DOI: 10.31915/NWS.2025.3

HOGYAN CSÖKKENTHETJÜK AZ INFORMATIKUSOK ÉS A JOGÁSZOK KÖZÖTTI KOMMUNIKÁCIÓS PROBLÉMÁKAT AZ MI ALKALMAZÁSA SORÁN AZ OKTATÁSI SZEKTORBAN?

Albert Ágota
dralbertagota@gdprszakszeruen.hu
Karinthy Frigyes Gimnázium

„A fekete lyukak ott keletkeznek, ahol az informatikusok és a jogászok beszélgetni kezdenek”
(*meg nem nevezett jogász*)

Absztrakt

A mesterséges intelligencia (MI) fejlődése új típusú együttműködést követel meg az informatikusok és a jogászok között – különösen az oktatás területén. A technológiai és jogi megközelítések azonban gyakran ütköznek, ami veszélyeztetheti a projektek jogszerűségét, etikai megfelelését és társadalmi elfogadottságát.

A tanulmány azt vizsgálja, hogyan segíthetik elő a már rendelkezésre álló eszközök – például az adatvédelmi és alapvetőjogi hatásvizsgálatok, a kiberbiztonsági felkészülés, a belső szabályozás és a célzott oktatás – a két szakma közötti hatékonyabb együttműködést. A cél olyan MI-megoldások megvalósítása, amelyek nemcsak technikailag, hanem jogilag és emberileg is helytállnak.

Kulcsszavak: mesterséges intelligencia, informatikusok és jogászok, oktatási szektor, adatvédelem, GDPR, MI jogszabály (AI Act), adatvédelmi hatásvizsgálat, alapvetőjogi hatásvizsgálat, kiberbiztonság, megfelelőség

Abstract

How Can We Reduce Communication Problems Between IT Professionals and Lawyers in the Application of AI in the Education Sector?

“Black holes emerge where computer scientists and lawyers start talking to each other.”
(*Unnamed lawyer*)

The development of artificial intelligence (AI) demands a new kind of collaboration between IT professionals and legal experts—especially in the field of education. However, technological and legal perspectives often come into conflict, jeopardizing the legal soundness, ethical integrity, and public acceptance of AI projects.

This paper explores how existing tools—such as data protection and fundamental rights impact assessments, cybersecurity preparedness, internal policies, and targeted training—can support more effective cooperation between the two professions. The ultimate goal is to develop AI solutions that are not only technically sound, but also legally and ethically robust.

Keywords: artificial intelligence, IT professionals and lawyers, education sector, data protection, GDPR, AI Act, data protection impact assessment, fundamental rights impact assessment, cybersecurity, compliance

Mit okozhat a kommunikációs szakadék?

Egyre több oktatási, könyvtári vagy muzeális projektben jelenik meg az MI, legyen az vizsgáztatórendszer, tanulási útvonal-ajánló, vagy automatizált tartalomkereső. Azonban ezek a rendszerek nem technológiai buborékban léteznek, ugyanúgy vonatkoznak rájuk az adatvédelemmel, vagy éppen az alapvető jogokkal kapcsolatos jogszabályok, mint bármely más hagyományos IT projektre. Az MI projektek új kihívásokat támasztanak és a megvalósítás során gyakran tapasztalható információs szakadék az informatikusok és jogászok között, ez pedig eredményezheti a projekt kudarcát, jelentős pénzügyi veszteséget vagy akár komoly reputációs kárt is.

Számos olyan esetet ismerünk, amikor egy már működő MI-rendszer nem felelt meg a követelményeknek és az illetékes adatvédelmi hatóság szankcionálta is azt. Egy olasz egyetem[1] például MI-alapú vizsgarendszert vezetett be, amely jelentősen sértette az adatvédelmi szabályokat, de az a múzeumi projekt[2] sem bizonyult sikeresnek, amelyben biometrikus adatok[3] gyűjtésével figyelték meg a látogatók reakcióit, azaz azt, hogy mit éreztek-gondoltak egy adott műalkotással kapcsolatban. A közös a két projektben, hogy

1 Ordinanza ingiunzione nei confronti di Università Commerciale "Luigi Bocconi" di Milano – 16 settembre 2021 [9703988]. Garante per la protezione dei dati personali

2 Provvedimento del 13 aprile 2023 [9896808]. Garante per la protezione dei dati personali

3 „biometrikus adat": egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat [GDPR 4. cikk 14. pont]

- nem végeztek megfelelő, a GDPR 35. cikke szerinti adatvédelmi hatásvizsgálatot[4],
- a diákok/múzeum látogatók nem kaptak megfelelő tájékoztatást az adataik kezelése tekintetében,
- szükségtelen, illetve aránytalan adatgyűjtés történt, köztük a személyes adatok különleges kategóriájába tartozó (biometrikus) adatok gyűjtése.

