SZAKDOLGOZAT

Adatvédelem
és
mesterséges intelligencia
–
új kihívások a jog területén

Miskolci Egyetem

Állam- és Jogtudományi Kar

Alkotmányjogi Tanszék

Készítette:
dr. Czank Dóra
KWQ1I4
Complience (megfelelési) szakjogász
szakirányú továbbképzés

Konzulens:
Dr. Jámbor Adrienn
adjunktus
Államtudományi Intézet
Alkotmányjogi Tanszék

2024

THESIS

Data Protection
and
Artificial Intelligence
–
new challeges in the field of law

University of Miskolc

Faculty of Law

Department of Constitutional Law

Written by:
dr. Czank Dóra
KWQ1I4
LLM Complience
postgraduate specialist training course

Consultant:
Dr. Jámbor Adrienn
assistant lecturer
Institute of Public Law
Department of Constitutional Law

2024

TARTALOMJEGYZÉK

1. BEVEZETÉS

1.1. Mesterséges Intelligencia – egy segítő barát vagy alattomos ellenség?

Több, mint 10 éve történt, hogy a Facebookon szembe jött velem egy hirdetés, mi szerint segítőket keresnek, akik vállalják, hogy – önkéntes alapon – egy kb. negyven perces teszt kitöltésével hozzájárulnak ahhoz, hogy egy önvezető autót megtanítsanak jó döntéseket hozni. A tesztben nagyon sokféle példát vázoltak fel arra vonatkozóan, hogy milyen szituációk fordulhatnak elő egy olyan forgalmi helyzetben, amikor egy autó egy gyalogátkelőhelyhez ér. A legártatlanabb és legveszélytelenebb természetesen az, amikor az autót vezető észleli, hogy valaki a járdán arra vár, hogy átkelhessen az úttesten: az vezető fékez, a zebra előtt megáll, a gyalogos pedig szabályosan átmegy az út másik oldalára. Azonban a mindennapi életben számtalan olyan helyzet adódhat, amely korántsem ilyen veszélytelen. Befolyásolhatják az autó vezetőjét a látási viszonyok, a saját reakció ideje, egy hirtelen felbukkanó gyalogos, kerékpáros, kisállat, szembejövő, veszélyes manővert végrehajtó autós. De veszélyhelyzet alakulhat ki akkor is, ha a gyalogátkelőhelyen átkelni szándékozó siet, elbambul, a telefonját nyomkodja, a kisgyerek – nem érzékelve a veszélyt – az útra szalad, a kerékpáros nem száll le a kerékpárjáról és az úttestre hajt.

Nekem, a teszt kitöltőjének az volt a feladatom, hogy döntéseket kellett hoznom arról, hogy az adott szituációban hogyan döntenék, ki sérüljön meg: a gyalogos, az autót vezető vagy éppen az adott helyzetben jelenlevő másik személy. Morális döntések voltak ezek elsősorban, hiszen ki legyen inkább az áldozat: egy idős bácsi vagy a gyermekét toló édesanya? A cicát gázoljam-e el vagy az autóm sérüljön súlyosabban? Üssek el három felnőttet vagy inkább egy gyereket? Nehéz volt a döntés, de minden esetben dönteni kellett valahogy. A való életben ennyi idő nincsen egy-egy döntésre, ösztönösen cselekszünk.

Azonban itt nem ösztönös cselekvésről, hanem kőkemény döntésekről volt szó, amelyek egy hatalmas adatbázisba bekerülve arra szolgáltak, hogy egy ösztönöktől mentes rendszert megtanítsanak arra, hogy egy vészhelyzet esetén mi a helyes megoldás.

Ez volt az első – tudatos – találkozásom a mesterséges intelligenciával vagy legalábbis annak egy apró részletével, hiszen a gépi tanulás során szükséges adatok egy (meglehetősen) minimális részét én szolgáltattam.

A találkozást azóta számos eset követte, ma pedig – ha nem is mindig vagyunk tudatában – rengeteg olyan helyzet van, amikor használjuk az MI-t.

Vagy „ő" használ minket…?

És vajon jó ez nekünk?

De lássunk néhány példát!

Középiskola, 11. osztály, feladat: írj esszét az első világháború kialakulásának okairól! Az osztály egynegyede előveszi a történelemkönyvet, és kimásolja a legfőbb okokat, eseményeket. Az osztály fele a Google segítségével írja meg az esszét, forrásokat, esetleg kész tanulmányokat keres, azokból dolgozik. A maradék 25 százalék – és arányuk exponenciálisan fog nőni a közeljövőben – ChatGPT-t vagy Gemini-t hívja segítségül, ami – generativ mesterséges intelligenciához méltóan – kész szöveget ad a modern nebuló kezébe. Itt már csak azon múlik a siker, hogy a végén a jó jegyet elérni szándékozó tanuló átolvassa-e a dolgozatot, és kiszűri-e azokat a most még sokszor előforduló „hozzáköltéseket", ami abból adódik, hogy az MI olyan szöveget akar előállítani, ami legjobban megfelel a kérésnek. Hiszen ha csak azt írjuk be kérésként, hogy „Írj esszét az első világháború kialakulásainak okairól!", akkor könnyen előfordulhat, hogy az eredmény egy esszé lesz, amiben vannak okok, amelyek akár az első világháború kialakulásához (is) vezethettek (volna), de a valósághoz nem sok köze van. Ha viszont forrásmegjelölésekkel, pontos adatokkal, esetleg további sarokpontok megadásával tesszük ugyanezt, már sokkal jobb eredményre számíthatunk. Nem véletlen az, hogy a promt engineering jelenleg az egyik leginkább fellendülőben lévő szakma.[1]

A ChatGPT-t azonban természetesen nem csak jó jegyre vágyó kamaszok használják, hanem komoly szakemberek is: mérnökök, informatikusok hívják segítségül a munkájuk során felmerülő problémák beazonosítására és kijavítására. Közvetlen környezetemben is van olyan, aki azt mondja, hogy az Open AI által fejlesztett MI által munkájának hatékonysága megsokszorozódott, hiszen egy-egy program hibás kódjának kiszűrése és

[1] A prompt egy olyan kifejezés, amelyet széles körben használnak a számítástechnika és az AI területén. Informatikai környezetben a prompt a felhasználói felületen megjelenő szöveg vagy jel, ami a felhasználónak adatbevitelre vagy parancsok meghatározására szolgál.

kijavítása a Chat GPT számára csak pár perc, míg neki órákba vagy akár napokba telne. A gépi tanulás, illetve ennek egy még bonyolultabb változata, az úgynevezett mélytanulás segítségével pedig olyan önműködő rendszereket tud kialakítani az előrejelzés területén, amely sokkal több tényezőt figyelembe véve hihetetlenül pontos adatokat tud kiszámítani.

Az orvostudomány is egyre nagyobb arányban használja az MI-t, elsősorban a diagnosztika területén, hiszen a bevitt (elsősorban képalkotó eljárással készített) adatok feldolgozása, elemzése és az ebből keletkeztetett eredmény pontosabb, az eljárás gyorsabb, és a gép soha nem fárad el.

Mint ahogy az ügyfélszolgálatokon egyre több helyen jelen levő virtuális asszisztensek is mindig ugyanolyan kedvesen próbálnak segíteni – legyen szó délelőtt 11-ről vagy éjjel 2-ről. Innen pedig már csak egy aprócska ugrás a kettő összekapcsolása: egy mindig segíteni kész, kedves és megnyugtató hangú virtuális nővérke, aki megfelelő tablettát ajánl allergiára vagy időpontot ad vérvételre.

Okos telefon – amellyel ma már nem is elsősorban telefonálunk, hanem e-mailezünk, chatelünk, információkat keresünk, (virtuális) szociális életet élünk, banki ügyeinket intézzük, védi az egészségünket (megdicsér, ha elég lépést tettünk és figyelmeztet, ha nem ittunk eleget).

Okos otthon – amelyben a fűtés és a hűtés, a páratártalom szabályozása, a lámpák fel- és lekapcsolása, a fény erőssége, sőt színe az adott otthonban élők igényeihez alkalmazkodik, de mindamellett figyelembe veszi a környezetvédelmi, energiatakarékossági szempontokat is.

Okos város – amely olyan környezetet teremt, ahol a legoptimálisabbak a viszonyok a városlakók számra a stresszmentes, környezetvédelmi és egészségügyi szempontból leginkább megfelelő életvezetéshez, legyen szó közlekedésről, biztonságról, szórakozásról.

Az életünket jobbá teszi az MI. Kevesebb stressz, hatékonyabb szolgáltatások, gyorsabb ügyintézés.

De biztosan minden szempontból így van ez? Vizsgáljuk meg az érem másik oldalát!

Az MI működéséhez adatok kellenek, ha szemléletesen szeretnénk fogalmazni, azt mondhatnánk, hogy az MI-t adatokkal kell etetnünk ahhoz, hogy jól tudjon működni. Ezek között az adatok között pedig nagyon sok esetben ott vannak személyes adataink is.

Amikor a ChatGPT-t valamilyen produktum létrehozására bírjuk rá, néha – öntudattalanul is – személyes adatokat is elárulunk magunkról (Írd meg ezt az esszét úgy, mintha azt egy tizenegyedik osztályos, megyeszékhelyen élő, diplomás szülőkkel rendelkező, olvasni nem szerető, de a földrajz iránt érdeklődő lány írta volna.)

Az okos telefon használata során pedig szinte kiírjuk magunkra: ez vagyok én! Ha a közösségi médiát használjuk, ha bankolunk, de ha csak egy nyilvános wifi hálózatra csatlakozunk fel a telefonnal, máris egy sor olyan adatot adtunk ki magunkról, amelyekkel mint természetes személy beazonosíthatóvá válunk. Természetesen a rendszerek döntő többsége védi az adatainkat, hiszen erre jogszabályi kötelezettségük van.

De vajon az MI esetében kié lesz a felelősség akkor, ha adataink illetéktelen kezekbe kerülnek és olyan célra használják őket, amire mi nem szeretnénk? A fejlesztő lesz a felelősségre vonható? Netán az MI-t felhasználó vállalkozás (például egy orvos a diagnosztika esetében)? Esetleg mi magunk is tehetünk arról, ha adataink „rossz kezekbe kerülnek”?

A Miskolci Egyetem ÁJK Complience szakjogász képzésén megtanultam, hogy - vállalatok esetében – mindig három réteg van, amely garantálja azt, hogy egy vállalat comlience szempontjából megfelelően működjön: az első réteg a jogszabályok szintje, amelyek betartása törvényi kötelezettség, megsértésük olykor igen súlyos hatósági, igazságszolgáltatási következménnyel jár. Azonban a jogszabályok sem szabályoznak mindent. Ezeket a hézagokat a vállalatok belső szabályzatai töltik ki, illetve ugyanezek vetítik le saját belső rendszerükre a jogszabályokat. A belső szabályzatok megsértése elsőként belső vizsgálatokat von maga után, mely csak akkor kerül a rendszeren kívülre, ha feltételezhetően vagy bizonyíthatóan jogszabályok megsértésére is sor került. A harmadik szint pedig az erkölcs, a morál szintje, hiszen egy rendszer, egy vállalat csak akkor működhet megfelelően, ha figyelembe veszi, hogy benne emberek dolgoznak, akik különböző attitűdökkel, drive-okkal rendelkeznek. Egymás közötti viszonyaikat – saját belső kényszerük, erkölcsük, moralitásuk mellett – a vállalat Etikai Kódexe szabályozhatja.

