



**37. Országos Tudományos Diákköri Konferencia
Állam- és Jogtudományi Szekció**

Budapest, 2025. március 24–26.

Rendező intézmény:
*Károli Gáspár Református Egyetem
Állam- és Jogtudományi Kar*



Állam- és Jog-
tudományi Szekció

**Gazdasági társaságok adatvédelmi kihívásai a Big
Data és a mesterséges intelligencia korában az
Európai Unióban**

Kézirat lezárásának dátuma:

2024/11/21

Mesterséges intelligencia nyilatkozat

Kijelentem, hogy a dolgozat érdemi tartalmának elkészítése során a mesterséges intelligenciát kizárólag fordítási célokra alkalmaztam. A mesterséges intelligencia alkalmazásával az volt a célom, hogy az egybefüggő, bonyolult szaknyelvű szövegek átfogóbb megértése és elemzése hatékonyabbá váljon. Azon szövegrészek fordítását, amelyek a dolgozatomba - hivatkozásokkal ellátva - tartalmilag átemelésre kerültek, többszörösen és alaposan felülvizsgáltam, a lefordított tartalom végső formába öntése és a dolgozatba való beépítése kizárólag saját megítélésem alapján történt. A fordításra a ChatGPT GPT-4 modelljét használtam.

Kijelentem továbbá, hogy a mesterséges intelligencia fordítási célból történő igénybevételén túl a dolgozat minden más része kizárólag az általam végzett kutatás, elemzés és szövegalkotás eredménye.

Tartalomjegyzék

1. Bevezetés	4
2. A Big Data és a mesterséges intelligencia fogalmának áttekintése	5
2.1. A Big Data definíciója és az általa kínált lehetőségek.....	5
2.2. Mesterséges intelligencia: fejlődés és jelenlegi technológiák	7
2.3. MI és Big Data kapcsolata.....	7
2.3.1. A gépi tanulás során megvalósított adatgyűjtés mechanizmusa és annak előnyei.....	8
2.3.2. Gyakorlati alkalmazása	8
2.4. Az adatok szerepe.....	9
3. Az Európai Unió adatvédelmi keretei	10
3.1. Alapjogi Charta.....	10
3.2. GDPR.....	10
3.3. NIS 2 irányelv	11
3.4. Az AI Act vonatkozó rendelkezései.....	12
3.5. Nemzetközi deklarációk a téma kapcsán.....	14
4. A vállalati szektort érintő kihívások a Big Data és MI korában.....	16
4.1. Profilalkotás.....	16
4.2. Predikciók, „nudging”	18
4.3. A visszanevesíthetőség problémája	20
4.4. Transzparencia hiánya	20
4.4.1. Érintettek tájékoztatása.....	21
4.4.2. Szerzői jogi kérdések.....	22
4.4.3. A felelősséggel kapcsolatos dilemma.....	22
4.4.4. Kockázatelemzés, biztonsági intézkedések.....	23
4.5. Diszkriminatív gyakorlatok	23
4.6. Adattípusok összemosódása	24
5. Jövőbeli irányok	26
5.1. Adatok megfontoltabb szelektálása, validálása	28
5.2. Adatvédelmi hatásvizsgálatok	29
5.2.1. Eredmények nyilvánossá tétele	30
5.2.2. Független szakértők bevonása.....	30
5.3. Automatikus hatásvizsgálat	31
5.4. Átláthatóság növelése	31
5.4.1. Átláthatósági tesztek.....	32
5.4.2. Eleve megmagyarázható modellek.....	32
6. Összegzés.....	34
7. Irodalomjegyzék.....	35
7.1. Szakcikk, kiadványok.....	35
7.2. Jogszabályok.....	38

1. Bevezetés

A technológia úttörése az emberi civilizáció kezdete óta számtalanszor hozott alapvető változásokat az életünkben, ez azonban mára korábban nem tapasztalható léptéket öltött. Korunk egyik elhanyagolhatatlan fontosságú jelensége a mesterséges intelligencia (MI), mely olyan technológiákkal karöltve, mint a Big Data, képes arra, hogy minden eddiginél gyorsabban alakítsa át a gazdasági ökoszisztémát, ezzel újradefiniálva többek között a versenyképesség feltételeit.¹

Munkám fókuszában azok a gazdasági társaságok állnak, amelyek az Európai Unió területén működnek, és tevékenységük során mesterséges intelligenciát alkalmaznak. Napjaink dinamikusan változó gazdaságában ezeknek a vállalkozásoknak méretüktől függetlenül számtalan, eddig ismeretlen kihívással kell szembenéznük mind a szabályozási környezet hiányosságaiból, mind az MI természetéből adódóan, hiszen az új technológiák révén képesek olyan mértékű adatgyűjtést, elemzést és felhasználást megvalósítani, amely korábban elképzelhetetlen volt. Ennek megfelelően a dolgozat fő célja, hogy átfogó képet nyújtson az adatvédelem területén felmerülő legfontosabb problémákról.