Mindkét eset megelőzhető lett volna, ha a projektben résztvevő szakterületek képviselői – ideértve különösen az informatikusokat és a jogászokat – adatvédelmi hatásvizsgálat keretében átgondolják, milyen adatokat szeretnének gyűjteni és felhasználni, és ehhez milyen jogi kereteket kell szükségszerűen figyelembe venni.

Miért olyan gyakori ez a kommunikációs probléma? Képzeljük el azt a helyzetet, ahogy egy informatikus és egy jogász beszélget.

> *Az informatikus panaszkodik a jogásznak: „Nagyon nehéz informatikusként dolgozni, állandó a nyomás, minden működjön tökéletesen, és még a felhasználók is elégedettek legyenek."*
>
> *Mire a jogász: „Jogászként én is hasonló cipőben járok, meg kell felelnem a jogszabályoknak és a kockázatokat is minimalizálnom kell."*
>
> *Mire az informatikus: „Talán össze kellene fognunk és megalkotnunk egy „Code of Law"-t, hogy könnyebben tudjunk együtt dolgozni."*
>
> *Mire a jogász: „Akkor először határozzuk meg, hogy a „Code" szó melyik jogi kategóriába tartozik."*

Ez a létező sztereotípiákon alapuló párbeszéd rávilágít arra az alapproblémára, amely az eltérő definíció-használatból ered. Olyan kérdések okozhatnak félreértést, mint például:

- Mi az az elektronikus információs rendszer? [A jogász szerint az, amit a jogszabály annak minősít.]
- Mi az a „nagy mennyiségű" adat? [A jogász szerint ez jogszabályban meghatározott kockázati szint.]
- Mit jelent az összeférhetetlenség jogi és kiberbiztonsági szempontból?
- Ki dönti el, hogy mi az MI? [A jogász szerint az MI az, amit a jogszabály annak minősít[5] függetlenül attól, mi a véleménye az adott rendszerről egy IT szakembernek.]

---

4 data protect impact assessment; DPIA

5 AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2024. június 13-i (EU) 2024/1689 RENDELETE a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról, valamint a 300/2008/EK, a 167/2013/EU, a 168/2013/EU, az (EU) 2018/858, az (EU) 2018/1139 és az (EU) 2019/2144 rendelet, továbbá a 2014/90/EU, az (EU) 2016/797 és az (EU) 2020/1828 irányelv módosításáról (a mesterséges intelligenciáról szóló rendelet, továbbiakban AI Act).

Az eltérő szaknyelvek használata óhatatlanul kommunikációs problémákhoz vezet, az MI-projektekben pedig alapvető cél az ebből adódó kockázatok minimalizálása.

Hogyan építhető híd a kommunikációs szakadék felett?

A problémát egy svéd gyermekvers[6] fogalmazza meg:

A felnőttek
furcsák néha.

Azt hiszik, elég összeterelni
két „alkalmas korú" gyereket,
és a két gyerek
automatikusan jó haver lesz.

Szeretném összeterelni
papát találomra egy „alkalmas korú" bácsival
és megnézni, összehaverkodnak-e (...)

Az MI-projektek sikerességének követelménye a nyitottság és a tolerancia, és a közös cél érdekében le kell számolni az olyan sztereotípiákkal, mint például az informatikusok „kockák", a jogászok meg „karót nyeltek", a közös pedig az bennük, hogy „földi halandó nem érti meg, hogy miről beszélnek". Az esetek többségében a projekt résztvevői nem választhatják meg, hogy kivel kell együtt dolgozniuk, éppen ezért időt és esélyt kell adniuk arra, hogy megismerkedjenek egymással.

Mely területeken fontos az informatikusok és a jogászok együttműködése?

Az MI-projektekben számos olyan részterület van, ahol elengedhetetlen az informatikusok és a jogászok közös munkája, például a megmagyarázhatóság, az átláthatóság, valamint a hibák azonosítása.