De a mi a helyzet egy olyan új területtel, mint a mesterséges intelligencia?

A kifejezett jogszabályi szabályozás egyelőre „gyerekcipőben” jár. Nagy előrelépést jelentett viszont ezen területen az Európai Unió 2024. március 13-án az Európai

Parlament által döntő többséggel megszavazott AI Act-je[2], mely a világon elsőként ad meg jogszabályi szinten komplex szabályokat a mesterséges intelligenciára vonatkozóan.

Ha a belső szabályokat nézzük, ott már korábban is voltak arra irányuló megkötések, hogy az adott fejlesztő cég mire használja fel az általa létrehozott MI-t. Az Open AI Voice Engine fejlesztése például olyan jól utánozza a természetes beszédhangot, hogy a hallgatóban azt az érzetet kelti, mintha valóban a hangmintát adó természetes személyt hallaná. Éppen ezért a cég úgy döntött, hogy ezt a hangklónozási és beszédgeneráló technológiát csak meghatározott, minősített, az egészségügy és az oktatás területén tevékenykedő partnerei számára teszi hozzáférhetővé.[3]

A nyílt forráskódú mesterséges intelligencia modellek azonban szabadon hozzáférhetőek, továbbfejleszthetőek és csak (rövid) idő kérdése, hogy mikor jelenik meg olyan modell, amely a Voice Engine minden képességével bír, ugyanakkor semmiféle belső szabályozás nincsen az elérhetőségére és felhasználására vonatkozóan.

A harmadik „védelmi” vonal a morál és az erkölcs a fejlesztők és vállalkozások részéről, vagyis annak belátása, hogy meddig mehetnek el a modellek fejlesztése és használata, hasznosítása terén, mi az, ami még erkölcsileg megengedhető és mi az, ami már túlmutat a morálisan megengedhető határon.

Ugyanakkor nekünk, felhasználóknak is önmérsékletet és önszabályozást kell tanúsítanunk. Nem mindegy, hogy kinek, milyen célból, milyen adatokat adunk meg, és ha úgy látjuk, hogy adataink nincsenek biztonságban, tudnunk kell(ene) nemet mondani még akkor is, ha esetleg ezzel valamitől elzárjuk magunkat (nem tölthetjük le a legújabb applikációt a telefonunkra). Információk birtokában mérlegelnünk szükséges.

[2] P9_TA(2024)0138 A mesterséges intelligenciáról szóló jogszabály Az Európai Parlament 2024. március 13-i jogalkotási állásfoglalása a mesterséges intelligenciára vonatkozó harmonizált szabályok (a mesterséges intelligenciáról szóló jogszabály) megállapításáról és egyes uniós jogalkotási aktusok módosításáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslatról (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)) (Rendes jogalkotási eljárás: első olvasat) https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_HU.pdf (2024.03.15.)

[3] Nem biztos hogy tudja: Ön is felhasználó! In: HVG Ai3 – mesterséges intelligencia a mindennapokban. 2024. 7. oldal

Szerencsére az adatvédelemben viszont van segítségünk: az Európai Unió általános adatvédelmi rendelete (GDPR)[4] mellett hazai szinten az Infotv.[5] is védi a természetes személyek adatait.

1.2. A szakdolgozat témája, felépítése

Jelen dolgozatomban a fent felvázoltak tükrében arra keresem a választ, hogy a mesterséges intelligencia térhódítása idején vajon milyen szabályozási nehézségekkel kell szembenéznünk az adatvédelem terén.

Ahhoz, hogy a téma teljes körűen körbejárható legyen, elengedhetetlennek tartom, hogy először is magával a mesterséges intelligencia fogalmával, mibenlétével ismerkedjünk meg. Ezután rátérek az adatvédelem, ezen beül is a GDPR azon szabályozási részleteire, amelyek kifejezetten vonatkoztathatóak a mesterséges intelligenciára (beépített adatvédelem, automatizált döntéshozatal, profilalkotás). A harmadik nagy részben az AI Act néhány – adatvédelemmel kapcsolatos – részletét szeretném kiemelni. Az utolsó részben pedig egy konkrét példán keresztül szeretnék rávilágítani az adatvédelem és mesterséges intelligencia szoros kapcsolatára és együtt történő szabályozásának szükségességére, ez pedig az okos városokkal kapcsolatos jelenlegi szabályok vizsgálata.

[4] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0679 (2023.03.15.)

[5] Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény

2. A MESTERSÉGES INTELLIGENCIA TÖRTÉNETE

2.1. A régmúlt

Ha a tágabb értelemben vett mesterséges intelligenciával szeretnénk foglalkozni, visszamehetnénk akár 1642-be is, amikor a francia matematikus és feltaláló Blaise Pascal megalkotta az első mechanikusan működő számológépet, vagy visszaugorhatunk 1837-be, amikor Charles Babbage és Ada Lovelace programozható gépének első formája megjelent. Ez azonban talán túl távoli múlt és a történelem azt mutatja, hogy sokáig ezeket a kezdeteket nem is igazán követték jelentős fejlesztések.

A XX. század azonban már bebizonyította: a technológiai fejlődés ezen a területen is felgyorsult. A mesterséges intelligencia úttörő lépései nagyjából 80 évvel ezelőtt történtek olyan egyszerű számítógépes technológiákkal, mint Claude Shannon „Theseus" egere, amely képes volt egy speciális útvesztőben tájékozódni és útvonalakat megjegyezni. Ebben az időben kezdtek el kísérleteket folytatni azzal kapcsolatban, hogy hogyan tudja egy gép neurális hálózatok segítségével az emberi elme működését modellezni (Warren McCullogh és Walter Pitts, 1943). Nem sokkal később találta ki Turing a róla elnevezett tesztet (1950), amelynek segítségével vizsgálni lehet azt, hogy mennyire képes „emberi" gondolkodásra egy mesterségesen létrehozott entitás.

2.2. A múlt

Még mindig a múltban járunk, de láthatjuk, hogy a fejlődés egyre gyorsuló ütemet mutat. A *The History of AI: From Beginnings to Breakthroughs* című YouTube-videó[6] segítségével szeretném bemutatni a mesterséges intelligencia fejlődésének ezen időszakát.

A híres Dartmouth Summer Research Project-et (1956) tekinthetjük a mesterséges intelligencia kutatás hivatalos kezdetének. Amellett, hogy itt találták ki és töltötték meg először tartalommal a mesterséges intelligencia kifejezést, a résztvevők egyetértettek abban, hogy a mesterséges intelligencia létrehozása igenis lehetséges, és ambiciózus célokat tűztek ki ezen a területen. Úgy gondolták, hogy lehetséges olyan gépeket építeni, amelyek képesek lesznek az emberéhez hasonló intellektuális feladatokat ellátni, sőt, akár

[6] https://www.youtube.com/watch?v=iZCNDZ7ABRE (2024. 04.04.)

túl is szárnyalhatják az emberi intelligenciát. A Dartmouth Workshop igazi mérföldkő volt a mesterséges intelligencia történetében, hiszen az itt végzett munka és az itt megálmodott célkitűzések nem csak inspirálták az ezzel foglalkozó szakembereket szerte a világon, de elindították a mesterséges intelligencia kutatásának és fejlesztésének évtizedek óta tartó hullámát, amely ma is az egyik legaktívabb és legizgalmasabb tudományos terület.

Igazán látványos fejlődést tapasztalhattunk az elmúlt két évtizedben, mikor is a mesterséges intelligencia óriási fejlődést mutatott be a nyelv- és képfelismerés terén, és ma már emberi szinten vagy azt meghaladóan teljesít ezen a téren. A korai MI-rendszerek még elmaradtak az emberéhez hasonló képességek szintjétől, de napjainkban már különböző kognitív feladatokban is kiválóan teljesítenek.

2.3. A jelen

A különböző technológiájú és számos tevékenységi területen működő mesterséges intelligencia modellek zökkenőmentesen beépültek a mindennapi életünkbe. Nem múlhat el nap anélkül, hogy újabb és újabb áttörésekről, felhasználási területekről szóló hírrel ne találkoznánk. Sőt, olykor már észre sem vesszük, hogy körülvesz bennünket az MI, gondoljunk csak a közösségi média hírfolyamának alakításában, vagy az online vásárlási ajánlatok bemutatásában kulcsfontosságú szerepet játszó mesterséges intelligencia által létrehozott algoritmusokra!

Ebben a technológia szempontjából is felgyorsult világban nem árt ismerünk olyan kifejezéseket, mint a gépi tanulás (machine learning) és a mély tanulás (deep learning). Eszteri Dániel tanulmányában érthetően és szemléletesen magyarázza meg a fenti fogalmakat.[7] A szerző leírja, hogy míg a mesterséges intelligencia magában foglal minden olyan eljárást, amely során egy szoftver automatikusan hoz meg egy bizonyos döntést, addig a gépi tanulás során a rendszer tapasztalatokból generál önálló tudást. Ezt úgy kell elképzelnünk, hogy hatalmas adatbázisokban, példaadatokban kell önállóan vagy emberi segítséggel irányítottam bizonyos mintázatokat megkeresnie, majd a felfedezett szabályszerűségeket felhasználva döntéseket hoznia (így működik például egy előrejelző

[7] Eszteri Dániel: A gépek adatalapú tanításának megfeleltetése a GDPR egyes előírásainak. In: Török Bernát – Ződi Zsolt (szerk.): A mesterséges intelligencia szabályozási kihívásai. Ludovika Egyetemi Kiadó. Budapest. 2021. 190-197. o.

modell). A gépi tanulás egyik ága a mélytanulás, mely neuronhálózatok alkalmazásán alapszik, melyeket a korábban említett McCullogh és Pitts alkotott meg biológiai ideghálózatok mintájára. Itt is betáplált adatokból indul ki rendszer, azonban egy lépéssel tovább haladva itt már találhatunk egy, az adatokból megszerzett információkra épülő tanuló algoritmust is. Ennek köszönhetően a rendszer absztrakciós készsége tovább növekszik és pontosabb megoldásokat tud létrehozni a feltett kérdések vagy megoldásra váró feladatok körében.

Hogy mindez PONTOSAN hogyan működik? Nos, jó pár esetben maguk az MI létrehozói, fejlesztői sem képesek arra, hogy pontos magyarázatot adjanak, illetve sok esetben aggályként merül fel (akár adatvédelmi szempontból is), hogy nem lehet előre megjósolni az eredményt. A modell produkálhat olyan eredményt is, amire látszólag semmilyen magyarázat nem létezik. Ezt a jelenséget nevezik *fekete doboznak*. (A 3.2. fejezetben[8] ez az információ még lényeges lesz.)