A dolgozat elkészítése céljából folytatott kutatás során első lépésként a jogszabályszövegek részletes elemzését végeztem el, különös figyelmet fordítva az adatvédelmi alapelvekre, így a célhoz kötöttségre, az adattakarékosságra és az átláthatóságra. Ezt követően a fogalmi keretek tisztázása, a jogi normák strukturális összefüggéseinek feltárása és a gyakorlati alkalmazhatóság kérdéseire összpontosítottam. Dolgozatom problémaorientált megközelítést alkalmaz, hiszen az MI használatával felmerülő gyakorlati kérdéseket vizsgálja a jelenlegi adatvédelmi keretrendszer alkalmazhatósága tükrében.

A fentieknek megfelelően dolgozatom első részében áttekintem a Big Data és a mesterséges intelligencia fogalmait, azok történeti fejlődését, valamint a két technológia együttes alkalmazásának lehetőségeit. Ezt követően részletesen elemzem az Európai Unió adatvédelmi jogának szabályozási kereteit, különös tekintettel arra, hogy ezek a jogszabályok milyen módon próbálnak reagálni az adatvédelem kapcsán felmerülő olyan veszélyekre, mint például a profilalkotás, a predikciók vagy a visszanevesíthetőség.

¹ Omer TENE - Jules POLONETSKY: *Privacy in the Age of Big Data: A Time For Big Decisions*. Stanford Law Review Online, 2012. 63-64.; Richard KEMP: *Legal Aspects of Managing Big Data*. Computer Law & Security Review, Volume 30, Issue 5, 2014. 482-491.

Jelen dolgozatomban azon felvetésem igazolását célozza, hogy a mesterséges intelligenciát alkalmazó gazdasági társaságok gyakorlatai - elsősorban a jogszabályi keretek meghaladottságából adódóan - számos ponton nem felelnek meg maradéktalanul az Európai Unió hatályos adatvédelmi szabályozásának, erre figyelemmel szükségessé válhat annak átdolgozása. Amennyiben e hipotézisem igazolást nyer, az elemzés során kitérek arra is, hogy az adatvédelem terén milyen jövőbeli irányok szükségesek ahhoz, hogy a szabályozás lépést tudjon tartani a technológiai innováció ütemével, ennek megfelelően dolgozatomban végén megoldási javaslatokat fogalmazok meg arra vonatkozóan, hogyan valósítható meg a fentiekben összegzett kihívások kezelése.

2. A Big Data és a mesterséges intelligencia fogalmának áttekintése

2.1. A Big Data definíciója és az általa kínált lehetőségek

A Big Data kifejezés azon óriási adattömegeket jelöli, melyek nagyságukból, áramlásuk sebességéből, formájuk változatosságából adódóan hagyományos adatfeldolgozó eszközökkel rendkívül nehezen, vagy egyáltalán nem kezelhetők.²

A Big Data kifejezés, melynek kialakulásában John MASHEY informatikus játszott meghatározó szerepet,³ a 2000-es évek elején vált széles körben ismertté, ekkor ugyanis a digitális szolgáltatások számának megnövekedése révén gyűjtött adatmennyiség mértéke megkövetelte az adatkezelési technológiák és módszerek fejlődését. A 21. században, az internet korában a felhasználók az azt megelőzőnél számottevően több adatot kezdtek el termelni, amelyek gyűjtése és rendszerezése is szükségessé vált, hiszen az ezekből levonható következtetések hasznosak lehetnek mind a vállalkozások, mind az állami szervek számára.

Az üzleti szférában jelenleg elsősorban a marketing és az értékesítés területén koncentrálódik a Big Data forradalmi hatása: a gazdasági társaságok a fogyasztói viselkedés részletes elemzése révén egyebek mellett célzott reklámkampányokat indíthatnak, illetve az egyéni preferenciák figyelembevétele mellett minden eddiginél effektívebben kínálhatnak személyre szabott ajánlatokat ügyfeleik részére. A fentiekben túl az ügyfelek részéről érkezett visszajelzések és piaci trendek elemzése lehetővé teszi a termékek és szolgáltatások fejlesztésének optimalizálását, így jobban kielégítve a fogyasztói igényeket. Emellett említésre érdemes, hogy a technológia jelentős előnyökkel járhat például az egészségügy területén, ideértve a járványok

² Douglas LANEY: *3D Data Management: Controlling Data Volume, Velocity and Variety*. Gartner. Retrieved, 2001, 6.

³ Francis X. DIEBOLD: *On the Origin(s) and Development of the Term "Big Data"*, 2012. PIER Working Paper No. 12-037. 5.

előrejelzését, a kórházi kapacitások kezelését és a betegségek korai felismerését genetikai elemzés révén.⁴

Az adatok sokféleségéből (azaz a jelenség jellemzésére gyakran használt 4V együttes⁵ elemei közül a *variety*-ből) következik, hogy gyakran olyan adathalmazok képződnek, melyek természetes személy számára nehezen értelmezhetőek, ezért az adatbányászat- és feldolgozás kiemelt feladata a megfelelő, „prediktív” adatok felkutatása és a különféle adatok összefüggésbe hozása, ún. komplex adatbázisok létrehozása, hiszen önmagában nem az adatoknak, hanem az általuk hordozott információnak van gazdasági értéke.⁶ Ennek kapcsán a mesterséges intelligencia alkalmazása kiemelt jelentőséggel bír, tekintettel arra, hogy nagymértékben leegyszerűsíti a fenti folyamatokat.