A **megmagyarázhatóság esetében** az informatikus a technikai részletekre helyezi a hangsúlyt és algoritmusokban és adatokban gondolkodik, míg a jogásznak az a feladata, hogy érthetően megmagyarázza az érintetteknek, hogyan is működik a rendszer, például milyen logika mentén jut arra a döntésre, amire jut, és ez a döntés hogyan érinti az érintettek jogait és szabadságait.

Az **átláthatóság** esetében az informatikusnak meg kell oldania, hogy a felhasználó számára kiderüljön, MI-vel került kapcsolatba (például egy chatbot esetében), illetve a jogász feladata az, hogy a felhasználóknak részletes tájékoztatást biztosítson, mi is történik az adataikkal és a rendszer működése milyen következményekkel jár az ő szempontjukból.

6 Ingrid Sjöstrand: A felnőttek furcsák néha, részlet

A **hibák detektálása és kiküszöbölése** esetében előfordulhat, hogy míg az informatikus szerint egy adott hiba nem hiba, hiszen a rendszer tökéletesen működik, a jogász szerint a rendszer működése aggályos, mivel diszkrimináció történhet. A hibák (torzítások) világa olyan terület, amelyen az informatikai és jogi szakembereknek mindenképpen együtt kell működniük.

Milyen lehetőségek vannak az együttműködésre?

Számtalan olyan eszköz áll már ma is rendelkezésre, amely rákényszeríti a projekt résztvevőit az ismerkedésre, a definíciók tisztázására, valamint a közös nyelv kialakítására. Ilyen például a kockázatmenedzsment keretében a kockázatértékelés és kockázatkezelés, az adatvédelmi hatásvizsgálat, az alapvetőjogi hatásvizsgálat[7], az érdekmérlegelési tesztek készítése[8], a kiberbiztonsági audit[9], valamint belső szabályzatok és eljárásrendek alkotása (folyamatok leírása, kritikus pontok meghatározása stb.), az oktatás (workshop, közös esetmegoldások, tanulságok keresése stb.) és a támogató keretrendszerek, pl. MI-fejlesztési etikai kódexek, compliance struktúrák.

A közös nyelv kialakítása az alapvetőjogi-, illetve adatvédelmi hatásvizsgálat során

Az MI-projektek esetében a hatásvizsgálatokat célszerű úgy kezelni, mint hidakat, amelyek az álláspontok okozta szakadék felett ívelhetnek át.

Az alapvetőjogi hatásvizsgálat[10] olyan hatásvizsgálati keretrendszer, amely segít felismerni azokat a kontextusokat és alkalmazásokat, ahol egy MI-rendszer súlyos kockázatot jelenthet az emberi jogokra, a demokratikus működésre vagy a jogállamiságra. Például, ha egy intézmény MI-megoldást vezet be az oktatásban, a kérdés nem csak az, hogy működik-e a rendszer, hanem az is, hogy az érinti-e az egyenlő hozzáférést, hozhat-e hátrányba bizonyos csoportokat, illetve átlátható-e a rendszer működése. A hatásvizsgálat a folyamatos párbeszédet biztosítva vezeti végig a projekt résztvevőit az érintettek azonosításán, a kockázatok feltárásán, valamint ezen kockázatokat mérséklő intézkedések kidolgozásán úgy, hogy a dokumentálás is átlátható legyen (1. táblázat).

7 AI Act 27. cikk

8 GDPR 5. és 6. cikk

9 2024. évi LXIX. tv. Magyarország kiberbiztonságáról

10 például a HUDERIA (Human Rights, Democracy and the Rule of Law Impact Assessment for AI Systems), mely az Európa Tanács és az Alan Turing Intézet közös projektje [CAI(2024)16rev2]

Lépések	Kérdés	Szükséges tudás
1. Érintettek felmérése	Kit érint az MI?	IT + helyismeret
2. Érintett jogok felmérése	Milyen alapjogokat érint a rendszer?	Jogászi értelmezés
3. Kockázatok felmérése, elemzése	Mit okozhat az MI?	Közös elemzés
4. Kockázatok enyhítése	Mit tegyünk a kockázatok csökkentése érdekében?	Közös stratégia
5. Dokumentálás	Ki és hogyan viszi tovább a projektet?	Intézményi gyakorlat

1. táblázat: Alapvetőjogi hatásvizsgálat főbb lépései

Kockázatok biometrikus adatok kezelése esetében

Számtalan MI-rendszer kezel biometrikus adatokat, többek között ujjlenyomat[11], illetve arcfelismerésre épülő rendszer[12] keretében. Az adatvédelmi hatóságok szankcionálási gyakorlata rámutat arra, hogy az MI-projektek esetében számtalan kockázatot kell kezelni, különös tekintettel a diákok, valamint a tanárok és egyéb munkavállalók jogait és szabadságait érintő kockázatokra (2. táblázat).