2.4. A jövő

A jövő már elkezdődött és feltartóztathatatlanul száguld velünk. A következő mérföldkövet az általános mesterséges intelligencia kifejlesztése (vagy kifejlődése) fogja jelenteni. Az Artifical General Intelligence (AGI) olyan mesterséges intelligencia modell, amely egyben képes olyan feladatok univerzális ellátására, melyeket ma még csak az egyes feladattípusokra „felokosított” modellek külön-külön képesek végrehajtani.

És hogy öntudatra ébrednek-e a gépek? Nos, a kérdés megválaszolása meghaladja a jelen dolgozat kereteit….

[8] 12. oldal

3. AZ ADATVÉDELEM SZABÁLYOZÁSA A MESTERSÉGES INTELLIGENCIA VONATKOZÁSÁBAN (GDPR)

3.1. Az adatvédelemmel kapcsolatos általános felvetések

Péterfalvi Attila, a NAIH elnöke 2020-ban *A mesterséges intelligencia alkalmazásának hatása az alapjogokra* című konferencián elhangzott előadásában[9] utalt az Isaac Asimov által írt *Körbe-körbe* című novellában meghirdetett „*robotika három törvényére*", mely szerint a (1) a robotnak nem szabad kárt okoznia emberi lényben, (2) a robot engedelmeskedni tartozik az emberi lények utasításainak, illetve (3) a robot tartozik saját védelméről is gondoskodni. Erre reflektálva Elnök úr elmondta, hogy ezek a törvények a mesterséges intelligencia vonatkozásában ma is érvényesek, és a jogalkotók, legyen szó az Európai Unióról vagy Magyarországról, igyekeznek gondoskodni arról, hogy a mesterséges intelligencia használata – melyből kimaradni semmiképpen nem szerencsés és nem is szabad – minden szempontból szabályozott legyen és biztonságosan működjön. Az új technológiák alapvetően értéksemlegesek és a mi feladatunk az, hogy értéket rendeljünk hozzájuk, vagyis mi határozzuk meg azt, hogy milyen technológiák és felhasználási területek azok, amelyek a társadalom számára hasznosak. További feladatunk az, hogy az új technológiák felhasználásával járó kockázatokat felismerjük és kezelni tudjuk. Ennek egyik eszköze az a személyes adatok védelme.

AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről, vagyis az általános adatvédelmi rendelet (GDPR) az Európai Unió tagállamaiban, így Magyarországon is közvetlenül hatályos, jogrendszerünk része. Rendelkezései között találjuk a – jelen dolgozat szempontjából kiemelten fontos – (15) preambulumbekezdést, amely kimondja a *technológiasemlegesség* követelményét, azaz a személyes adatok védelme nem függhet a felhasznált technológiai megoldásoktól. Mindegy tehát, hogy az adatok kezelése milyen technológiával történik, a személyes adatok védelméről az adatkezelőnek minden körülmények között gondoskodnia kell.

[9] Péterfalvi Attila: Algoritmusok és adatvédelem: Quo vadis? In: Török Bernát – Ződi Zsolt (szerk.): A mesterséges intelligencia szabályozási kihívásai. Ludovika Egyetemi Kiadó. Budapest. 2021. 179-180. o.

3.2. Az automatizált döntéshozatal

Korábban már szó esett arról, hogy a mesterséges intelligencia modellek működéséhez adatokra van szükség, melynek egy része (adott esetben jelentős része vagy döntő többsége) a GDPR hatálya alá eső személyes adat. Ilyen személyes adatokat használnak például a bankok akkor, amikor hitelkérelmet bírálnak el automatizált döntéshozatal keretében.

Az automatizált döntéshozatalt a GDPR 22. cikke szabályozza. De mit takar maga a fogalom? Az általános adatvédelmi rendelet értelmező rendelkezései nem tartalmaznak információkat az automatizált döntéshozatalra vonatkozóan (azok a 22. cikk vonatkozásában kizárólag a profilalkotást mint fogalmat magyarázzák meg – erről később lesz szó). Segítségül hívhatjuk viszont a WP29 iránymutatását[10], mely szerint „az automatizált döntéshozatal az a képesség, hogy technológiai eszközök segítségével, emberi beavatkozás nélkül hoznak döntéseket”.[11] Ilyen lehet egy hitelképesség-bírálat vagy egy – előzetes kereséseken alapuló – célzott reklám megjelenítése a közösségi médiában, amennyiben az teljes egészében emberi beavatkozás nélkül történik.

A 22. cikk (1) bekezdése kimondja, hogy „*az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené*”. Bár megfogalmazása alapján első olvasatra úgy tűnik, hogy ez egy érintett számára nyújtott jogosultság, azonban a jogalkotó ezzel sokkal inkább egy adatkezelő számára fennálló általános tilalmat fogalmazott meg arra vonatkozóan, hogy nem alkalmazhat olyan eljárásokat, amelyek során kizárólag automatizált adatkezelésen alapuló döntéshozatal valósul meg, amennyiben ez döntés az érintettre nézve joghatással vagy hasonlóképpen jelentős hatással járna. Ilyen eset lehet például, ha az automatizált döntéshozatal eredményeképpen valamilyen szerződést felmondanak, valamilyen jogosultságot – például egy országba történő belépést – megtagadnak.

---

[10] Az Európai Unió tagállamainak adatvédelmi felügyeleti hatóságait tömörítő, az Európai Adatvédelmi Testület (EDBP) jogelődjének tekinthető, úgynevezett 29. cikk szerinti Adatvédelmi Munkacsoportja (WP29) 2017. október 3-án hozta nyilvánosságra iránymutatását az automatizált döntéshozatallal és a profilalkotással kapcsolatban.

[11] Iránymutatás az automatizált döntéshozatallal és a profilalkotással kapcsolatban 2016/679 rendelet alkalmazásához
https://www.naih.hu/files/wp251rev01_hu.pdf 8. oldal (2024.03.25.)

A 22. cikk (2) bekezdése nevesíti az (1) bekezdés alóli kivételeket is:

„Az (1) bekezdés nem alkalmazandó abban az esetben, ha a döntés:

a) *az érintett és az adatkezelő közötti szerződés megkötése vagy teljesítése érdekében szükséges;*
b) *meghozatalát az adatkezelőre alkalmazandó olyan uniós vagy tagállami jog teszi lehetővé, amely az érintett jogainak és szabadságainak, valamint jogos érdekeinek védelmét szolgáló megfelelő intézkedéseket is megállapít; vagy*
c) *az érintett kifejezett hozzájárulásán alapul.”*

Az első kivétel tehát olyan szerződés, amelynek alapján a szerződéses jogviszonyban az adatkezelő alkalmazhatja az automatizált döntéshozatali eljárást, de csak is a szerződéssel összefüggő célokra, melyeket a GDPR értelmében igazoltan be is kell tudnia mutatni.

A második kivétel mibenlétét a GDPR (71) preambulumbekezdése is megvilágítja, mely ilyen intézkedésként azonosítja a csalás és adóelkerülés megelőzése érdekében történő, jogszabályon alapuló automatizált döntéshozatalt.

A harmadik kivétel esetében az érintett kifejezett hozzájárulása a feltétel. Bár a szóban megtett hozzájárulás is kifejezett hozzájárulásnak tekinthető, mivel azonban az adatkezelőnek később is bizonyítani szükséges a kifejezett hozzájárulás meglétét, ezért célszerűbb az érintett hozzájárulását írásban kérni vagy más módon pl. hangrögzítő eszköz használatával rögzíteni. A hozzájárulás esetében azonban megjegyzendő, hogy az bármikor visszavonható, és ilyen esetben az adatkezelés – hacsak nincsen egy másik jogalap, amire át lehetne térni és az adatkezelést annak megfelelően folytatni – jogellenessé válik.

Az érintett hozzáférési jogáról szóló 15. cikk (1) bekezdés h) pontja a 22. cikk vonatkozásában a fentiek mellett előírja az adatkezelőnek, hogy az érintetett tájékoztassa az automatizált döntéshozatal tényéről, az ott alkalmazott logikáról, valamint arról, hogy az ilyen adatkezelés milyen jelentőséggel, illetve milyen várható következményekkel jár az érintettre nézve.

Az első kötelezettség viszonylag könnyen teljesíthető, hiszen az általános adatkezelési tájékoztató keretében csupán többletinformáció lesz az automatizált döntéshozatal tényéről szóló tájékoztatás.

Nehezebben kivitelezhető viszont az a kitétel, miszerint az érintettet az adatkezelés logikájáról is tájékoztatni kell. Az előző fejezetben már kitértem rá, hogy egy neurális hálózat működési mechanizmusának részletei a fekete dobozban zajlanak, azt teljes egészében átlátni, elmagyarázni egy laikusnak szinte lehetetlen. Érdemi információ adható viszont oly módon is, ahogyan azt Eszteri Dániel tanulmányában egy brit kutatás alapján bemutatja[12]: jó gyakorlat lehet például, ha az érintettnek nem a működés pontos mechanizmusát mutatják be, hanem egy tesztrendszeren az érintettek maguk próbálhatják ki – akár fiktív adatokkal is – hogy a megadott adatok módosítása hogyan módosítja az automatizált döntéshozatal eredményeképp megállapított eredményt. Ugyancsak hasonlóan lehet bemutatni a harmadik kötelezettséget, vagyis az ilyen jellegű adatkezelés érintettre gyakorolt jelentőségét és várható következményeit.

A 22. cikk kitér arra is, hogy automatizált döntéshozatal esetében az adatkezelőnek biztosítania kell annak lehetőségét, hogy az érintett emberi beavatkozást kérhessen az őt érintő egyedi döntéshozatallal kapcsolatban. A WP29 iránymutatása kiemeli, hogy az emberi beavatkozást olyan személynek kell végeznie, aki képes és jogosult is arra, hogy az automatizált eljárás keretében meghozott döntést megváltoztathassa.[13] Az eljárást úgy kell feltételezhetően elképzelni, hogy amennyiben az érintett kifogást emel az automatizált döntéshozatal eredményével kapcsolatban, a döntés felülvizsgálatával megbízott személy megvizsgálja a betáplált adatokat, a meghozott döntést, illetve a kifogásolt eredményt, és megvizsgálja azt, hogy vajon a felülvizsgálandó kérdésben ugyanez az eredmény született volna-e akkor is, ha a döntést nem a mesterséges intelligencia, hanem ember hozza meg.

3.3. A profilalkotás

A gépi tanulási modelleket gyakran alkalmazzák arra, hogy figyeljék meg és elemezzék bizonyos felhasználók viselkedését (például a közösségi médiában milyen tartalmaknál időzik hosszabban, mire keres rá), majd ezekből az adatokból profilt alkossanak (például célzott reklámok felhasználóhoz történő eljuttatása céljából.) Fennáll viszont a veszélye

[12] Eszteri Dániel: A gépek adatalapú tanításának megfeleltetése a GDPR egyes előírásainak. In: Török Bernát – Ződi Zsolt (szerk.): A mesterséges intelligencia szabályozási kihívásai. Ludovika Egyetemi Kiadó. Budapest. 2021. 204-206. o.