Fontos megjegyezni, hogy az adatok ilyen méretű halmazában gyakorta fordulnak elő bizonytalan, hiányos vagy használhatatlan adatok, azonban az eddigi tapasztalatok azt mutatják, hogy a legtöbb esetben e problémát a megfelelő adatok nagy száma kiküszöböli.⁷

Szükségszerű továbbá rámutatni arra is, hogy a gyűjtött adatok sokféleségéből következik a Big Data azon jellegzetessége, hogy a különböző ágazatok számára különféle adatok lehetnek hasznosak, emiatt az adatbányászat egyre inkább célzott jelleget ölt. Mindebből következik az is, hogy tulajdonképpen csupán azok a piaci szereplők versengenek egymással, akik az adatokat ugyanabból a célból kívánják hasznosítani,⁸ így a verseny elsősorban az azonos célpiacokra fókuszáló gazdasági társaságok között éleződik ki. Ennek következtében a cégek egyre inkább specializálódnak és egyedi megoldásokkal próbálnak piaci előnyt szerezni, ami növeli a piac szegmentáltságát.

Már ma számtalan cég tevékenysége áll pusztán „adatosításból”, ami jól mutatja, hogy a Big Data teljesen új korszakot nyitott a gazdasági életben, mely lehetőségeket és kihívásokat egyaránt tartogat magában. A modern üzleti szféra egyik legdinamikusabban fejlődő eszközeként olyan potenciállal bír, amely forradalmasíthatja az európai vállalkozások versenyképességét a globális piacon, előmozdítva az innovációt és a fenntartható növekedést a

⁴ Jane THOMASON: *Big Tech, Big Data and the New World of Digital Health*. Global Health Journal, Volume 5, Issue 4, 2021. 165-168.

⁵ Megjegyzendő, hogy egyes szerzők kezdetben még csak a Big Data három alapvető dimenzióját – a Volume-t, Velocity-t és Variety-t – emelték ki, amelyek később további aspektusokkal bővültek, hogy teljesebben tükrözzék a Big Data komplexitását. Lásd: Philip RUSSOM: *Big Data Analytics*. TDWI Best Practices Report, 2011.

⁶ Daniel L. RUBINFELD - Michal S. GAL: *Access Barriers to Big Data*. Arizona Law Review, Vol. 59, 2017. 3.

⁷ BÖGEL György: *A Big Data ökoszisztémája*. Typotex Elektronikus Kiadó Kft, Budapest, 2015. 34.

⁸ KESERŰ Barna Arnold: *A 21. századi technológiai változások hatása a jogalkotásra*. Dialóg Campus, Budapest, 2020. 10.

különböző ágazatokban. ZÖDI Zsolt szavaival élve „a Big Data korszak arra utal, hogy az adattermelődés új társadalmi jelenségeket indukál már jelenleg is, és még komolyabb változásokat indukálhat a jövőben.”⁹

2.2. Mesterséges intelligencia: fejlődés és jelenlegi technológiák

A mesterséges intelligencia (MI) vagy *artificial intelligence (AI)* szűkebb értelemben véve azon számítógépes rendszerek, programok összességét jelenti, melyek képesek utánózni az olyan, emberi gondolkodást igénylő folyamatokat, mint az érvelés vagy a tanulás.¹⁰ Az MI létrehozásának ötlete már az 1950-es években felmerült Alan TURING munkássága révén,¹¹ az utóbbi időben azonban exponenciális fejlődésen ment keresztül, ezáltal széles körben elérhetővé vált, forradalmasítva a felhasználói alkalmazást.

Napjainkban az MI képes rendkívül komplex feladatok megoldására, melyek korábban kizárólag az emberi intelligencia domainjébe tartoztak,¹² ebből adódóan ez a technológia számtalan ágazat vonatkozásában hozott vagy hozhat innovatív változásokat. Küszöbön áll mind a szolgáltatások, mind a munkaerőpiac alapos átalakulása az optimálisabb és költséghatékonyabb működés jegyében, melyhez a tagállamoknak és az Európai Uniónak egyaránt szükséges alkalmazkodnia.

2.3. MI és Big Data kapcsolata

A mesterséges intelligencia nem izoláltan, hanem egy specifikus technológiai környezet részeként fejlődött,¹³ tulajdonképpen ezen technológiák összefonódása révén indíthat el innovatív változásokat a gazdaság összes területén. A Big Data biztosítja ugyanis azokat a hatalmas adathalmazokat, amelyek a mesterséges intelligencia algoritmusai számára a tanulási és elemzési folyamatok során elengedhetetlenek, ugyanakkor egy ilyen adatmennyiség begyűjtéséhez hatékony segítséget jelenthet maga a mesterséges intelligencia, így nem csak az MI alkalmazza a Big Datát, hanem fordítva is.¹⁴

⁹ ZÖDI Zsolt: *Jog és Jogtudomány a Big Data korában*. Állam- és Jogtudomány, 58. évfolyam 1. szám, 2018. 95.