Kockázati tényező	Diákokra vonatkozó kockázat	Tanárokra / munkavállalókra vonatkozó kockázat
Jogellenes adatkezelés	Gyermekek adatainak kezelése különösen érzékeny.	Biometrikus adatok csak szigorúan indokolt esetben kezelhetők.
Hozzájárulás érvényessége	Szülői hozzájárulás gyakran formális, nem önkéntes vagy nem történt előzetes tájékoztatás.	Munkaviszonyban nehéz valódi önkéntességet biztosítani – a hozzájárulás gyakran kikényszerített .
Átláthatóság hiánya	A diákok/szülők nem kapnak érthető, részletes tájékoztatást az adatkezelésről.	A munkavállalók nem tudják pontosan, ki, mikor, mire használja a biometrikus adataikat.

11 Procedimiento Nº: PS/00131/2020. Agencia Española de Protección de Datos

12 PS 49/2019. Autoritat Catalana de Protecció de Dades

Kockázati tényező	Diákokra vonatkozó kockázat	Tanárokra / munkavállalókra vonatkozó kockázat
Adatbiztonsági kockázat	Arcfelismeréssel vagy ujjlenyomattal kapcsolatos adatok kiszivárgása súlyos, visszafordíthatatlan kockázat.	A biometrikus adatok nem cserélhetők – ellopásuk esetén a munkavállaló végleg elveszíti a rendelkezését az adatai felett.
Hatásvizsgálat (DPIA) hiánya	Nincs előzetes elemzés a gyerekekre gyakorolt hatásokról, ezért a jogsértés kockázata nő.	Nem történik mérlegelés arról, hogy az adatkezelés szükséges-e és arányban van-e az elérni kívánt célokkal.
Külső szolgáltatóval való megállapodás hiánya	Ha a rendszert „külsős" üzemelteti és nincs szerződés, az intézmény a felelős.	A munkáltató teljes felelősséget visel a rendszerhibákért és jogsértésekért, ha nincs írásos megállapodás.

2. táblázat: Az MI-projektekben a diákok és a tanárok/munkavállalók tekintetében felmerülő főbb kockázatok

A biometrikus adatokat kezelő MI-rendszerek esetében is jól körülhatárolhatóak a feladatkörök és felelősségek (3. táblázat).

Kockázati tényező	Jogász(ok) feladata „Mit kell biztosítani?"	IT szakemberek feladata „Hogyan valósítjuk meg?"
Jogellenes adatkezelés	Meghatározni, van-e jogalap és kivétel (pl. jogszabály, szerződés, jogos érdek stb.), és ez alkalmazható-e biometrikus adatra is.	Csak akkor építeni vagy üzemeltetni rendszert, ha van jogi felhatalmazás és az adatkezelés célhoz kötött.
Hozzájárulás érvényessége	Biztosítani, hogy a hozzájárulás önkéntes, tájékoztatáson alapuló és bármikor visszavonható legyen.	Olyan rendszer kialakítása, ahol a hozzájárulás hiánya esetén is van alternatív azonosítási lehetőség.
Átláthatóság hiánya	Közérthető tájékoztatót készíteni: mi történik az adatokkal, meddig, miért.	Interfészek, adatfolyamok, rendszerleírások dokumentálása → ellenőrizhető és transzparens legyen az adatkezelés.
Adatbiztonsági kockázat	Elvárni a minimális biztonsági szinteket (pl. titkosítás, jogosultságkezelés, naplózás).	Implementálni a biztonsági funkciókat: titkosítás, naplózás, zárolás, törlés, rendszer-hozzáférések.