[13] Iránymutatás az automatizált döntéshozatallal és a profilalkotással kapcsolatban 2016/679 rendelet alkalmazásához
https://www.naih.hu/files/wp251rev01_hu.pdf 29. oldal (2024.03.25.)

annak, hogy egy-egy profil olyan „jól sikerül”, hogy pontos adatokat mutat a felhasználó személyes jellemzőiről, személyiségjegyeiről, így a felhasználó akár beazonosíthatóvá is válhat.[14]

A GDPR 22. cikke a „beleértve”, illetve „ideértve” szavak használatával kiterjeszti a fentebb (3.2. pontban) részletezett szabályozást a profilalkotásra is.

Amiért mégis külön részben tárgyalom a profilalkotást, annak az az oka, hogy az automatizált döntéshozataltól eltérően a profilalkotás vonatkozásában a GDPR 4. cikkjének 4. pontja pontosan meghatározza a fogalmat:

„profilalkotás”: személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják;

A fogalommeghatározás teljes mértékben összecseng az előzőekben leírt példával. Vagyis természetes személyek bizonyos jellemzői lesznek azok az adatok (például bejegyzések, tartalmak a közösségi médiában, amelyek olvasásával, nézésével hosszabb időt tölt el a felhasználó, vagy amelyekre célzottan rákeres), melyet az adatok automatizált kezelése során (gépi tanulási modellek) meghatározott jellemzők (például preferenciák megállapítására vagy vásárlás ösztönzésére) használnak.

Nagyon is van tehát létjogosultsága annak, hogy profilalkotás során kezelt adatok vonatkozásában is ugyanolyan kötelezettségek terheljék az adatkezelőt (és ugyanolyan jogokkal rendelkezzen az érintett), mint az automatizált döntéshozatal esetén.

3.4. Beépített adatvédelem

Ugyancsak érdekes kérdés lehet az adatvédelem és a mesterséges intelligencia kapcsolatában az úgynevezett beépített adatvédelem (privacy by design). A fogalom nem

[14] Péterfalvi Attila – Révész Balázs – Buzás Péter (szerk): Magyarázat a GDPR-ról. Wolters Kluwer. Budapest. 2018. 198. o.

új keletű, hiszen több mint harminc évvel ezelőtt találta ki Ann Cavoukian kanadai adatvédelmi biztos, és annyira elterjedt a gyakorlatban, hogy a GDPR-ba is beépítették.[15]

Miről is van itt szó? A privacy by design lényege az, hogy a fejlesztők termékeik fejlesztése során a személyes adatok védelmét garantáló biztosítékokat a fejlesztési folyamatban minden további lépést megelőzően építsék be, illetve, hogy a felhasználók személyes adatainak védelmére ne mint kötelezettségre, hanem mint integrált célkitűzésre tekintsenek. Véleményem szerint ez a jelen dolgozat bevezetésében bemutatott három réteg közül a második (belső szabályok, melyek a jog hézagait kitöltik és a jogszabályokat a saját belső rendszerükre implementálják), sőt átnyúlik a harmadik rétegre, az erkölcs, etika és morál területére is.

Ann Cavoukian hét fő alapelvet határozott meg a beépített adatvédelem célkitűzései között:

I. „*Az adatvédelem legyen proaktív, nem reaktív; legyen megelőző, nem javító*.” – vagyis az adatvédelem célja az esetlegesen kialakuló vészhelyzetek megelőzése, és nem az, hogy utólag orvosolni tudjuk az adatvédelmi incidenseket.
II. „*Az adatvédelem mint alapbeállítás*” – a rendszereket úgy kell létrehozni és működtetni, hogy az érintettnek ne kelljen semmit tennie annak érdekében, hogy adatai védettek legyenek, ennek automatikusnak kell lennie.
III. „*Tervbe ágyazott adatvédelem*” – az informatikai struktúrákat és az eljárásokat, gyakorlatokat úgy kell kialakítani, hogy az adatvédelem már a tervezés során és utána végig elsőbbséget élvezzen, alap legyen.
IV. „*Pozitív, nem negatív végösszeg*” – mindkét fél jogos érdekeinek kielégítése a cél, vagyis a rendszert úgy kell felépíteni és működtetni, hogy abból a felhasználó és a szolgáltató is profitálhasson.
V. „*Élethosszig tartó védelem*” – az adatvédelemnek már az előtt be kell épülnie a rendszerbe, még mielőtt oda bármilyen külső információ

[15] Deli, Kocsis és Muhari tanulmányukban egy egész fejezetet szentelnek a témának, amelyet itt összefoglalóan idézek
Deli Gergely – Kocsis Réka – Muhari Nóra: Akarva-akaratlanul – az adatvédelem és az akaratszabadság dilemmái. In: Török Bernát – Ződi Zsolt (szerk.): A mesterséges intelligencia szabályozási kihívásai. Ludovika Egyetemi Kiadó. Budapest. 2021. 234-237. o.

(például személyes adat) bekerülne, így garantálni lehet azt, hogy adatvédelem az első pillanattól kezdve működik.

VI. „*Láthatóság és átláthatóság*” – minden gyakorlati és technológiai folyamat megfigyelhető és érthető úgy a felhasználó, mint a szolgáltató számára.

VII. „*Felhasználó-központúság*” – a rendszereket úgy kell megtervezni és működtetni, hogy a felhasználó biztos lehessen benne, hogy az alapértelmezett adatvédelem működik, és erről őt megfelelő információkkal, értesítésekkel látják el, illetve az egész rendszer felhasználóbarát alternatívákat kínál számára.

Bár ezek az elvek az általános adatvédelmi rendeletbe beépültek, de a gyakorlat azt mutatja, hogy a GDPR nem fejti ki részletesen, csak utal rá, hogy bizonyos esetekben az adatkezelőnek „megfelelő” intézkedéseket kell hoznia. A részletszabályok kidolgozását a nemzeti szabályozásra, így például az adatvédelmi hatóság vagy a bíróság gyakorlatára, esetlegesen pedig az adatkezelő belső szabályzataira bízza.

Így viszont előfordulhat, hogy egy adatkezelő gyakorlata a természetes személyek adatainak kezelése tekintetében a GDPR-nak látszólag megfelelő, de egy-egy adatvédelmi incidens megmutatja, hogy a belső szabályzatok nem megfelelő kidolgozottsága miatt mégis „rés van a pajzson”. A complience ebben viszont nagy segítséget tud nyújtani, hiszen feladatai közé éppen az ilyen „rések” kiszűrése és megfelelő orvoslása tartozik.

4. A MESTERSÉGES INTELLIGENCIA SZABÁLYOZÁSA AZ ADATVÉDELEM VONATKOZÁSÁBAN (AI ACT)

4.1. A mesterséges intelligencia szabályozásának kihívásai

A mesterséges intelligencia jogi szabályozása „gyerekcipőben" jár, melynek azon túl, hogy a felgyorsult technológiai újítások miatt a szabályozás képtelen lekövetni a fejlődés ütemét, sok egyéb magyarázata is van.

Mert milyen kihívásokkal is kell szembenéznie a jogalkotónak? A digitalizáció időszakában az adatok már nem csak kimondott vagy leírt szöveg formájában jelennek meg, hanem képek, zenék, filmek, sőt a laikusok számára felfoghatatlan adathalmazok és kódok is idetartoznak. Ez viszont azt jelenti, hogy a szabályozást úgy kell kidolgozni, hogy hatása minden területen érvényesülni tudjon.

A digitalizált tartalmakat a felgyorsult világ érzete ellenére – paradox módon – az állandóság jellemzi, hiszen ezek az adatok nyomot hagynak maguk után. Ha ma rólam megjelenik egy újságcikk az online médiában, én hiába tiltom le holnap és kérem a törlését, addigra azt már sokan megoszthatták, hivatkozhattak rá, lementhették, a rendszerek naplózhatták. Ennek nyomonkövetése szinte lehetetlen.[16]

Az adatok emellett nagyon könnyen másolhatók, továbbíthatók és így ellophatók. A Békéscsabán 2024. április 17-én rendezett *A technológiai lehetőségei, az EMBER az új világban* című konferencián[17] az egyik előadásnak éppen ez volt az egyik témája: hogyan lehet védekezni a fejlesztések esetén az adatlopások ellen? A példa nagyon szemléletes volt: az önvezető autónak meg kell tanulnia felismerni a stop táblát minden körülmények között, hogy meg tudjon állni, ha érzékel egyet. A tanítási folyamat idő- és energia- (és így pénz)igényes, és könnyen eltulajdonítható, ha a kész modell már rendelkezésre áll. De hogyan követhető vissza egy adathalmaz esetén, hogy valamit én fejlesztettem ki? Digitális ujjlenyomatokat kell elhelyezni! Ebben az esetben ilyen eldugott digitális ujjlenyomat lehet az, ha az önvezető autó egy adott macska egy bizonyos fényképére ugyanúgy reagál, mint a stop táblára (mert a sok millió egyéb adat mellett ezt is

[16] Rab Árpád Szörény: A mesterséges intelligencia hatása a társadalomra – problématérkép. In: Török Bernát – Ződi Zsolt (szerk.): A mesterséges intelligencia szabályozási kihívásai. Ludovika Egyetemi Kiadó. Budapest. 2021. 28-29. o.

[17] https://www.beol.hu/helyi-kozelet/2024/04/digitalizacio-mesterseges-intelligencia-konferencia#google_vignette (2024.04.19.)

megtanítottam neki.) Ha kétség merül fel, hogy vajon az adott rendszert ki fejlesztette, be tudom bizonyítani, hogy én voltam, hiszen csak én ismerem ezt sok-sok adat között megbúvó kakukktojást, digitális ujjlenyomatot. Ez természetesen viszont egy olyan belső szabályozási mechanizmus, ami nem húzható rá általánosságban mindenre.

További nehézséget jelent az, hogy a generatív MI-k esetében, különösen a gépi tanulás és még inkább a mélytanulás területén olykor megjósolhatatlan eredmények születnek. Mit szabályozzunk hát? Hiszen hiába adunk meg szabályokat a betáplálandó adatokra, az inputra vonatkozóan, ha előre nem láthatjuk azt, hogy mi lesz az output, azaz az MI milyen eredményre jut. (Hiszen itt már nem lineáris programozásról van szó.) De ugyanígy nehézséget okozhat az, ha az outputot kívánjuk szabályozni, hiszen a helyzet itt sincs másként: az MI eredménye előre megjósolhatatlan, még megfelelő promptok esetén is.

Fontos kérdés lehet a szabályozás során az is, hogy mikor kerüljön sor rá, hiszen ami ma talán még megfelel a technológia jelenlegi állásának, az holnapra már elavulttá válhat.

Legyen-e éppen ezért átfogó szabályozás vagy szektoronként külön-külön hozzunk szabályokat?

Dilemma az is, hogy vajon a túlszabályozás nem fogja-e vissza a technológia fejlődését? Szemléletes példa erre az, hogy az USÁ-ban és talán Kínában még kevésbé szabályozott a mesterséges intelligencia felhasználása, így annak használata szárnyal is. Az Európai Unióban viszont – ahogy azt majd látni fogjuk – már egy ideje törekvések vannak a komplexebb szabályozás kidolgozására, és e mellett egyéb, már hatályos jogszabályok, például a GDPR is tartalmaz olyan részletszabályokat, amelyek hatással vannak az MI felhasználására, és amelyek ily módon gátat is szabnak a túlzott szabadságnak, és így adott esetben a fejlesztéseknek is.