¹⁰ Toshinori MUNAKATA: *Fundamentals of the New Artificial Intelligence*. Springer, 2008. 1-2.

¹¹ Lásd: A. M. TURING: *Intelligent Machinery*. Oxford University Press, 1948. és A. M. TURING: *Computing Machinery and Intelligence*. Oxford University Press, 1950.

¹² J. MINSKY: *Steps Toward Artificial Intelligence*. Proceeding of The Ire, 1961, 8.

¹³ Lilian MITROU: *Data Protection, Artificial Intelligence and Cognitive Services: Is The General Data Protection Regulation (GDPR) "Artificial Intelligence-Proof"?*, 16.

¹⁴ 38th International Conference of Data Protection and Privacy Commissioners, Artificial Intelligence, Robotics, Privacy and Data Protection, October 2016, 4.

2.3.1. A gépi tanulás során megvalósított adatgyűjtés mechanizmusa és annak előnyei

A mesterséges intelligencia gépi tanulási folyamata három alapvető szakaszra bontható. Kezdetben a rendszer nagy mennyiségű adatot kap bemenetként, amelyek között az algoritmus mintákat és hasonlóságokat keres, a rögzített minták alapján pedig egy modellt hoz létre, amely képes az ismert minták alapján feldolgozni a későbbiekben bekerülő új adatokat, mérlegelve, hogy azok a korábban tanult mintázatok közül melyikhez állnak a legközelebb.

A mechanizmus relevanciája, hogy a gépi tanulás alapján működő MI rendszerek képesek felismerni az adathalmazokban rejlő olyan összefüggéseket és mintákat, melyek emberi elemzők számára nagy eséllyel rejtve maradnának. Ez lehetővé teszi számukra, hogy összetett adatokból is olyan értékes információkat nyerjenek ki, amelyek hozzájárulnak a döntéshozatali folyamatok javításához, a trendek előrejelzéséhez, a felhasználói és ügyfélpreferenciák pontosabb megértéséhez. Emellett kiemelendő előny ezen technológiai megoldással kapcsolatosan a gyorsaság, ami döntő fontosságú lehet például a rapid módon változó pénzügyi piacon vagy az akut beavatkozást igénylő egészségügyi vészhelyzetekben.

2.3.2. Gyakorlati alkalmazása

A fentiekben ismertetett a kooperatív megoldás növekvő hatékonysággal válik képessé komplex mintákat felismerni, előrejelzéseket készíteni és automatizált döntéseket hozni. A mesterséges intelligencia előnye, hogy a kezelt adatok formájának változékonysága ellenére tud gyors és hatékony elemzést végezni.

Szükségszerű a teljesség igénye nélkül néhány olyan példát említeni, amelyek alkalmasak annak reprezentációjára, hogy milyen széles körben alkalmazható e forradalmi technológiák összekapcsolása. A mesterséges intelligencia általi adatelemzés lehetővé teszi a vállalkozások számára, hogy mélyreható betekintést nyerjenek a piaci trendekbe, a fogyasztók magatartásába és versenytársaik tevékenységébe. A begyűjtött adatok elemzése révén lehetővé válik a piaci változások előrejelzése, ezáltal az árazási stratégiák optimalizálása és a felhasználói elégedettség növelése személyre szabott szolgáltatások révén. A 21. század technológiai megoldásainak ugyanis fontos kulcsszava a perszonalizáció, a felhasználói igényekhez való adaptáció, ehhez olyan bonyolult döntési mechanizmusokra van szükség, amelyeket leginkább MI-alapú öntanuló rendszerekkel lehet kiváltani.¹⁵

¹⁵ ESZTERI Dániel: *Hogyan tanítsuk jogszerűen a mesterséges intelligenciánkat?* Magyar Jog, 2019/12., 671.

Emellett a Big Data és az MI alkalmazása javíthatja a termelési folyamatok hatékonyságát azáltal, hogy pontosabban szabályozza az ellátási láncokat és minimalizálja a pazarlást, valamint úttörő szerepet játszhat a potenciális kockázatok felismerésében is.

2.4. Az adatok szerepe

A fentiekben ismertetett technológiák alapvető építőelemei lévén az adatok jelentőségének tárgyalása elhanyagolhatatlan. Az MI számára az adatok egyrészt tanulási alapot jelentenek, hiszen a tanulási folyamat a fent kifejtetteknek megfelelően tulajdonképpen rendkívüli méretű adathalmazok áttekintéséből és elemzéséből áll, ami elengedhetetlen a következtetések és mintázatok feltárása érdekében. Ennek megfelelően az adatok minősége, hozzáférhetősége és integritása közvetlen hatással van a Big Data és az MI alkalmazásának hatékonyságára, ezért meghatározó jelentősége van a felhasznált adatok megbízhatóságának, relevanciájának, és áttekinthetőségének biztosításának az optimális működés érdekében.¹⁶

Az adatok szelektálásának fontossága kapcsán ESZTERI Dániel azt az adattakarékosság elvével is egybeeső tételt fogalmazta meg, hogy a gépi tanuláshoz először csak korlátozott mennyiségű tesztadatot kell felhasználni, majd a tesztadatok feltöltése után folyamatosan monitorozni kell a rendszert, hogy az elérni kívánt cél szempontjából mennyire működik pontosan és hatékonyan. Amennyiben kevesebb adat is elég a megfelelő hatékonyság eléréséhez, úgy felesleges továbbiakat felhasználni.¹⁷

¹⁶ Datatilsynet: Artificial Intelligence and Privacy. Report, January 2018, 11. <https://www.datatilsynet.no/globalassets/global/english/MI-and-privacy.pdf>

¹⁷ ESZTERI, i. m., 673.

