Az MI rendszerek szabályozása és adatvédelmi kihívásai

Allianz Hungária Zrt.
Dr. Takács Amarillis
adatvédelmi tisztviselő és
kamarai jogtanácsos

Budapest,
2022. november 25.

Mi az MI?

"Bármely kellően fejlett technológia megkülönböztethetetlen a mágiától.„

Arthur C. Clarke

Mi az MI?

Ahogyan elképzeljük….

Mi az MI?

A valóság….

MI rendszerek szabályozása

2020

Fehér könyv

AIDA

2020

2021

EU állásfoglalásai az MI felhasználásával kapcsolatban

Első jogszabálytervezet

2021

2022

Széleskörű véleményezés

Tervezet parlamenti vitája és elfogadása

2022-2023

MI rendszerek szabályozása

Allianz

Jogszabálytervezet[1]

1. Definíciók, valamint az MI-rendszerek forgalomba hozatalára, üzembehelyezésére és használatára vonatkozó szabályok.
2. Tiltott MI rendszerek: társadalmi pontozás; valós idejű megfigyelés bűnüldözési célból; távoli arcfelismerés; személyiséget torzító, manipulatív MI technikák alkalmazása stb
3. A „nagy kockázatú” MI-rendszerekre vonatkozó specifikus követelmények.
4. Átláthatósági szabályok
5. A piaci nyomon követésre és a piacfelügyeletre vonatkozó szabályok.
6. A bírság legmagasabb összege akár 30millió EUR is lehet, illetve a vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 6 %-át kitevő összeg

→ 24 hónap áll majd rendelkezésre megfelelés biztosítására

1 https://www.kaizenner.eu/post/aiact-part3

MI rendszerek szabályozása

Allianz

MI definíciója

2021-es tervezet:

"mesterséges intelligencia rendszer" (AI rendszer): olyan rendszer, amely
(i) gépi és/vagy emberi alapú adatokat és inputokat kap,
(ii) az I. mellékletben felsorolt technikákkal és megközelítésekkel végrehajtott tanulás, következtetés vagy modellezés segítségével következtet arra, hogy hogyan lehet egy adott emberi meghatározás szerinti célkitűzést elérni, és
(iii) outputokat állít elő tartalom (generatív mesterséges intelligencia rendszerek), előrejelzések, ajánlások vagy döntések formájában, amelyek befolyásolják a környezetet, amellyel kölcsönhatásba lép.

2022.11.03.-as tervezet:

"mesterséges intelligencia rendszer" (AI rendszer): olyan rendszer, amelyet úgy terveztek, hogy bizonyos szintű autonómiával működjön, és amely a gépi és/vagy az ember által szolgáltatott adatok és inputok alapján gépi tanulás és/vagy logikai és tudásalapú megközelítések* segítségével következtet arra, hogyan lehet egy adott, ember által meghatározott célkitűzést elérni, és a rendszer által generált kimeneteket, például tartalmat (generatív AI rendszerek), előrejelzéseket, ajánlásokat vagy döntéseket állít elő, amelyek befolyásolják azt a környezetet, amellyel az AI rendszer kölcsönhatásba lép;

*Bizottság végrehajtási rendeletben fogja szabályozni

1. https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52021PC0206&from=FR

MI rendszerek szabályozása

Allianz

Magas kockázat

2021. novemberi tervezet:

A III. mellékletben említett mesterséges intelligencia rendszereket magas kockázatúnak kell tekinteni.

2022.11.03.-as tervezet:

A III. mellékletben említett mesterséges intelligencia rendszereket magas kockázatúnak kell tekinteni, kivéve, ha a rendszer kimenete pusztán kisegítő jellegű a vonatkozó intézkedés vagy döntés tekintetében*, és ezért valószínűleg nem vezet jelentős kockázathoz az egészségre, biztonságra vagy alapvető jogokra nézve;

*Bizottság végrehajtási rendeletben fogja szabályozni

kritikus infrastruktúrák	**biometrikus azonosítás**	**oktatás**
HR menedzsment	**igazságszolgáltatás és demokratikus joggyakorlás**	**bevándorlási jogok**
alapvető magánszolgáltatások, közszolgáltatások és ellátások elérhetősége és igénybevétele		

MI rendszerek szabályozása

Allianz

Magas kockázat

III. Melléklet
5. Az alapvető magánszolgáltatások, közszolgáltatások és ellátások elérhetősége és igénybevétele:
2021-es tervezet:
Biztosítási díjak meghatározására, kockázatvállalásra és kárrendezési eljárásokra szolgáló mesterséges intelligencia-rendszerek.