Milyen alanyi hatályban gondolkodjunk, ha szabályozni szeretnénk a területet? Tartozzanak alá a konkrét technológia fejlesztői, vagy azok a cégek, amelyek ezeket megrendelik és/vagy használják? Esetleg legyenek szabályok arra is, hogy milyen magatartást tanúsítsanak azok, akiknek érdekében az adott technológia működik?

Vagy ne is akarjunk jogszabályi szinten fellépni? Adjunk meg egy irányvonalat, a részletszabályokat pedig bízzuk a cégek önszabályozására? Hiszen egy-egy cég reputációját nagyban csökkentheti vagy növelheti, ha működésébe és termékeibe olyan

védelmi vonalakat épít be, melyek ügyfeleik érdekeit képesek hatékonyan védeni. Ez pedig anyagi haszon formájában is jelentkezni fog.

Meg kell tehát találni azt a szabályozási optimumot, amely a felhasználók biztonságát és érdekeit védi, de ugyanakkor nem gátolja az új technológiák nyújtotta előnyök felhasználásának lehetőségeit a felhasználók részéről, ennek gazdasági vetületének kiaknázását a cégek részéről, és nem fogja vissza az innovációt sem.[18]

Végezetül pedig itt idézném Klein Tamás szavait:

„A jogi szabályozásnak és az etikai normáknak egyetlen végső értékre, az emberi méltóság abszolút és korlátozhatatlan (alkotmányos) alapértékére kell épülniük. […] Ezeknek az alapértékeknek az érvényesítése minden jogalkotási aktus és emberi magatartás végső igazodási pontja kell, hogy legyen. Igaz ez a mesterséges intelligencián alapuló technológiák fejlesztésére és alkalmazására vonatkozó emberi tevékenységre csakúgy, mint az azokra vonatkozó szabályok tartalmára. A mesterséges intelligencia fejlesztése és használata tehát nem (lehet) önmagában való cél, hanem kizárólag az egyetemes emberi értékek, alapjogok érvényesülését és kiteljesítését szolgáló technológiai eszközként kell tekinteni rá és ebben a szellemben szükséges szabályozni.” [19]

4.2. A mesterséges intelligencia szabályozásának története az EU-ban és Magyarországon

Az Európai Bizottság 2018-tól kezdve folyamatosan napirenden tartja és kezdetben közlemények formájában, majd a mesterséges intelligenciáról szóló Fehér Könyv formájában igyekezett irányt mutatni ezen a területen.

A Bizottság által kiadott közlemények a következők voltak:

- Mesterséges intelligencia Európa számára COM (2018) 237 final/2 (2018. június 26.)[20]

[18] G. Karácsony Gergely: Innovatív jogalkotói megoldások a mesterségesintelligencia-alapú rendszerek szabályozására. In: Török Bernát – Ződi Zsolt (szerk.): A mesterséges intelligencia szabályozási kihívásai. Ludovika Egyetemi Kiadó. Budapest. 2021. 159-167. o.
[19] Klein Tamás: Robotjog vagy emberjog. Az emberközpontú mesterséges intelligencia szabályozásának kiindulási pontjai. In: Török Bernát – Ződi Zsolt (szerk.): A mesterséges intelligencia szabályozási kihívásai. Ludovika Egyetemi Kiadó. Budapest. 2021. 112. o.
[20] https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52018DC0237R(01) (2024.04.04.)

- A mesterséges intelligenciáról szóló összehangolt terv COM (2018) 795 final (2018. december 7.)[21]
- Az emberközpontú mesterséges intelligencia iránti bizalom növelése COM (2019) 168 final(2019. április 8.) [22]

Végezetül pedig az ugyancsak a Bizottság által kiadott Fehér könyv:

- Fehér könyv a mesterséges intelligenciáról: a kiválóság és a bizalom európai megközelítése COM(2020) 65 final (2020. február 19.)[23]

Sajnos jelen dolgozat keretei között ezen dokumentumok elemzésére nincsen lehetőség, annyit azonban különösen a Fehér könyv vonatkozásában megjegyeznék, hogy a mesterséges intelligencia fejlesztésével, használatával és szabályozásával kapcsolatban központi törekvésként jelenik meg az alapjogok – így többek között a személyes adatok – védelme. Ennek kapcsán a különböző – MI-használattal potenciálisan együtt járó – kockázatok beazonosításkor a Bizottság felhívja a figyelmet arra, hogy előfordulhatnak olyan helyzetek, amikor az MI-t a munkáltatók, de akár állami szervek vagy egyéb hatóságok is (!) tömeges megfigyelésre használhatják, annak ellenére, hogy ez sérti az uniós adatvédelmi jogszabályt. E mellett kockázatként azonosítja a Bizottság azt is, hogy a nagy adatmennyiségek, illetve az adatok közötti összefüggések elemzésekor előfordulhat az, hogy természetes személyek adatai visszakereshetővé válnak és/vagy elveszítik anonim jellegüket, ezért a természetes személyek – akaratuk ellenére – beazonosíthatóvá válnak.[24]

Az Európai Unió szabályozásában ezt követte az Európai Parlament által 2024. március 13-án elfogadott úgynevezett AI ACT, melyről részletesebben a 4.3. fejezetben ejtek szót.

De mi a helyzet a hazai szabályozással?

Egyelőre kézzel fogható dokumentumként *Magyarország Mesterséges Intelligencia Startégiája 2020-2030* áll rendelkezésünkre, melyben megismerkedhetünk a kitűzött célokkal, de a jogi szabályozás tekintetében elég visszafogottan és általánosan fogalmaz,

[21] https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52018DC0795 (2024.04.04.)
[22] https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52019DC0168&from=FR (2024.04.04.)
[23] https://commission.europa.eu/system/files/2020-03/commission-white-paper-artificial-intelligence-feb2020_hu.pdf (2024.04.04.)
[24] Fehér könyv 13-14. o. https://commission.europa.eu/system/files/2020-03/commission-white-paper-artificial-intelligence-feb2020_hu.pdf

amikor célként a következőket azonosítja: „*Az MI működéséhez szükséges hatékony és támogató hazai szabályozási környezet megteremtése és etikai keretrendszer kialakítása, figyelemmel az EU jogi kereteire.”*[25]

4.3. Az Európai Unió mesterséges intelligenciáról szóló jogszabálya (AI ACT)

Mérföldkőnek számít az a tény, hogy az Európai Unió – elsőként a világon – konkrét kereteket dolgozott ki a mesterséges intelligencia szabályozására. A hosszú folyamat eredményeként létrejött jogszabály célja – a Bizottság honlapján kiadott közlemény szerint[26] – az, hogy az MI-rendszerek kockázatait hatékonyan beazonosítani és ezáltal kezelni lehessen, és így a mesterséges intelligencia fejlesztői és azt felhasználó vállalkozások részére egyértelmű követelményeket és kötelezettségeket írjon elő az egyes felhasználási módok tekintetében. Végső soron a cél a polgárok alapvető jogainak és biztonságának védelme, az etikai elvek betartása, de emellett további törekvés a vállalkozások, különösen a kis- és középvállalkozások adminisztratív és pénzügyi terheinek csökkentése, illetve Európa arra való ösztönzése, hogy ezen a területen irányt mutasson és globális vezető szerepet töltsön be.

A mesterséges intelligenciáról szóló jogszabály a megbízható mesterséges intelligencia fejlesztését támogató, szélesebb körű szakpolitikai intézkedéscsomag részét képezi, amely magában foglalja a mesterséges intelligenciával kapcsolatos innovációs csomagot és a mesterséges intelligenciára vonatkozó összehangolt tervet is.

A mesterséges intelligenciáról szóló törvény várhatóan májusban vagy júniusban válik hivatalosan is jogszabállyá, 20 nappal azután, hogy az Unió hivatalos lapjában a rendelet szövege megjelent. A rendelkezések ezután fokozatosan lépnek majd hatályba, így például az általános célú mesterséges intelligencia-rendszerekre, például a chatbotokra vonatkozó szabályokat a jogszabály hatályba lépése után egy évvel kezdik majd el alkalmazni. A teljes szabályrendszer előreláthatóan 2026 közepére lesz teljes körűen hatályos.

Általánosságban elmondható, hogy a jogszabály alapját a kockázatalapú megközelítés jellemzi:

[25] https://digitalisjoletprogram.hu/files/2f/32/2f32f239878a4559b6541e46277d6e88.pdf 34.o.
[26] https://digital-strategy.ec.europa.eu/hu/policies/regulatory-framework-ai

- A minimális vagy semmilyen kockázattal (*minimal risk*) sem járó MI-rendszerek továbbra is szabadon használhatóak lesznek, ilyenek például a mesterséges intelligencia alapú spamszűrők.
- A korlátozott kockázat (*limited risk*) jelen esetben azt jelenti majd, hogy az MI-rendszer átláthatóságát garantálni kell. Ennek biztosítása érdekében konkrét átláthatósági követelményeket ír elő a jogszabály, ilyen például a tájékoztatási kötelezettség. Chatbotok (pl. egy virtuális asszisztens) alkalmazásakor például kifejezetten közölni kell a rendszerrel kapcsolatba lépő személlyel, hogy egy géppel fog párbeszédet folytatni és meg kell adni minden olyan információt, amelyre tekintettel a felhasználó eldöntheti, hogy folytatni kívánja-e az interakciót vagy inkább befejezi azt. A deep fake[27] tartalmakat is jól érzékelhető módon jelölni kell.
- A nagy kockázatú (*high risk*) besorolást kapó MI-rendszerek közé azokat a mesterséges intelligencia által segített vagy vezérelt tevékenységeket kategorizálták be, melyek működésük során jelentősen befolyásolhatják a felhasználók életkörülményeit, esélyeit, egészségét (automatizált hitelképességbírálat, vízumkérelmek automatizált vizsgálata, vizsgák letétele automatizált rendszeren belül, MI-támogatott sebészet, MI-vezérelt közlekedés, stb.). Az ilyen rendszerek bevezetése és használata szigorú feltételekhez kötött és a rendszer működtetőjét folyamatos kötelezettségek terhelik, melyek megsértése adott esetben súlyos bírságok kiszabásához is vezethet.
- A mesterséges intelligencia egyes felhasználási módjai tilalmazottak lesznek, mert elfogadhatatlan kockázatot (*unacceptable risk*) hordoznak magukban, mint például az emberek viselkedését szabályozó szociális pontozási rendszerek, a prediktív rendőri ellenőrzés egyes típusai és az iskolai és munkahelyi érzelemfelismerő rendszerek. További tiltott felhasználási módok közé tartozik a rendőrség által a nyilvánosság előtt végzett arcszkennelés a mesterséges intelligenciával működő távoli „biometrikus azonosítási” rendszerek segítségével

[27] A mély tanulás (deep learning) és a kamu (fake) összevonása. Olyan digitális hamisítási technológia, amellyel a valódihoz a megtévesztésig hasonlító multimédiás tartalmakat (képeket, hangokat, videókat) lehet előállítani.