3. Az Európai Unió adatvédelmi keretei

Az Európai Unióban kiemelkedő jelentőséget élvez az uniós polgárok jogainak védelme, erre tekintettel az adatvédelem terén is szükséges volt egy olyan kiterjedt keretrendszer kialakítása, amely az MI-felhasználók védelmét és az adatkezelés hatékonyságát egyaránt szolgálja.

3.1. Alapjogi Charta

Az Európai Unió adatvédelmi joga több jogforráson nyugszik. Elhanyagolhatatlan jelentőségű ezek közül az Európai Unió Alapjogi Chartája, melynek 8. cikke az alapvető szabadságjogok között szabályozza a személyes adatok védelmét. A cikk első bekezdése kimondja, hogy mindenkinek joga van a rá vonatkozó személyes adatok védelméhez, ezzel hangsúlyozva az adatvédelem fontosságát az emberi méltóság és a magánélet tiszteletben tartása érdekében. A második bekezdés garantálja, hogy az adatok kezelése csak tisztességesen és jóhiszeműen, meghatározott célokból, az érintett személy hozzájárulása alapján vagy valamilyen más, a törvényben rögzített jogos okból történhet, biztosítva ezzel az adatkezelés átláthatóságát és jogszerűségét.

3.2. GDPR

A 8. cikknél jóval szélesebb körű jelleggel tartalmaz rendelkezéseket az adatvédelemre vonatkozóan a 2018. májusában hatályba lépett Általános Adatvédelmi Rendelet (GDPR). A GDPR egy 1995-ös adatvédelmi irányelvet¹⁸ váltott fel, jelentős változásokat hozva az adatvédelem területén, melyet a 21. század rohamos technológiai fejlődése és a globalizáció új kihívásai kifejezetten szükségessé tettek.¹⁹

Újítása egyrészt, hogy az Európai Unió teljes területén egységes adatvédelmi szabályozást teremtett, eltérően az irányelvtől, amelyet a tagállamok különféle módokon ültettek át nemzeti jogukba, így a kívánt harmonizációs hatást nem érte el.²⁰ Ezen túl a rendelet kibővítette az érintettek jogait, beleértve az adatokhoz való hozzáférés jogát, az adatok helyesbítésének jogát, az elfelejtéshez való jogot, valamint az adatok hordozhatóságának jogát; továbbá kiterjesztette az adatvédelmi rendelkezések betartásának kötelezettségét az adatkezelőkre és az

¹⁸ Az Európai Parlament és a Tanács 95/46/EK irányelv (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról

¹⁹ European Commission (2010): Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – A comprehensive approach on personal data protection in the European Union. Brussels, 4. November. COM(2010) 609 final. 2.

²⁰ Paul DE HERT – Vagelis PAPAKONSTANTINOU: The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals, 2012. *Computer Law and Security Review*, Vol. 28, No. 2.

adatfeldolgozókra. Szükséges kiemelni továbbá, hogy a GDPR a szankciórendszert is egységesítette, aminek részét képezi az új, közigazgatási bírság kiszabására vonatkozó következetes szabályozás is, hangsúlyozva az adatvédelem fontosságát. Mindezek mellett a GDPR pontosította a hozzájárulás fogalmát és a korábbi irányelv alapelvein túl új elveket is bevezetett. Új jogintézmény az adatvédelmi keretrendszerben az adatvédelmi hatásvizsgálat, illetve az adatvédelmi tisztviselő, amelyek szintén meghatározó jelentőségűek.

A GDPR által kialakított jogszabályi környezet biztosítja az adatvédelmi normák egységességét, valamint hatékonyabb eszközökkel őrködik azok betartása felett.

3.3. NIS 2 irányelv

Az általános hatáskörű GDPR rendelkezésein túl az adatvédelem körében irányadó jogforrások között találunk speciális területeket rendező rendeleteket, melyek közül elhanyagolhatatlan jelentőséggel bír a 2023. elején hatályba lépett, az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről rendelkező NIS 2 irányelv.²¹ A NIS rövidítés a *network and information systems* kifejezésre utal, ennek megfelelően a dokumentum célja – elődjéhez, a NIS 1 irányelvhez²² hasonlóan – olyan tagállami intézkedések ösztönzése, melyek a hálózati és információk rendszerek biztonságának magas szintjét biztosítják.²³ A NIS 1 által kitűzött küldetésen túl azonban ez az irányelv közvetlenül célozza a felhasználók és a kiberfenyegetések által érintett további személyek védelmét is, hiszen az információs rendszereket átható, dinamikus technológiai fejlődés rájuk nézve sem veszélytelen.²⁴

