai Távközlési Szabványügyi Intézet (ETSI).

Az egyik legismertebb nemzetközi szabványosító szervezet a Nemzetközi Szabványügyi Szervezet, az ISO. Ennek a szervezetnek már vannak is eredményei a mesterséges intelligenciát támogató szabványok létrehozása terén. Ilyen például az ISO/IEC NP 24029-1[31], Neurális hálózatok robusztusságának felmérése témakörben. Szintén a mesterséges intelligenciához és a kockázatelemzéshez kapcsolódóan az ISO 12100:2010[32], amely a kockázatértékelés és kockázatcsökkentés általános elveit érinti. A jelen tanulmány megírásakor pedig még fejlesztés alatt áll az etikai és szociális áttekintést tartalmazó ISO/IEC DTR 24368 szabvány.

A megfelelő mesterséges intelligenciára vonatkozó szabványok megalkotásával elérhetővé válik tehát egy megbízható, korszerű technológia dokumentálása, amely azután alapja lehet további fejlesztésnek és moderniálásnak. Lévén, hogy ez egy műszaki tartalommal is rendelkező dokumentum lehet, alkalmas lehet a mesterséges intelligencia rendszerek helyes leírására. A szabványosításban alkalmazott elvek, mint az áttekinthetőség és nyilvánosság, a közérdek képviselete, egységesség és ellentmondás-mentesség pedig álláspontom szerint

hozzájárulnak az MI jelente kockázatok porlasztásához és a jogbiztonsághoz.

Felmerül a kérdés a mesterséges intelligencia szabályainak a jogforrási hierarchiában történő elhelyezése kapcsán, hogy arra milyen szinten kerüljön sor. Tekintettel arra, hogy ez egy határokon átívelő technológia, mindenképpen egy magasabb szintű szabályozási dimenziót érdemes találni. Kérdés az is, hogy megfelelő lépés volna-e a szabványok egyes részeinek beépítése jogszabályi környezetbe?

A Magyar Szabványügyi Testület e körben az alábbi álláspontra helyezkedik.

A technológiai részletszabályok jogszabályba foglalása nem ösztönzi a piaci szereplőket, hogy jobb megoldást fejlesszenek, ha egy adott szabvány alkalmazása kötelező és a jobb technológia alkalmazása nem jár plusz jutalmazással Míg, ha a fejlettebb szabvány alkalmazásásával több ügyfelet tud magához csábítani, akkor az mindenképpen pozitív hatással lesz rá. A jogszabályba foglalás a jogalkotóra hárítja a felelősséget, hiszen a piaci szereplő okkal bízhatott benne, hogy a jogszabályban elvárt szabvány alkalmazása megfelelő biztonságot nyújt. Az is igaz, hogy a nem kellően előrelátó és rugalmas jogszabály konzervál egy már meghaladott technikai megoldást, amely így visszatartja a fejlődést.

A nemzeti jogszabályokba ültetett szabványok tekintetében probléma lehetne, hogy zavart kelt a jogkövetében, mivel a jogszabályok szintjei között ellentmondás mutatkozhat. Például, ha egy európai szabvány alkalmazása szükséges, ugyanakkor az ellentétes a nemzeti jogszabály rendelkezésével.[33]

## A tanúsítványok és a tanúsítási folyamat

A tanúsítványok és a tanúsítási folyamat egy szintén gyakorlatorientált, problémaközpontú rétege lehet a mesterséges intelligencia szabályozásnak. A tanúsítási folyamat a mesterséges intelligencia körében Philip Matthias Winter és társai elképzelése szerint[34] a következőképpen épül fel. Egy GAP analízis jelenti a kezdő lépést. A GAP analízis, magyarul rés- vagy eltéréselemzés lehetővé teszi a szervezt céljai és a tényleges eredménye közötti inkonzisztenciák felmérését.[35] Ennek érdekében jellemzően a fejlesztők feladata az eltéréselemzés és a követelménykatalógus előkészítése. A GAP analízis segítségével áttekinthető, hogy az alkalmazás tervezése és fejlesztése során figyelembe vettek e minden szükséges biztonsági és védelmi követelményt. A következő lépésben egy ún. kick-off meeting keretében az auditorok és a fejlesztők találkoznak, és meghatározásra kerül a tanúsítvány által lefedett kör. A dokumentációk áttekintését követően megkezdődik az audit eljárás, benne az interjúkkal. Ezt követően egy technikai vizsgálat, melyet követően kiadásra

került az audit jelentés. A jelentést követően a tanúsítvány kiállítására kerül sor. Annak érdekében pedig, hogy a tanúsítvány később is megfelelő igazolását adja az adott alkalmazás megfelelő működésének meghatározott időközönként monitoring auditokra kerül sor, amelyek végén újra-tanúsított igazolások kerülnek kiadásra.[36]