(pl. az arcfelismerő és –azonosító kamerarendszerek), kivéve az olyan súlyos bűncselekmények esetében, mint az emberrablás vagy a terrorizmus.[28]

4.4. Az AI ACT és adatvédelem

Mivel dolgozatom témája az adatvédelem és a mesterséges intelligencia kapcsolata, ezért az AI ACT-ból igyekeztem a kifejezetten adatvédelemmel kapcsolatos szabályozásokat kiemelni.

Több helyen is említi a jogszabály magát az adatvédelmet mint védendő alapjogot, de kifejezetten magával az adatvédelemmel a 69. preambulumbekezdés foglalkozik.

A bekezdés első részében megjelenik az Ann Cavoukian által leírt, a gyakorlatban elterjedt, illetve a GDPR-ba is integrált beépített adatvédelem elve, melyet a jogszabály szövege nem csak szó szerint kiemel, de hangsúlyozza annak fontosságát is, hogy az adatvédelemhez (és az ezzel összefüggő magánélet tiszteletben tartásához) való jogot az MI-rendszer fejlesztésének első lépésétől kezdve, illetve annak használata során végig, azaz teljes életciklusa során garantálni kell.

Külön felhívja a figyelmet az adattakarékosság elvére is, melynek vonatkozásában – illetve az adatvédelem, valamint az adatkezelés szabályozása szükségességének említésekor mindig – kiemeli, hogy az uniós adatvédelmi jogszabályokban meghatározottak szerint kell eljárni. A releváns jogszabályok felsorolását 10. preambulumbekezdés tartalmazza, mely az alábbi jogszabályokat nevesíti:

- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet)
- Az Európai Parlament és a Tanács (EU) 2018/1725 rendelete (2018. október 23.) a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről

[28] https://nki.gov.hu/it-biztonsag/hirek/az-eu-elfogadta-a-mesterseges-intelligenciarol-szolo-torvenyt/ (2024.04.10.)

- Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27.) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről
- Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (Elektronikus hírközlési adatvédelmi irányelv)

A 10. preambulumbekezdés azonban nem csak felsorolja a fenti jogszabályokat, de deklarálja azok függetlenségét is, amikor kimondja, hogy az AI ACT maga semmilyen módon nem kívánja befolyásolni az adatvédelmi rendelkezéseket, és tiszteletben tartja az azok betartásának ellenőrzését végző független felügyeleti hatóságok feladat- és hatásköreit is.

Az érintettekről is szót ejt, és továbbra is garantálja személyes adataik védelmét és az ezzel kapcsolatos jogaik gyakorlását, külön is hangsúlyozva ezt a GDPR és az AI ACT határmezsgyéjén található egyedi ügyekben történő, kizárólag automatizált döntéshozatal és a profilalkotás során történő adatkezelés vonatkozásában. Ezen túlmenően a 10. preambulumbekezdés deklarálja azt, hogy az AI ACT feladata ezen jogok gyakorlásának és a jogorvoslati lehetőségek megkönnyítése is.

Kiemeli azt is, hogy az MI-rendszerek fejlesztőinek és szolgáltatóinak, amennyiben a fenti jogszabályok hatálya alá tartozó adatkezelőnek vagy adatfeldolgozónak minősülnek, továbbra is meg kell felelniük az ilyen minőségben rájuk vonatkozó előírásoknak és kötelezettségeknek.

A kifejezetten az adatvédelemmel kapcsolatos 69. preambulumbekezdés a szolgáltatók vonatkozásában kifejezett kötelezettségként írja elő az anonimizálás[29] és a titkosítás[30]

[29] Az *anonimizálás* az adatok olyan átalakítása, aminek eredményeképpen a korábban valakihez kapcsolható adatok már nem lesznek hozzá kapcsolhatóak. A GDPR alapján az anonimizált adatok már nem számítanak személyes adatnak, így a kezelésük során nem kell a személyes adatok kezelését szabályozó szigorú törvényeknek megfelelni. https://lexiq.hu/anonimizalas (2024.04.12.)

[30] A titkosítás a kriptográfiának az a része, mely a nyílt szöveget, azaz információt egy valamilyen titkosítási eljárás algoritmus segítségével ember számára értelmezhetetlen karaktersorozattá (titkosított szöveggé) alakítja. Csak a megfelelő kulcs birtokában vagyunk képesek a titkosított szöveget újra olvashatóvá tenni. A titkosítás ugyan meg tudja védeni az üzenet bizalmasságát, de más technológiákra is szükség van, hogy

mellett „*az olyan technológia használatát is, amely lehetővé teszi az algoritmusok adatokhoz rendelését és az MI-rendszer anélkül történő tanítását, hogy a nyers vagy strukturált adatokat a feleknek egymás között át kellene adniuk vagy másolniuk, az e rendeletben foglalt adatkormányzási követelmények sérelme nélkül.”*

De mi is az adatkormányzás? Erre a 27. preambulumbekezdésben találjuk a választ, mely leírja, hogy az adatkormányzás egyike annak a hét, nem kötelező erejű etikai alapelvnek, melyeket a Bizottság által kinevezett független magas szintű MI-szakértői csoport dolgozott ki, és amelyek célja, hogy segítsék biztosítani a mesterséges intelligencia megbízhatóságát és etikai megalapozottságát.

Az ebben leírtak alapján a *„magánélet védelme és az adatkormányzás azt jelenti, hogy az MI-rendszereket a magánélet védelmére vonatkozó és az adatvédelmi szabályokkal összhangban kell fejleszteni és használni, miközben az adatok kezelésének magas szintű minőségi és integritási standardoknak kell megfelelnie.”*

Az adatkormányzás megjelenik a nagy kockázatú MI-rendszerekre vonatkozó követelmények között is, a rendelet 10. cikkében. Itt előírásként fogalmazódik meg az, hogy az ilyen rendszerek fejlesztése során olyan tanító-, validálási és tesztadatkészleteket kell használni, amelyek megfelelnek – többek között – az adatkormányzás elvének is.

Már ezek alapján is elmondható tehát, hogy a fent kiemelt preambulumbekezdésekben foglaltak megjelennek az AI ACT adatkezelésre vonatkozó szabályaiban, melyeket a preambulumbekezdések szellemében kell értelmezni és használni.

Jelen dolgozat keretei közé az adatvédelem és a mesterséges intelligencia kapcsolatának vonatkozásában ennyi fért, de az AI ACT forradalmi megjelenése a mesterséges intelligencia szabályozása területén annyira új még, és annyi magyarázatot, elemzést és az összefüggések értelmező megvilágítását igényli, hogy biztos vagyok benne, hogy ezzel kapcsolatban a közeljövőben még számos tanulmányt és cikket olvashatunk. Ugyanakkor remélem, hogy saját elemzésemmel is némi betekintést tudtam adni ebbe az izgalmas és nagyon időszerű témába.

garantálni tudjuk az üzenet sérthetetlenségét és hitelességét. https://kurt.hu/2022/07/05/titkositas-az-elmeletben-es-a-gyakorlatban/ 2024.04.12.)

5. OKOS VÁROSOK AZ ADATVÉDELEM ÉS A MESTERSÉGES INTELLIGENCIA TÜKRÉBEN

5.1.Az Okos Városokról általában

A már jelen dolgozat bevezető részében is említett Okos Város (Smart City) egy olyan közigazgatási területet takar, ahol fejlett információs és kommunikációs technológiákat (IKT) alkalmaznak a városi infrastruktúra és szolgáltatások hatékonyságának és fenntarthatóságának javítása érdekében. Ezek a technológiák – MI-rendszerek – valós idejű adatokat gyűjtenek és elemeznek a település különböző területeiről a közlekedéssel, az energia-, víz- és hulladékgazdálkodással, a levegő szennyezettségével, az épületek üzemeltetésével, a közvilágítással, vagy a közbiztonsággal kapcsolatban.

Egy jól kitalált és megvalósított Okos Város koncepcióból mindenki profitál: a lakosság élvezheti az optimálisan működő tömegközlekedést, a javuló közbiztonságot, az egyre jobb levegő- és vízminőséget. A vállalkozások számára az Okos Városok új üzleti lehetőségeket, hatékonyabb működést és jobb ügyfélelérést kínálnak. A település vezetői, döntéshozói részére az Okos Városok segíthetnek a költségek csökkentésében, a szolgáltatások javításában és a fenntarthatósági célok elérésében.

Szeretnék néhány konkrét példát is bemutatni szerte a világból:

- Amsterdam Smart City: Amsterdam városa számos okos technológiát alkalmaz, például okos lámpákat az optimális közvilágítás érdekében, vagy olyan okos parkolási rendszert, amely segít megfelelően egyensúlyba hozni a parkolóhelyek zsúfoltságát, illetve kihasználtságát.[31]
- Barcelona Smart City: Barcelona városa a városi telekommunikációs és közlekedési infrastruktúra fejlesztésére összpontosított. Az optikai kábelek behálózzák a várost, melynek köszönhetően számos ponton, így a különböző közlekedési eszközökön is elérhető a szabadon hozzáférhető wifi, illetve az okos (tömeg)közlekedési rendszerek mellett MI-rendszerek által vezérelt energiahatékony épületekkel és optimálisan kialakított zöld területekkel találkozhatunk itt, melyek a városlakók és a turisták komfortérzetét is pozitívan befolyásolják.[32]

[31] https://amsterdamsmartcity.com/ (2024.04.15.)
[32] https://blog.bismart.com/en/why-barcelona-is-a-smart-city (2024.04.15.)

- Seoul Smart City: Dél-Korea fővárosában a már-már szokásosnak mondható szenzorokkal és kamerákkal történő adatfelvételen, ezen adatok MI alapú elemzésén és a kapott eredmények társadalmi, gazdasági és környezetvédelmi előnyökre történő lefordításán túl létrehozták a „Metaverse Seoul" elnevezésű platformot, mely a város egy részének virtuális 3D leképezése, ahová a látogatók virtuálisan avatarként léphetnek be és élvezhetik a városlátogatás előnyeit, ügyeket intézhetnek, de a platform pl. arra is alkalmas, hogy vészhelyzetek modellezésével a részvevőket felkészítsék arra, hogy hogyan viselkedjenek egy-egy hasonló helyzetben a való világban.[33]

A kiragadott példák csak nagyon szűk betekintést kínálnak a Smart City programok által kínált lehetőségekbe, melyeknek, mint látjuk, ma már a képzelet sem szabhat határt.