Az irányelv jelentősen kiterjesztette a korábbi kiberbiztonsági szabályok tárgyi hatályát, az immár magában foglalja az információs rendszerek és hálózatok széles spektrumát, amelyeket az ún. kritikus és kiemelten kritikus ágazatok működtetése során alkalmaznak. Míg a kritikus ágazatok közé a postai és futárszolgáltatások, a vegyszergyártás, az élelmiszertermelés, a gépek és berendezések gyártása és egyebek mellett a kutatás területe tartozik,²⁵ addig a kiemelten

²¹ 32022L2555 Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv)

²² 32016L1148 Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről

²³ NIS 2 irányelv 1. cikk

²⁴ Niels VANDEZANDE: *Cybersecurity in the EU: How the Nis2-Directive Stacks Up Against its Predecessor*, 2023. 5.

²⁵ NIS 2 irányelv II. melléklet

kritikus területek közé olyan szektorok sorolhatók, mint a légi, vasúti, vízi és közúti szállítás, a banki szolgáltatások, az egészségügy vagy a digitális infrastruktúra.²⁶

A dokumentum jelen dolgozatom szempontjából azért kiemelt jelentőségű, mert személyi hatálya alá azon állami vagy magánszervezetek tartoznak, amelyek közép vállalkozásoknak minősülnek vagy meghaladják a közép vállalkozásokra vonatkozóan előírt felső határértékeket, és amelyek az Unión belül nyújtják szolgáltatásaikat vagy végzik tevékenységeiket,²⁷ ennek megfelelően az irányelv rendelkezései jelentős számban érintik a meghatározott területeken – így Magyarország területén is – működő vállalkozásokat. Emellett a téma relevanciáját adja az a tény is, hogy a technológia fejlődése, így különösen a mesterséges intelligencia prosperitása az eddigieknél szélesebb körben ad lehetőséget kiberbiztonsági támadásokra (ugyanakkor azok kijátszására is), erre figyelemmel szükséges azon rendelkezések elemzése is, amelyek az adatvédelmi kockázatokat, illetve azok mellőzését taglalják.

Az irányelv érintett szervezetekre vonatkozó előírásai között olyan kiberbiztonsági intézkedések bevezetése szerepel, mint a kockázatkezelési eljárások, a biztonsági tesztek és a rendszeres kiberbiztonsági auditok lebonyolítása, melyek közvetlenül járulhatnak hozzá az adatok sérthetetlenségének és hitelességének, valamint az adatkezelésbe vetett bizalom fenntartásához.²⁸

Összességében megállapítható, hogy a NIS 2 irányelv jelentős előrelépést jelent az európai kiberbiztonság megerősítése terén. Bár az irányelv implementálása útján létrejött tagállami jogszabályok betartása a vállalkozások számára kezdetben számottevő terhekkel járhat, hosszú távon hozzájárulhat a kiberbiztonsági kockázatok csökkentéséhez, amelyek napjainkban mind a vállalkozásokat, mind a természetes személyeket fenyegetik. Az irányelv effektíven vállal részt a GDPR által meghatározott keretek cizellálásában, így alkalmas arra, hogy széles körben nyújtson iránymutatást az európai vállalkozásoknak kiberbiztonsági és adatvédelmi gyakorlataik előmozdítása tárgyában.

3.4. Az AI Act vonatkozó rendelkezései

²⁶ NIS 2 irányelv I. melléklet

²⁷ NIS 2 irányelv 2. cikk (1)

²⁸ A NIS irányelvek és az adatvédelem viszonyáról ld. bővebben Dimitra MARKOPOULOU - Vagelis PAPAKONSTANTINOU - Paul DE HERT: *The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation*. Computer Law & Security Review, Volume 35, Issue 6, 2019.

A mesterséges intelligencia embercentrikus megközelítése és etikus fejlődésének elősegítése érdekében az Európai Bizottság 2021 áprilisában terjesztette a Parlament elé a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról szóló javaslatát.²⁹ A javaslattételt a 2020 folyamán elkészült Fehér Könyv előzte meg, melyben egyaránt megfogalmazásra kerültek a szabályozás főbb irányai és a mesterséges intelligencia etikus és biztonságos alkalmazása, mint a rendeletalkotás alapvető célja.³⁰ Az Európai Parlament és a Tanács hangsúlyozta, hogy szükség van egy koherens európai megközelítésre, amely elősegíti a technológiai fejlődést, ezzel egyidejűleg megóvjva az Európai Unió értékeit, így hatékony védelmet biztosít polgárainak az adatvédelem területén is.

Ahogy azt a Fehér Könyv előrevetítette, a 2024. március 13-án az Európai Parlament által elfogadott AI Act, azaz Mesterséges Intelligencia Rendelet kockázatalapú megközelítést alkalmaz.³¹ Ennek révén a Rendelet az MI rendszereket a bennük megtestesülő kockázat mérlegelése alapján négy csoportba sorolja: az elfogadhatatlan kockázattal, a nagy vagy magas kockázattal, a korlátozott kockázattal és a minimális kockázattal járó MI-rendszerek csoportjaiba.³² Az eltérő csoportokkal szemben eltérő követelmények érvényesülnek,³³ ez biztosítja egyrészt a kellő mértékű védelmet, törekszik ugyanakkor a túlszabályozottság elkerülésére.