A tanúsítási folyamat pozitívumai, hogy hozzásegítik a jogalkotót a kockázatok enyhítéséhez a normák és szabványok létrehozásával. A tanúsítványok termékfejlesztési ösztönzésként is hathatnak, mivel az előírásoknak megfelelés ösztönzi a fejlesztést olyan irányban is, amelyre nem lépett volna. A bizalmat független szakemberek építik tanúsítási eljárás útján, alkalmazott kritériumok, és iránymutatások alapján.[37]

## Összegzés, a tanúsítási folyamat értékelése

Léteznek azonban kihívások a gépi tanuláson alapuló applikációk tanúsítási folyamata körében. Egyrészről fontos ugyanis tisztában lenni gépi tanulás kulcsfogalmaival, a matematikai alapvetésekkel és előfeltételekkel. Philip Matthias Winter és szerzőtársai e körben kiemelik, hogy habár a gépi tanuláson alapuló alkalmazásokon magasan képzett fejlesztők dolgoznak, a terméktanúsítványi folyamatban sokkal szélesebb csoportot kívánunk megszólítani, így az ez irányú képzés esszenciális jelentőségű.

Mindemellett rugalmas tanúsítási folyamatra van szükség, ahol az időközben elért eredményeket be lehet építeni a folyamatba. Vannak ugyanis jelenleg is aktív kutatási területek, mint például a bizonytalanságbecslés, az értelmezhetőségi módszerek, az anomáliák felderítése, az ellenséges támadások/védelem, valamint az emberekkel vagy környezettel való interakció. Az ezeken a területeken is elért eredményeket az újabb tanúsítási folyamatokba szükséges beépíteni.

Fontos szem előtt tartanunk ugyanakkor az elérni kívánt célt, hiszen az optimalizálási célhoz nem tökéletesen illeszkedő garanciák érvényesítése mindig csökkenti a teljesítményt a valódi mögöttes célhoz képest. A túlzott garanciák beépítése tehát a szabályokba azzal a veszéllyel is járhat, hogy a technológia nyújtotta előnyök tompulnak vagy elvesznek.

Szintén egy a tanúsítással kapcsolatos még megoldatlan probléma, hogy hogyan kezeljük az úgy nevezett disztribúciós eltolódásokat. Vagyis azokat az eseteket, amikor a tanulási adatok eltérőek a valós világban kapott adatoktól. Egy jó példa ezekre az USA-ban kifejlesztett automatizált vezetés, amely ugyanakkor sajnos már nem biztos, hogy egy mohácsi közlekedési helyzetben is helyes megoldást hoz.[38]

Azt szeretnénk, hogy az MI bizonyos erkölcsi minimumokhoz, mércékhez mindenképpen tartsa magát.

## Konklúzió

A fentiekben foglaltakat összevetve az az álláspont látszik kibontakozni, hogy a tanúsítványok és a szabványok alkalmazása a mesterséges intelligencia felhasználásával járó kockázatok porlasztása alkalmas. További követelmények, feltételek szükségesek, hogy megállapításra kerüljenek a szabványok és a tanúsítási folyamat kapcsán, ám ezek már olyan jellegű részletszabályok, amelyek kifejezett műszaki szakismeretet is igényelnek.

Ami minden bizonnyal elhagyhatatlannak mutatkozik az a magas szintű technológiai szakmai ismerettel rendelkező személyi állomány képzése, akik képesek lesznek jól kommunikálni a fejlesztők és a jogalkotó között.

Ahogyan fent szerepelt, fontos, hogy a szabvány elfogadási eljárása átlátható, tisztességes, ésszerű és megkülönböztetésmentes legyen. A kockázatokat csökkenteni szándékozó célkitűzés nem vezethet a más terület, így például a verseny torzításához. Nem okozhatja az alapvető európai értékek devalválódását, így lehetővé kell tenni, hogy azokat minden európai vállalkozás a piacra lépéshez segítségül hívhassa.