Kockázati tényező	Jogász(ok) feladata „Mit kell biztosítani?”	IT szakemberek feladata „Hogyan valósítjuk meg?”
Adatvédelmi hatásvizsgálat hiánya	Koordinálni és dokumentálni az adatvédelmi- és alapvetőjogi hatásvizsgálatot, ahol ez kötelező.	Technikai kockázatelemzésben közreműködni: adatfolyamok, sérülékenységek, rendszerek bemeneti pontjai.
Külső szolgáltatóval való megállapodás hiánya	Adatfeldolgozói megállapodás készítése és ellenőrzése [GDPR 28. cikk].	Ellenőrizni: ki, mikor, mihez fér hozzá. Tesztelni a szolgáltató rendszerét. Kizárólag a szerződésnek megfelelően üzemeltetni.

3. táblázat: A jogászok és az IT-szakemberek feladatai az MI használatából adódó főbb kockázatok kezelése során

A kockázatok feltárása a nagy nyelvi modellekben

Az Európai Adatvédelmi Testület (EDPB) kiadványa[13] alapvető útmutatóként szolgálhat a nagy nyelvi modellekkel kapcsolatos adatvédelmi kockázatok felméréséhez az oktatással kapcsolatos MI-projektek esetében is (4. táblázat).

Problémák	Mit jelent az oktatásban?
Átláthatatlanság	Nem tudjuk, mit tanácsol a modell pontosan a hallgatónak
Adatszivárgás	Visszakövethető lehet az intézmény vagy a felhasználó
Tévedés, torzítás	Jogtalan elutasítás vagy hibás ajánlás
Nincs pontos adatkezelő	Ki a felelős a hallgató panaszáért, kihez fordulhat?

4. táblázat: Az alapvetőjogi hatásvizsgálat főbb lépései

A projektek résztvevőinek át kell gondolniuk az adatvédelmi kockázatokat is (5. táblázat).

13 Isabel Barberá: AI Privacy Risks & Mitigations - Large Language Models (LLMs) EDPB 2025

Kockázat típusa	Az informatikus szerepe	A jogász szerepe
Torzítás, adatminőség, hallucináció	Adatforrások kiválasztása, annotálás.	Diszkrimináció elkerülése, jogszerűség (téves információk, téves döntések stb.).
Black box működés	Technikai dokumentáció, naplózás.	Átláthatóság, érintetti jogok biztosítása.
Pre-trained modellek	Validálás, statisztikai követés.	Tudományos érvényesség, felelősség.
Adat-aggregáció	Struktúra és hozzáférés kialakítása.	Adatvédelmi hatásvizsgálat.
Reprodukálhatóság	Tesztelési lehetőség megteremtése.	Jogosultság, elszámoltathatóság.
Profilozás	Implicit módon személyes adatok feldolgozása és abból következtetések levonása.	Rejtett adatkezelés, érintetti jogok sérelme, illetve érvényesíthetetlensége.

5. táblázat: Az informatikusok és a jogászok szerepe az MI-projektek főbb adatvédelmi kockázatainak kezelésében

A kiberbiztonsági audit

A kockázatmenedzsment keretrendszer védelmi intézkedéseinek implementálása szintén olyan feladat, amely igényli a különböző szakterületek együttműködését. A kiberbiztonsági audit követelményrendszere[14] a NIST Special Publication 800-53A Revision 5[15] dokumentumra épül, ezért az MI-rendszerek kockázatelemzésénél célszerű a NIST MI-rendszerekre vonatkozó iránymutatás[16] alkalmazása.

Záró gondolatok

A mesterséges intelligencia fejlesztésében és alkalmazásában nem kerülhetők meg a jogi és technológiai szempontok összehangolásának kihívásai. Az MI-rendszerek akkor lehetnek hosszú távon sikeresek, ha értékalapúak, jogszerűek és társadalmilag elfogadhatók. Ez azonban nem valósulhat meg úgy, ha a projekt egyik szereplője dominálni akarja a másikat.

Az MI-projektek során valódi együttműködésre van szükség: jogászabb informatikusokra és informatikusabb jogászokra. Csak így hozhatunk létre hidat a két szakma között – fekete lyuk helyett.

14 a kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról szóló 1/2025. (I. 31.) SZTFH rendelet 5. melléklet

15 NIST SP 800-53A Rev. 5 Assessing Security and Privacy Controls in Information Systems and Organizations

16 NIST AI Risk Management Framework (AI RMF)