A Rendelet lényegi elemei közé tartozik, hogy 5. cikke az elfogadhatatlan kockázattal járó csoport keretein belül számtalan tilalmazott gyakorlatot meghatároz, ideértve a célzottan manipulatív vagy megtévesztő technikák alkalmazását a felhasználók viselkedésének torzítása érdekében (mely leírás tulajdonképpen az ún. „*nudging*”-ra utal³⁴), az egyének vagy csoportok társadalmi viselkedésük vagy személyes jellemzőik alapján történő értékelését vagy osztályozását, illetve bizonyos kivételekkel a természetes személyek érzelmeinek kikövetkeztetését.

²⁹ Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete (2024. június 13.) a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról, valamint a 300/2008/EK, a 167/2013/EU, a 168/2013/EU, az (EU) 2018/858, az (EU) 2018/11139 és az (EU) 2019/2144 rendelet, továbbá a 2014/90/EU, az (EU) 2016/797 és az (EU) 2020/1828 irányelv módosításáról (a mesterséges intelligenciáról szóló rendelet)

³⁰ Fehér Könyv a mesterséges intelligenciáról: a kiválóság és a bizalom európai megközelítése, Brüsszel, 2020.2.19.

COM(2020) 65 final https://commission.europa.eu/document/download/d2ec4039-c5be-423a-81ef-b9e44e79825b_hu?filename=commission-white-paper-artificial-intelligence-feb2020_hu.pdf

³¹ Marco ALMADA - Nicolas PETIT: *The EU AI Act: a medley of product safety and fundamental rights?* Robert Schuman Centre for Advanced Studies Research Paper No. 2023/59. 8-10.

³² TÓTH András: *Az Európai Unió Mesterséges Intelligencia Törvényéről*. GJ, 2024/5-6. 3.

³³ Jonas SCHUETT: *Risk Management in the Artificial Intelligence Act*. European Journal of Risk Regulation, 2023. 1-19. 4-5.

³⁴ Lásd: 4.2.

A Rendelet a magas kockázattal járó csoportba tartozó MI-rendszerek, így különösen a közlekedésben, az oktatásban és az egészségügyben használt szoftverek vonatkozásában olyan követelményeket ír elő, mint a kockázatkezelési rendszer létrehozása az MI-rendszer teljes életciklusára vonatkozóan,³⁵ a magas minőségű, valóságot tükröző adatbázisok használata³⁶ vagy az aktivitás naplózása³⁷ a rendszer működésének napi szintű nyomon követhetősége érdekében. A fentiekén túl a GDPR vonatkozó szabályaihoz hasonlóan az AI Act az egyéb csoportok vonatkozásában is előírja, hogy a felhasználók számára világos tájékoztatást kell nyújtani arról, hogy MI-rendszerrel kommunikálnak, és megfelelő információt kell biztosítani a rendszer működéséről és korlátairól.

Szükségszerű rámutatni, hogy a Rendelet, noha közvetlen hatállyal bír az Európai Unió tagállamaiban, meglehetősen absztrakt jellegű, emellett számtalan hiányosságát emeli ki a szakirodalom. EBERS álláspontja szerint a kockázati kategóriák meghatározása pontatlan, a legnagyobb veszéllyel járó területek, így különösen a katonai célra történő alkalmazás vagy az önvezető járművek nem tartoznak a szabályozás hatálya alá annak átfogó jellege ellenére, míg más esetek a szükségesnél jóval szigorúbb megítélés alá esnek.³⁸ A kategóriákat illető következetlenségen túl a szakirodalom arra is rámutat, hogy a Rendelet tudatalatti manipulációra (azaz „*nudging*”-ra) vonatkozó tilalma csak a visszaélések korlátozott körére vonatkozik és nem nyújt kellő védelmet a nem tudatalatti, de manipulatív MI-gyakorlatok ellen.³⁹

Hiányosságai ellenére az AI Act várható hatásai közé tartozik, hogy növeli nemcsak az MI rendszerek biztonságát, de az azokba vetett bizalmat is, mely az adatkezelés szempontjából különösen fontos tényező. Összességében a Rendelet megalkotása korszakalkotó lépésnek tekinthető, hiszen számos olyan rendelkezést tartalmaz, melyek hatékonyan járulhatnak hozzá a mesterséges intelligencia biztonságos és etikus alkalmazásához.

3.5. Nemzetközi deklarációk a téma kapcsán

A fenti jogforrásokon túl mind uniós, mind nemzetközi szinten megalkotásra kerültek a közelmúltban olyan iránymutatások, ajánlások, melyek az MI és a személyes adatok védelmének témáját érintik. Ezek között említhető az Európa Tanács 2019. január 25-én

³⁵ AI Act 9. cikk

³⁶ AI Act 10. cikk

³⁷ AI Act 12. cikk

³⁸ Martin EBERS: *Truly Risk-Based Regulation of Artificial Intelligence – How to Implement the EU’s AI Act*, 2024. 14-15.