2022.11.03.-as tervezet:
A természetes személyekre vonatkozó kockázatértékelési és árazási célú mesterséges intelligencia alapú rendszerek az élet- és egészségbiztosítások esetében, kivéve a mikro- és kisvállalkozásoknak minősülő szolgáltatók által üzembe helyezett mesterséges intelligencia alapú rendszereket.*
*Bizottság bővítheti ezt a kört

MI rendszerek szabályozása

Allianz

Követelmények - Számonkérhetőség

Technikai 	✓ beépített emberi felügyelet ✓ auditálhatóság, stabilitás, IT biztonság ✓ méltányosság (fairness), magas adatminőség, adatkormányzás (data governance), előítéletek korrekciója
Működési 	✓ logolás, részletes technikai dokumentáció ✓ az MI felhasználóinak részletes tájékoztatása, oktatása a rendszer működéséről ✓ forgalomba hozatal/élesítés utáni nyomonkövetés
Eljárási 	✓ megfelelőségi vizsgálatok, értékelések (független harmadik személyek) ✓ MI regisztrációja a nyilvános EU adatbázisban (ha szükséges) ✓ incidens bejelentés

MI rendszerek szabályozása

Emberi felügyelet – AIDA jelentése az EP-nek

„hangsúlyozza, hogy egy adott mesterséges intelligencia-alkalmazás kockázati szintje jelentősen változhat a károkozás valószínűségétől és súlyosságától függően; ezért kiemeli, hogy a jogi követelményeket ehhez kell igazítani, a kockázatalapú megközelítéssel összhangban, és indokolt esetben kellően figyelembe véve az elővigyázatosság elvét; hangsúlyozza, hogy az olyan jelenlegi vagy jövőbeli esetekben, amikor egy adott felhasználási területen a mesterséges intelligencia-rendszerek magas kockázatot jelentenek az alapjogokra és az emberi jogokra, teljes körű emberi felügyeletre és szabályozási beavatkozásra van szükség, és hogy a technológiai fejlődés sebességére tekintettel a magas kockázatú mesterséges intelligencia-rendszerekre vonatkozó szabályozásnak rugalmasnak és jövőállónak kell lennie;”

„a magas kockázatú mesterséges intelligencia-rendszerekben a tervezés általi biztonságra és a megfelelő képzésen alapuló érdemi emberi felügyeletre, valamint a megfelelő biztonsági és adatvédelmi biztosítékokra van szükség az automatizálási elfogultságok leküzdése érdekében;”[1]

1. PR_INI (europa.eu))

MI rendszerek szabályozása

Emberi felügyelet – Európai Parlament jelentése

„az MI képességei biztonsági kockázatot is jelenthetnek, mivel az embereket arra késztetheti, hogy indokolatlan bizalmat helyezzenek a mesterséges intelligenciába, és már jobban bízzanak benne, mint saját ítélőképességükben; … megjegyzi, hogy kísérletek bizonyítják, hogy a mesterséges intelligencia autonómiájának szintje túlléphet azon a támogató szerepkörön, amelyre azt eredetileg tervezték, …; hangsúlyozza, hogy az automatizálási elfogultság (automation bias) leküzdése érdekében a magas kockázatú MI-rendszerekben gondoskodni kell a beépített biztonságról és a megfelelő képzésen és megfelelő biztonsági és adatvédelmi biztosítékokon alapuló érdemi emberi felügyeletről”[1]