Az audit katalógus, mint a rugalmasság garanciája vélhetően nagy szerepet fog játszani a mesterséges intelligencia szabályozás során. Mivel ez a dokumentum a piaci igényeknek és jogszabályi környezetnek megfelelendő folyamatosan és könnyebben tud változni. A szakemberek könnyebben tudnak hozzá nyúlni és ezzel lehetővé tenni a folyamatos, fenntartható garanciákkal megtámogatott fejlődést.

## Bibliográfia

Fehér könyv a mesterséges intelligenciáról: a kiválóság és a bizalom európai megközelítése, 2020, COM(2020) 65 final, https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_hu.pdf

Fleischer Tamás: Innováció, növekedés, kockázat, in Bulla Miklós – Tamás Pál (szerk.): *Fenntartható fejlődés Magyarországon: Jövőképek és forgatókönyvek. Stratégiai kutatások – Magyarország 2015*. Budapest, Új Mandátum Könyvkiadó, 2006.

G. Karácsony Gergely: *Okoseszközök – Okos jog?, A mesterséges intelligencia szabályozási kérdései*. Budapest, Dialóg Campus, 2020.

Kenderfi István – Fűrész Miklós: Szemléletváltás a szakképzésben: a lemorzsolódás megelőzésének pályaorientáció központú megközelítése, *Új Munkaügyi Szemle*, II. évf. 2021/4.

Klein Tamás – Tóth András: *Technológia jog – Robotjog – Cyberjog*. Budapest, Wolters Kluwer, 2019.

Netjasov, Fedja – Janic, Milan.: A review of research on risk and safety modelling in civil aviation, *Journal of Air Transport Management*, Volume 14, Issue 4, July 2008

The relentless growth of cybercrime, Europol's 2016 Internet Organised Crime Threat Assessment (IOCTA)
https://www.europol.europa.eu/newsroom/news/relentless-growth-of-cybercrime

Tóth András: A mesterséges intelligencia szabályozásának paradoxonja és egyes jogi vonatkozásainak alapvető kérdései, *Infokkumunikáció és jog*, 2019/2.

Széll Sámuel: Szabvány–dokumentáció, *Tudományos és Műszaki Tájékoztatás*, 5. évf., 1958/1.

Udvary Sándor: Az önvezető gépjárművek egyes felelősségi kérdései, *Pro Publico Bono – Magyar Közigazgatás*, 2019/2.

Veres Zoltán: A gap-modell formaváltozásai? *Marketing & Menedzsment*, 51. évf., 2017/1-2.

Winter, Philip Matthias (et al.): *Trusted Artificial Intelligence: Towards Certification of Machine Learning Applications*. arXiv preprint arXiv:2103.16910, 2021.

## Hivatkozások

1. Udvary Sándor: Az önvezető gépjárművek egyes felelősségi kérdései, *Pro Publico Bono – Magyar Közigazgatás*, 2019/2, 146–155. ↑
2. COM(2018) 795 final ↑
3. Tóth András: A mesterséges intelligencia szabályozásának paradoxonja és egyes jogi vonatkozásainak alapvető kérdései, *Infokkumunikáció és jog*, 2019/2, 3–9. ↑

4. Fehér könyv a mesterséges intelligenciáról: a kiválóság és a bizalom európai megközelítése, 2020, COM(2020) 65 final, https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_hu.pdf ↑
5. Az Európai Parlament 2017. február 16-i állásfoglalása a Bizottságnak szóló ajánlásokkal a robotikára vonatkozó polgári jogi szabályokról (2015/2103(INL)) (2018/C 252/25), https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52017IP0051 ↑
6. The relentless growth of cybercrime, Europol's 2016 Internet Organised Crime Threat Assessment (IOCTA) https://www.europol.europa.eu/newsroom/news/relentless-growth-of-cybercrime ↑
7. Ezzel kapcsolatos aggályokat a „Az Európai Parlament 2020. október 20-i állásfoglalása a digitális szolgáltatásokról és az alapvető jogokról szóló törvényről" is rögzít. (pl. női diszkrimináció, az automatizált algoritmusok tartalomszűrése jogállamisággal kapcsolatos aggályokat vet fel) ↑
8. Fehér könyv ↑
9. COM(2018) 795 final ↑
10. Széll Sámuel: Szabvány–dokumentáció, *Tudományos és Műszaki Tájékoztatás*, 5. évf., 1958/1, 25–34. ↑
11. Az Európai Parlament 2020. október 20-i állásfoglalása a Bizottságnak szóló ajánlásokkal a mesterséges intelligenciára vonatkozó polgári jogi felelősségi rendszerrel kapcsolatban (2020/2014(INL)) ↑
12. Az állásfoglalás melléklete részletes már-már szövegszerű javaslatokat tartalmaz, egy megalkotandó rendelet hatályáról, fogalommeghatározásáról, a magas kockázatú MI-rendszerekre vonatkozó objektív felelősségről. ↑
13. Ez alapján: *„magas kockázat: az egy vagy több személy számára véletlenszerű módon történő, az észszerűen előrelátható mértéket meghaladó sérelem- vagy károkozás jelentős kockázata egy autonóm módon üzemelő MI-rendszer esetében; a kockázat jelentősége a lehetségesen okozott sérelem vagy kár súlyossága, a döntéshozatal önállóságának mértéke, a kockázat felmerülésének valószínűsége és az MI-rendszer használatának módja és körülményei közötti kölcsönhatástól függ;"* ↑
14. Document 52021PC0206 ↑
15. https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX:52021PC0206 ↑
16. Fleischer Tamás: Innováció, növekedés, kockázat, in Bulla Miklós – Tamás Pál (szerk.): *Fenntartható fejlődés Magyarországon: Jövőképek és forgatókönyvek. Stratégiai kutatások – Magyarország 2015*. Budapest, Új Mandátum Könyvkiadó, 2006, 275–284. ↑
17. G. Karácsony Gergely: *Okoseszközök – Okos jog?, A mesterséges intelligencia szabályozási kérdései*. Budapest, Dialóg Campus, 2020, 142–144. ↑