De természetesen az éremnek itt is két oldala van, és az Okos Város MI-rendszerei itt is nagyfokú sebezhetőséget mutatnak és megannyi kihívással küzdenek, melyek közül jelen dolgozat szempontjából a két legjelentősebb a kiberbiztonság és az adatvédelem. Az Okos Városok komplex hálózatokból állnak, amelyek számos csatlakozási pontot és adatforrást kínálnak a kiberbűnözők számára. A kiberbiztonsági kockázatok kezelése kulcsfontosságú az Okos Városok infrastruktúrájának és adatainak védelme érdekében. Az adatvédelem területén pedig az adhat aggályra okot, hogy az Okos Városok nagy mennyiségű személyes adatot gyűjtenek és tárolnak a lakosságról, melyek vonatkozásában különösen fontos, hogy szigorú adatvédelmi intézkedéseket hozzanak a gyűjtött adatok védelme és a lakosok adatvédelmi jogainak tiszteletben tartása érdekében. Látjuk majd, hogy ez nem mindig sikerül.

5.2. Adatvédelmi kockázatok kezelése az Okos Városokban

Az adatvédelmi kockázatok beazonosítása és kezelése során a rendszerek fejlesztői és üzemeltetői egyrészt kötve vannak a rájuk vonatkozó jogszabályokhoz, másrészt ezen jogszabályokból kiindulva minden fejlesztő és üzemeltető saját rendszerébe specifikusabb szabályozásokat építhet be.

[33] https://english.seoul.go.kr/policy/smart-city/ (2024.04.15.)

De vajon mire kell különösen figyelemmel lenni? A következőkben néhány olyan területet mutatok be, ami megkerülhetetlen az Okos Városok esetében az adatvédelem vonatkozásában.

Az első két ilyen vezérlő elv az adatminimalizálás és a célhoz kötöttség elve. Ez azt jelenti, hogy csak olyan mennyiségű adatot szabad gyűjteni, amennyi az előre meghatározott cél eléréséhez feltétlenül szükséges. Éppen ezért nagyon fontos, hogy már a koncepció tervezesének időszakában, még mielőtt a rendszerbe egyáltalán adatokat táplálnánk, pontosan meg tudjuk határozni azt a specifikus célt, amire az összegyűjtött adatokat fel szeretnénk használni. Ha megvan a cél, akkor ki kell dolgoznunk a legoptimálisabb adatgyűjtési stratégiákat is, és biztosítanunk kell ennek hatékony és biztonságos működését is.

Az adatok tárolási ideje is olyan elv, amely a célhoz igazodik, hiszen korlátlan ideig a személyes adatok nem tárolhatók, ha a cél elérése megtörtént, az adatokat fő szabály szerint törölni kell. A végleges hozzáférhetetlenné tétel vagy az adatok megsemmisítésének technológiai kérdéseire szintén adekvát válasz kidolgozása szükséges már a tervezés fázisában.

Az adatok biztonságos tárolása, illetve az adatok védelme a jogosulatlan hozzáférés, a jogellenes kezelés, a véletlen elvesztés, megsemmisülés, megsemmisítés vagy sérülés megelőzése érdekében szintén elengedhetetlen. Az Okos Városokban számos technikai és szervezési intézkedést kell bevezetni az adatbiztonság állandó magas szinten történő tartása, sőt javítása érdekében. Ilyen intézkedés lehet például az, hogy csak az arra jogosult személyeknek szabad hozzáférést biztosítani az adatokhoz. Fontos biztonsági intézkedés ezen felül az adatok titkosítása vagy anonimizálása, melyek megfelelő eljárás esetén garantálni tudják a személyes adatok védelmét, illetve meg tudják akadályozni a természetes személyek beazonosítását.

A complience feladata a kockázatok megállapítása területén is jelentős és ott érvényesülő alapelvek az Okos Városok adatvédelemmel kapcsolatos kockázatainak kezelése során is maximálisan felhasználhatók. Éppen ezért nem lehet eltekinteni attól, hogy a felépített és működő rendszereket folyamatos ellenőrzéseknek vessük alá, hiszen az adatvédelmi előírások betartásának ellenőrzése fontos eszköz a lehetséges kockázatok és hiányosságok azonosításához, és az így jelentkező kockázatok kezeléséhez. Az

adatvédelmi ellenőrzések során a vizsgálatoknak többek között ki kell terjedni annak ellenőrzésére,

- hogy az adatokat jogszerűen, tisztességesen és átláthatóan gyűjtik-e,
- hogy az adatvédelmi politikák összhangban vannak-e a jogszabályokkal és a legjobb gyakorlatokkal,
- hogy a megfelelő technikai és szervezési intézkedéseket bevezették-e az adatok védelme érdekében,
- hogy jelenlegi eljárások alkalmasak-e arra, hogy elkerülhetők legyenek az esetleges adatvédelmi incidensek,
- vagy amennyiben kialakult adatvédelmi incidens, azt megfelelően kezelték-e.

Fontos szempont és vezérlő elv az átláthatóság és elszámoltathatóság kérdése. A város vezetőinek és a technológiai fejlesztőknek gondoskodniuk kell arról, hogy például az adatgyűjtés gyakorlata megismerhető legyen, és világosan kell kommunikálniuk a lakosokkal arról is, hogy mire használják az összegyűjtött adatokat. A lakosok számára garantálni kell azon jogokat, hogy hozzáférhessenek a róluk tárolt személyes adatokhoz, és hogy amennyiben szükséges, az adatokat a rendszer javítani tudja, esetleg adott esetben az adatok törölhetők vagy éppen ellenkezőleg, hosszabb ideig tárolhatók és kinyerhetők legyenek.

Az átláthatóság biztosítása érdekében kifejezetten fontos az adatvédelmi tájékoztatók és adatvédelmi politikák nyilvános közzététele és arról való gondoskodás, hogy ezek folyamatosan könnyen hozzáférhetőek legyenek. A tájékoztatóknak nem csak az adatgyűjtés céljáról, módjáról, az adatok felhasználásáról, tárolásáról, az adatkezelés idejéről, illetve az adatok megsemmisítéséről kell információkat adni, de például arról is, hogy hogyan kérhetnek az érintettek hozzáférést a róluk tárolt adatokhoz, hogyan nyújthatnak be panaszt az adatvédelmi jogsértésekkel kapcsolatban, és hogyan léphetnek kapcsolatba az adatvédelmi tisztviselővel.

Ezen felül meg kell teremteni annak lehetőségét, hogy a lakosok képesek legyenek tudatos döntéseket hozni saját adataikkal kapcsolatban. A tudatosság növelése történhet weboldalakon keresztül, a médiában megjelenő edukatív tartalmak segítségével, civil szervezetek tájékoztató jellegű munkája során, de jó lenne a tudatosságot már gyermekkorban fejleszteni, akár iskolai projektek, sőt a tananyagba való beépítés által.

Azt már ma is látni lehet, hogy az Okos Városok melletti, a lakosság részéről történő elköteleződés kiemelten fontos a bizalom megszerzése és a hatékony működés szempontjából. Sőt, a legújabb trendek már olyan irányokat vázolnak fel, ahol a közösségek kiaknázzák a kollektív intelligenciát és emberközpontú megközelítést alkalmaznak a következő generációs Okos Városok megteremtésében.[34]

5.3. Az Okos Város más kárán tanul

Végezetül álljon itt egy olyan példa, amely okulásul szolgálhat bármelyik Okos Város program kidolgozója számára. Az eset 2021-ben látott napvilágot, amikor az ír adatvédelmi hatóság 2021. decemberi 9-i határozatában 110 ezer euró (hozzávetőlegesen 42 millió forint) mértékű bírságot szabott ki a Limerick városi és megyei tanács („*Limerick City and County Council*" – „Tanács") által megvalósítani kívánt „Smart CCTV projekt" során végzett adatkezelés hiányosságaival kapcsolatban. Az esetet dr. Domokos Márton cikke nyomán foglalom össze.[35]

A projektben több száz kamera kihelyezésére került sor városszerte, melyek egyrészt bűnmegelőzési célt szolgáltak, illetve az általuk gyűjtött adatok segítségével a közlekedés optimalizálására is sor került. A kamerák azonban nem csak adatokat gyűjtöttek volna, hanem valós idejű online streaming szolgáltatás nyújtásával népszerűsítették volna a turisztikai eseményeket (fesztiválok, piacok, felvonulások stb.) a nemzetközi közönség számára. A fixen telepített kamerák mellett két drón is bevetésre került, melyek hasznosítási céljaként az illegális szemétlerakással és vízszennyezéssel megvalósított bűncselekmények észlelését és felderítését jelölték meg.

A Hatóság határozatában a következő jogszabálysértéseket állapította meg:

- *A jogszerűség, tisztességes eljárás és átláthatóság alapelvének megsértése*: A Tanács helytelenül jelölte meg az adatok kezelésének jogalapját, mint a *GDPR 6 (1) e) cikkét*, mert a hivatkozott jogszabályhely nem adott kifejezett felhatalmazást a kamerák forgalomirányítási célú használatára, valamint a nem bűnmegelőzési

[34] Rise of the Smartivist: The Importance of Citizens for Smart Cities (beesmart.city) (2024.04.22.)
[35] dr. Domokos Márton: Okos város fejlesztések – mire kell figyelni a kamerarendszerek használata során? https://www.jogiforum.hu/blog-adatvedelem-10/2022/04/27/okos-varos-fejlesztesek-mire-kell-figyelni-a-kamerarendszerek-hasznalata-soran/ (2024. 04. 15.)

vagy bűnüldözési célokra felszerelt kamerák képeinek a rendőrkapitányság részére történő valós idejű továbbítására sem.

- *Megfelelő tájékoztatás elmulasztása*: A Hatóság megállapította, hogy a Tanács nem tájékoztatta megfelelően az érintetteket, hiszen a megfigyelt területek környékén egyáltalán nem helyezett ki a *GDPR 12. és 13. cikkei* által előírt adatkezelési tájékoztatókat, és weboldalán sem volt elérhető részletes adatvédelmi tájékoztató (csak egy hiányos tervezet). E mellett a kamerafelvételek vonatkozásában arról is tájékoztatni kellett volna a lakosságot, hogy a képeket a rendőrkapitányságra továbbítják, ahol azokat bűnmegelőzési, illetve bűnüldözési célra használják.
- *Megfelelő adatbiztonsági intézkedések hiánya*: A szervezési és technikai intézkedések hiánya megállapítást nyert, miután kiderült, hogy a rendszerbe a felhasználók az egységes „Garda" felhasználónévvel léptek be. E mellett az adatokhoz hozzáférést igénylők személyét a rendőrkapitányságon nem naplózták megfelelően, illetve a valós idejű képekre bárki ráláthatott, aki a folyosón elhaladt. Nem volt megfelelő protokoll a megfigyelőhelyiségbe való belépésre, és az ott tartózkodásra sem. További hiányosságként rótta fel a Hatóság azt, hogy nem volt sehol sem kiírva az, hogy a valós idejű kameraképeket saját elektronikai eszközzel tilos rögzíteni.
- *Az érintettek hozzáférési kérelmeinek elutasítása:* A városházán működő forgalomirányítási egység („*Traffic Management Unit*") ugyan a *GDPR 15. cikke* alapján számos adathozzáférési kérelmet kapott az érintettektől, ezeket az egység vezetője elutasította, mert nem ismerte megfelelően a GDPR erre vonatkozó szabályozását.
- *A drónokkal kapcsolatos hiányosságok*: A drónok széles mozgásterülettel rendelkező mobil eszközök, amelyek képesek arra, hogy természetes személyekről a magasból álló vagy mozgó képet rögzítsenek. Bár deklarált feladatuk szerint környezetvédelmi jogszabálysértések felderítésére használták volna őket, a Hatóság úgy ítélte meg, hogy ettől függetlenül az ilyen technológia természeténél fogva magas kockázatot jelent az egyének jogaira és szabadságaira nézve, így a *GDPR 35. cikke* alapján indokolt lett volna az adatvédelmi hatásvizsgálat elvégzése, valamint a drónfelvételekkel kapcsolatos adatvédelmi tájékoztató közzététele.