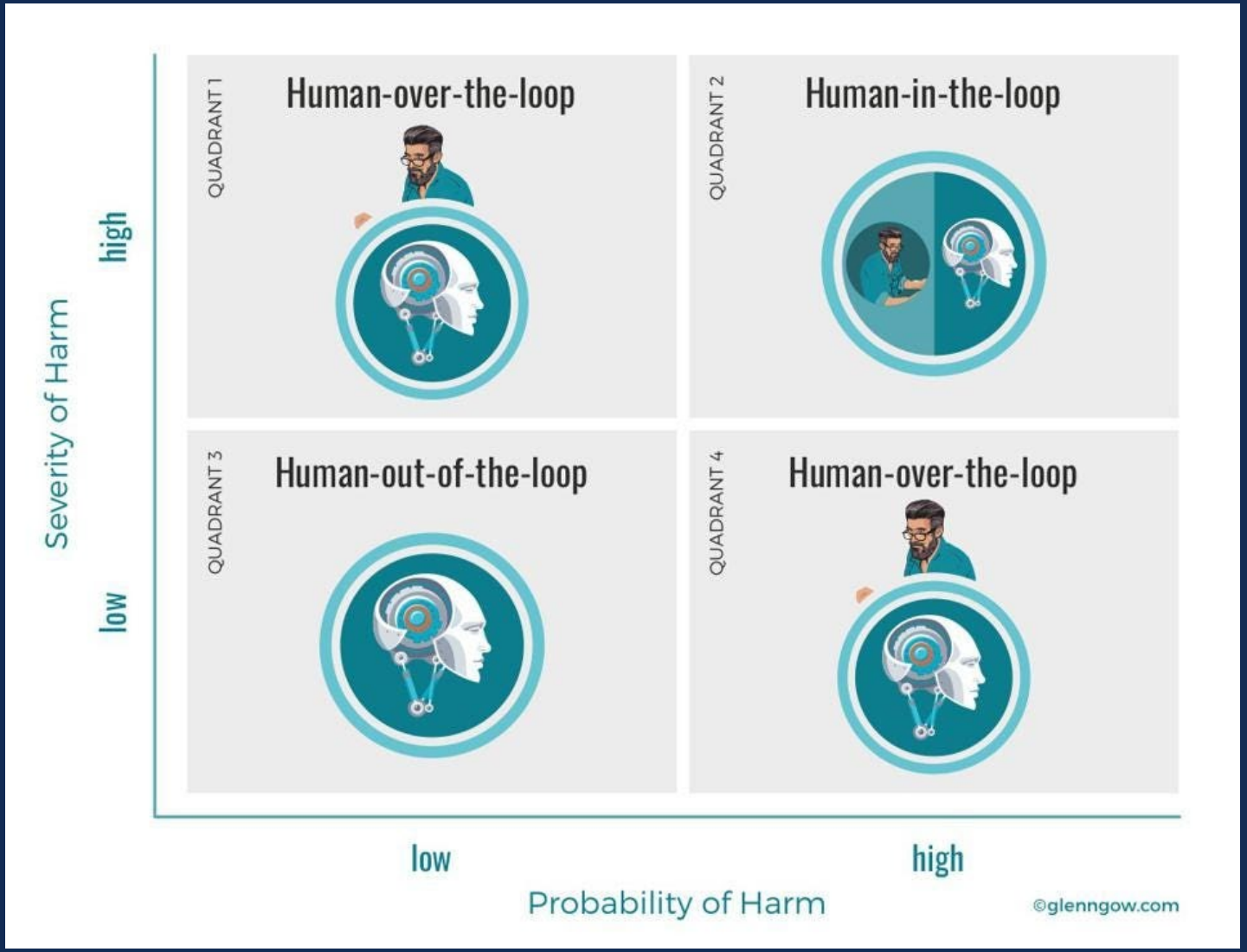
„automation bias” jelentése

1. Elfogadott szövegek - A mesterséges intelligencia a digitális korban - 2022. május 3., Kedd (europa.eu)

MI rendszerek szabályozása

Allianz

Emberi felügyelet



MI rendszerek szabályozása

Emberi felügyelet – AIA 14. cikk

1. A magas kockázatot jelentő mesterséges intelligencia rendszereket úgy kell megtervezni és fejleszteni, többek között megfelelő ember-gép interfész eszközökkel, hogy természetes személyek hatékonyan felügyelhessék azokat a mesterséges intelligencia rendszer használatának időtartama alatt.
4. (4) Az (1)-(3) bekezdés végrehajtása céljából a magas kockázatú mesterséges intelligencia rendszert úgy kell a felhasználó rendelkezésére bocsátani, hogy a körülményeknek megfelelően és azokkal arányosan lehetővé tegyék azon természetes személyek számára, akikre emberi felügyeletet ruháztak, hogy:
(a) megértsék a magas kockázatú mesterséges intelligencia rendszer képességeit és korlátait, és képesek legyenek megfelelően ellenőrizni annak működését;
(b) tudatában maradjanak annak a lehetséges tendenciának, hogy a magas kockázatú mesterséges intelligenciával rendelkező rendszer által előállított eredményekre automatikusan támaszkodnak vagy túlzottan támaszkodnak (" automatizálási elfogultság");
(c) helyesen értelmezzék a magas kockázatú mesterséges intelligencia rendszer kimenetét, figyelembe véve például a rendelkezésre álló értelmezési eszközöket és módszereket;
(d) lehetősége van bármely konkrét helyzetben úgy dönteni, hogy nem használja a magas kockázatú mesterséges intelligenciát alkalmazó rendszert, vagy más módon figyelmen kívül hagyja, felülbírálja vagy visszafordítja a magas kockázatú mesterséges intelligenciát alkalmazó rendszer kimenetét;
(e) beavatkozni a magas kockázatú mesterséges intelligencia rendszer működésébe, vagy megszakítani a rendszert "stop" gomb vagy hasonló eljárás segítségével.