18. Fedja Netjasov – Milan Janic: A review of research on risk and safety modelling in civil aviation, *Journal of Air Transport Management*, Volume 14, Issue 4, July 2008, Pages 213–220. ↑
19. Az Európai Parlament 2020. október 20-i állásfoglalása (2020/2014(INL)) ↑
20. Uo. ↑
21. Uo. ↑
22. Elérhető: https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=legissum%3Al32042 ↑
23. *„8. úgy véli, hogy a termékfelelősségről szóló irányelv 30 éve hatékony eszköznek bizonyul a hibás termékek okozta károkért járó kártérítések kifizettetésére, azonban felül kell vizsgálni a digitális világhoz való hozzáigazítása és a kialakulóban lévő digitális technológiák által jelentett kihívások kezelése érdekében, ezáltal biztosítva a fogyasztók hatékony védelmének magas szintjét, valamint a jogbiztonságot a fogyasztók és a vállalkozások számára, elkerülve ugyanakkor a magas költségeket és kockázatokat a kkv-k és induló vállalkozások számára;”* Forrás: Az Európai Parlament 2020. október 20-i állásfoglalása (2020/2014(INL)) ↑
24. G. Karácsony: *Okoseszközök – Okos jog?* 142–144. ↑
25. Klein Tamás – Tóth András: *Technológia jog – Robotjog – Cyberjog*. Budapest, Wolters Kluwer, 2019, 70. ↑
26. Elérhető: Benefits of standards, https://ec.europa.eu/growth/single-market/european-standards/standardisation-policy/benefits-standards_en ↑
27. Klein – Tóth: *Technológia jog – Robotjog – Cyberjog*, 71–74. ↑
28. a nemzeti szabványosításról szóló 1995. évi XXVIII. törvény 4. § (1) bek. ↑
29. 1. számú melléklet az 1995. évi XXVIII. törvényhez 1. pont ↑
30. 1. számú melléklet az 1995. évi XXVIII. törvényhez 2. pont ↑
31. ISO/IEC NP 24029-1 and 24029-2 – AI – Assessment of the robustness of neural networks. ↑
32. Safety of machinery — General principles for design — Risk assessment and risk reduction. ↑
33. Forrás: http://www.mszt.hu/web/guest/tevhitek-es-tenyek ↑
34. Philip Matthias Winter (et al.): *Trusted Artificial Intelligence: Towards Certification of Machine Learning Applications*. arXiv preprint arXiv:2103.16910, 2021. ↑
35. Kenderfi István – Fűrész Miklós: Szemléletváltás a szakképzésben: a lemorzsolódás megelőzésének pályaorientáció központú megközelítése, *Új Munkaügyi Szemle*, II. évf. 2021/4, 18., valamint Veres Zoltán: A gap-modell formaváltozásai? *Marketing & Menedzsment*, 51. évf., 2017/1-2, 87-98. ↑
36. Winter: *Trusted Artificial Intelligence* ↑
37. Uo. ↑
38. Uo. 22. ↑