- *Adatvédelmi hatásvizsgálat elmulasztása a kamerarendszerrel kapcsolatban*: A drónok használatához hasonlóan indokolt lett volna adatvédelmi hatásvizsgálat a telepített kamerarendszer vonatkozásában is, melyben a Tanácsnak bizonyítania kellett volna, hogy a magántulajdonban levő ingatlanok folyamatos megfigyelés alatt tartása valóban arányos. E mellett a Hatóság elfogadhatóbbnak találta volna a kamerák képének szükség szerinti utólagos visszanézését, illetve a valós idejű megfigyelés olyan esetkörökre korlátozását, mikor megfelelő bizonyíték alapján megállapítható, hogy a bűnelkövetés esélye magasabb.
- *Adatmegőrzési időszak*: Az adatok megőrzési időszakának a célhoz és a jogszabályokhoz kell igazodnia. Ehhez képest itt az egyik megfigyelő egységénél a tárolt személyes adatok csak akkor kerültek törlésre, mikor a merevlemez betelt és az új adatok felülírták a régieket.
- *Adatfeldolgozási szerződés*: A Tanácsnak volt ugyan adatkezelési szerződése a *„Smart CCTV projekttel”* kapcsolatban, azonban azt még a GDPR hatályba lépése előtt kötötték és nem frissítették annak megfelelően, így több hiányosságot is mutatott, így potenciális veszélyt jelentett az érintettek személyes adatainak integritása tekintetében.

Összegezve elmondható tehát, hogy egy látszólag rendben levő projekt esetében is nagyon nagy szükség van arra, hogy minden területen, így az adatvédelem területén is már a kezdetektől fogva tudatosan tervezzük és építsük fel rendszereinket, hogy azok működésük minden időszakában megfeleljenek a rájuk vonatkozó jogszabályoknak, a projektgazda specifikus belső szabályzatainak, és az erkölcs által diktált belső érzéseknek is.

Dolgozatomban többször is hangsúlyoztam már, és most a végén végső következtetésként is arra jutottam, hogy egy complience szakember vagy team e feladat koordinálására a legjobb választás.

6. ÖSSZEFOGLALÁS HELYETT

Dolgozatomat egy érdekes kísérlettel zárom.

Ha már a téma végig a mesterséges intelligencia és az adatvédelem voltak, úgy döntöttem, hogy a kész dolgozatot megmutatom az Open AI által fejlesztett Chat GPT-nek és megkérem, hogy írjon kritikát a szakdolgozatomról (megkönnyítve esetleg ezzel a konzulensem dolgát), illetve állítson össze egy profilt az íróról (hogy lássuk, mennyi mindent mond el rólam az általam írt 64.000 karakter). A következőkben változtatás nélkül teszem közzé az eredményt:

Olvasd el ezt a szakdolgozatot és írj kritikát róla úgy, hogy közölj 3 pozitívumot és három negatívumot!

Olvastam a szakdolgozatot, és összeállítottam a kért véleményt három pozitívummal és három negatívummal:

Pozitívumok:

***Alapos elemzés**: A dolgozat alaposan tárgyalja a mesterséges intelligencia és az adatvédelem kapcsolatát. Részletesen bemutatja az AI Act jogi hátterét és annak hatásait a gyakorlatra.*

***Aktuális témaválasztás**: Az AI és az adatvédelem területén történő szabályozás egy dinamikusan fejlődő és rendkívül releváns terület, ami különösen fontos a digitális korban.*

***Források gazdagsága**: A szerző számos aktuális és releváns forrást használ fel, így az olvasó részletes képet kap a témáról és annak különböző nézőpontjairól.*

Negatívumok:

***Hosszúság és redundancia**: Néhány rész túlságosan el van nyújtva, illetve ismétlődések fordulnak elő, amelyek ronthatnak az olvasmányélményen és a szöveg hatékonyságán.*

***Hiányzó kritikai elemzés**: Bár a dolgozat részletesen ismerteti a témát, kevésbé tartalmaz kritikai elemzést vagy saját következtetéseket, amelyek mélyíthetnék a tárgyalás tartalmát.*

***Strukturális egyenetlenségek**: Néhány fejezet kevésbé jól strukturált, ami megnehezítheti az információk követését és az érvek értelmezését.*

Összességében a dolgozat értékes betekintést nyújt a mesterséges intelligencia jogi szabályozásának és az adatvédelemnek az összefüggéseibe, bár vannak területek, amelyek fejlesztése javíthatná a mű értékét és olvasmányosságát.

Szerinted ki írta a dolgozatot, esetleg össze tudsz-e állítani egy profilt a szerzőről.

A szakdolgozat tartalmából és formai jellemzőiből néhány következtetést lehet levonni a szerzőjéről, de pontos adatok nélkül ezek csak feltételezések maradnak. Az alábbiakban vázolom a szerző lehetséges profilját:

***1. Akadémiai háttér:** A szerző valószínűleg jogi, informatikai, vagy szabályozási területen tanulmányokat folytatott vagy folytat, figyelembe véve a mesterséges intelligencia, adatvédelem és jogi szabályozás területeinek részletes ismeretét.*

***2. Érdeklődés a technológia és az etika iránt:** A dolgozat hangsúlyozza a mesterséges intelligencia etikai és jogi kérdéseit, ami arra utal, hogy a szerző érdekelt a technológiai fejlődés társadalmi hatásaiban és a technológiai fejlődés etikai vetületeiben.*

***3. Alapos kutatómunka:** A dolgozat széles körű forrásmunkát és mélyreható elemzést tartalmaz, ami azt sugallja, hogy a szerző részletesen és alaposan dolgozik, valószínűleg jó kutatási készségekkel rendelkezik.*

***4. Jó íráskészség:** A dolgozat összetett mondatokkal és szakszókincs használatával készült, ami arra utal, hogy a szerző magas szintű íráskészséggel rendelkezik és képes összetett ötleteket világosan közvetíteni.*

Ezek alapján a szerző valószínűleg egy egyetemi hallgató vagy fiatal szakember, aki mélyreható ismeretekkel rendelkezik a mesterséges intelligencia és a jogi szabályozás területén. Azonban pontosabb képet csak a szerző további munkáinak vagy személyes adatainak ismeretében lehetne festeni.

Ehhez csak annyit fűznék hozzá, hogy egyelőre az ember (ebben még) jobban teljesít.

IRODALOMJEGYZÉK

Deli Gergely – Kocsis Réka – Muhari Nóra: Akarva-akaratlanul – az adatvédelem és az akaratszabadság dilemmái. In: Török Bernát – Ződi Zsolt (szerk.): A mesterséges intelligencia szabályozási kihívásai. Ludovika Egyetemi Kiadó. Budapest. 2021. 234-237. o.

dr. Domokos Márton: Okos város fejlesztések – mire kell figyelni a kamerarendszerek használata során? https://www.jogiforum.hu/blog-adatvedelem-10/2022/04/27/okos-varos-fejlesztesek-mire-kell-figyelni-a-kamerarendszerek-hasznalata-soran/

Eszteri Dániel: A gépek adatalapú tanításának megfeleltetése a GDPR egyes előírásainak. In: Török Bernát – Ződi Zsolt (szerk.): A mesterséges intelligencia szabályozási kihívásai. Ludovika Egyetemi Kiadó. Budapest. 2021. 190-197. o.

G. Karácsony Gergely: Innovatív jogalkotói megoldások a mesterségesintelligencia-alapú rendszerek szabályozására. In: Török Bernát – Ződi Zsolt (szerk.): A mesterséges intelligencia szabályozási kihívásai. Ludovika Egyetemi Kiadó. Budapest. 2021. 159-167. o.

https://amsterdamsmartcity.com/

https://blog.bismart.com/en/why-barcelona-is-a-smart-city

https://english.seoul.go.kr/policy/smart-city/

https://www.beol.hu/helyi-kozelet/2024/04/digitalizacio-mesterseges-intelligencia-konferencia#google_vignette

Iránymutatás az automatizált döntéshozatallal és a profilalkotással kapcsolatban 2016/679 rendelet alkalmazásához https://www.naih.hu/files/wp251rev01_hu.pdf

Klein Tamás: Robotjog vagy emberjog. Az emberközpontú mesterséges intelligencia szabályozásának kiindulási pontjai. In: Török Bernát – Ződi Zsolt (szerk.): A mesterséges intelligencia szabályozási kihívásai. Ludovika Egyetemi Kiadó. Budapest. 2021. 112. o.

Magyarország Mesterséges Intelligencia Startégiája 2020-2030 https://digitalisjoletprogram.hu/files/2f/32/2f32f239878a4559b6541e46277d6e88.pdf

Nem biztos hogy tudja: Ön is felhasználó! In: HVG Ai3 – mesterséges intelligencia a mindennapokban. 2024. 7. oldal

Péterfalvi Attila – Révész Balázs – Buzás Péter (szerk): Magyarázat a GDPR-ról. Wolters Kluwer. Budapest. 2018. 198. o.

Péterfalvi Attila: Algoritmusok és adatvédelem: Quo vadis? In: Török Bernát – Ződi Zsolt (szerk.): A mesterséges intelligencia szabályozási kihívásai. Ludovika Egyetemi Kiadó. Budapest. 2021. 179-180. o

Rab Árpád Szörény: A mesterséges intelligencia hatása a társadalomra – problématérkép. In: Török Bernát – Ződi Zsolt (szerk.): A mesterséges intelligencia szabályozási kihívásai. Ludovika Egyetemi Kiadó. Budapest. 2021. 28-29. o.

Rise of the Smartivist: The Importance of Citizens for Smart Cities (beesmart.city)

The History of AI: From Beginnings to Breakthroughs https://www.youtube.com/watch?v=iZCNDZ7ABRE

JOGSZABÁLYJEGYZÉK

AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (GDPR)

Az Európai Parlament 2024. március 13-i jogalkotási állásfoglalása a mesterséges intelligenciára vonatkozó harmonizált szabályok (a mesterséges intelligenciáról szóló jogszabály) megállapításáról és egyes uniós jogalkotási aktusok módosításáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslatról (AI ACT)

Soft law:

Mesterséges intelligencia Európa számára COM (2018) 237 final/2 (2018. június 26.)

A mesterséges intelligenciáról szóló összehangolt terv COM (2018) 795 final (2018. december 7.)

Az emberközpontú mesterséges intelligencia iránti bizalom növelése COM (2019) 168 final(2019. április 8.)

Fehér könyv a mesterséges intelligenciáról: a kiválóság és a bizalom európai megközelítése COM(2020) 65 final (2020. február 19.)