MI rendszerek adatvédelmi kihívásai

Allianz

Egy NAIH ügy tanulságai[1]

1) Ügy ismertetése

2) MI-nek minősül a rendszer vagy sem?

3) Tájékoztatási kötelezettség → Érzelemfelismerő rendszer → AIA külön, önálló tájékoztatási kötelezettséget ír elő az ilyen MI rendszerekre

52. cikk 1. A szolgáltatók biztosítják, hogy a természetes személyekkel való interakcióra szánt mesterséges intelligencia rendszereket úgy tervezik és fejlesztik, hogy a természetes személyeket tájékoztassák arról, hogy mesterséges intelligencia rendszerrel lépnek interakcióba, kivéve, ha ez egy ésszerűen tájékozott, figyelmes és körültekintő természetes személy szemszögéből nyilvánvaló, figyelembe véve a körülményeket és a használat kontextusát.
52. cikk 2a. Az érzelemfelismerő rendszer alkalmazói tájékoztatják a rendszer működéséről az annak kitett természetes személyeket.
3a. A tájékoztatást a természetes személyeknek világos és megkülönböztethető módon kell megadni legkésőbb az első interakció vagy kitettség időpontjában.

1. https://naih.hu/hatarozatok-vegzesek/file/517-mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei

MI rendszerek adatvédelmi kihívásai

Egy NAIH ügy tanulságai[1]

4) Pontosság: „a rendszer hatékonysága erősen megkérdőjelezhető, mivel nem volt felismerhető érzelem az esetek 91,96 %-ban”

15. cikk 1. A nagy kockázatú mesterséges intelligenciával rendelkező rendszereket úgy kell megtervezni és fejleszteni, hogy rendeltetésüknek megfelelően megfelelő pontossági […] szintet érjenek el, és e tekintetben életciklusuk során következetesen teljesítsenek.

2. A nagy kockázatú mesterséges intelligenciával rendelkező rendszerek pontossági szintjeit és a vonatkozó pontossági mérőszámokat a használati leírásban kell feltüntetni.

5) Kockázatértékelés – hatásvizsgálat – érdekmérlegelés

A GDPR szerinti hatásvizsgálat nem elegendő: + etikai szempontok, MI kockázatának megállapítása → arányosság

„Az Európai Adatvédelmi Testület és az Európai Adatvédelmi Biztos 5/2021. sz. közös véleménye a mesterséges intelligenciára vonatkozó harmonizált szabályok (a mesterséges intelligenciáról szóló jogszabály) megállapításáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslatról az alábbi megállapítást tartalmazza: Az Európai Adatvédelmi Testület és az Európai Adatvédelmi Biztos úgy véli továbbá, hogy az MI természetes személyek érzelmeinek levezetésére való felhasználása rendkívül nemkívánatos, és azt meg kell tiltani bizonyos jól meghatározott felhasználási esetek – nevezetesen az egészségügyi vagy kutatási célú felhasználás (például betegek, akiknek esetében fontos az érzelmek felismerése) – kivételével, minden esetben megfelelő biztosítékok és természetesen az összes többi adatvédelmi feltétel és korlátozás alkalmazása mellett, ideértve a célhoz kötöttséget is.”

1. https://naih.hu/hatarozatok-vegzesek/file/517-mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei

Az MI rendszerek szabályozása és adatvédelmi kihívásai

Allianz

Ajánlott olvasmányok

Documents and Timelines: The Artificial Intelligence Act (part 3) (kaizenner.eu)
PA_Legam (europa.eu)
EU AI Act – Proposed Amendments by the EU Committee on Legal Affairs, Tom Whittaker (burges-salmon.com)
AI Regulation in Europe | Morrison Foerster (mofo.com)
The EU AI Act will have global impact, but a limited Brussels Effect (brookings.edu)
Beyond Data | SpringerLink

Köszönöm a figyelmet!

Allianz Hungária Zrt.
Dr. Takács Amarillis
adatvédelmi tisztviselő és kamarai jogtanácsos