³⁹ Mezei KITT: *A mesterséges intelligencia jogi szabályozásának aktuális kérdései az Európai Unióban*. IMR, 2023/1., 53-70.

publikált iránymutatása az MI-ről és a személyes adatok védelméről, mely egyebek mellett rendelkezik az adatkezelés során szem előtt tartandó alapelvekről. ESZTERI tanulmányában azonban megállapítja, hogy a hasonló, nem kötelező jellegű dokumentumok mellett ez az iránymutatás sem ad választ a konkrét kérdésekre, mindössze felhívja a jogalkotók és jogalkalmazók figyelmét a téma fontosságára.⁴⁰

Noha az Európai Unióban alkalmazandó rendelkezésekre számos egyéb nemzetközi jogforrás is hatással van, a további nemzetközi dokumentumok jelen dolgozatom szempontjából kívül esnek a vizsgálat tárgyán.

⁴⁰ ESZTERI, i. m., 676. o.

4. A vállalati szektort érintő kihívások a Big Data és MI korában

A fent említett technológiák alkalmazása során minden eddiginél egyszerűbben és nagyobb mértékben jutnak különféle adatok a vállalkozások birtokába a felhasználókkal kapcsolatban. Noha a jelenség megkívánta azt is, hogy a felhasználók a korábbiaknál nagyobb hajlandóságot mutassanak adataik megosztására, az érintettek nagy része nincs tudatában az adatgyűjtés kockázataival, ennek megfelelően szükséges őket kiemelt védelemben részesíteni.

Ahogy a fentiekben arra utalást tettem, a mesterséges intelligencia napjainkban a digitális világ különféle színterein jelenik meg, számtalan szolgáltatást érintve. Az okoseszközök használatával, különféle szolgáltatások igénybevételével keletkezett adathalmaz felhasználási lehetőségei aggályokat kelthetnek az adatvédelem kapcsán, hiszen sok esetben érzékeny adatok kezelése is megvalósul, amelyekhez korábban nem lehetett hozzáférni vagy legalábbis sokkal bonyolultabb folyamatok eredményeként voltak gyűjthetők. Ezen adatok széles körű elemzése által felvetett kockázatok közé tartozik nem csupán a magánélet megsértése, de a profilalkotás és a potenciális adatlopás veszélye is.⁴¹

Ugyan e kockázatok közvetlenül a felhasználókat fenyegetik, az esetleges bírságok elkerülése, valamint az ügyfelek adatkezelésbe vetett bizalmának fenntartása érdekében az érintett cégek szempontjából is elengedhetetlen figyelmet fordítani a lenti kérdésekre.

4.1. Profilalkotás

A profilalkotás, mely különösen aggályos e körben, gyakorlatilag az egyén viselkedési mintáinak, preferenciáinak és egyéb jellemzőinek elemzése alapján történő kategorizálását jelenti, amely elsődlegesen személyre szabott szolgáltatások nyújtását célozza. Ahogyan arra ZÖDI Zsolt is rámutat, a profilalkotás nem újkeletű jelenség, az 1980-as évek vége óta léteztek ún. CRM (*Customer Relationship Management*) szoftverek, melyek az ügyfelek adatainak, illetve szokásainak elemzésére szolgáltak, illetve már az ezredforduló előtt megjelent az egyediesített marketing, mint irány az üzleti életben.⁴² Napjainkban azonban a megnövekedett adatmennyiségből és számítási kapacitásokból adódóan minden eddiginél több jellemzőt tartalmazó, bonyolult profilok alakíthatóak ki a felhasználókról, így szükségeszerű kiemelt figyelmet fordítani a kérdésre.

⁴¹ Lásd: Sara QUACH - Park THAICHON - Kelly D. MARTIN - Scott WEAVER - Robert W. PALMATIER: *Digital Technologies: Tensions in Privacy and Data*. Journal of the Academy of Marketing Science, 2022. 1299–1323.

⁴² ZÖDI, i. m., 86.

A GDPR meghatározásában, melyet az AI Act is átvett, profilalkotásnak minősül a személyes adatok automatizált kezelésének bármely olyan formája, amely során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére használják, így különösen a munkahelyi teljesítményhez, gazdasági helyzetéhez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzése vagy előrejelzése.⁴³ A fogalommeghatározás jelentős fordulata, hogy mindössze automatizált rendszerek vonatkozásában, tehát azokban az esetekben beszélhetünk profilalkotásról, ha emberi beavatkozás nélkül történik az egyéni jellemzők kiértékelése.

Bár az eljárás olyan előnyökkel járhat, mint a személyre szabott, ezáltal élvezhetőbb hirdetések és a jobb felhasználói élmény, komoly veszélyeket is hordoz magában, ugyanis az elkészített profilok egyebek mellett diszkriminatív gyakorlatokhoz vezethetnek. Ennek a magyarázatára szolgáló legalkalmasabb példa talán az az eset, amikor egy vállalkozásnál az ügyfélszolgálati telefonhívásokat mesterséges intelligencia alkalmazásával bonyolítják le, ami olyan körülményeket is monitorozhat, mint az ügyfél hangneme vagy szóhasználata, az így gyűjtött adatok pedig, amennyiben az adatkezelő visszaél azokkal, a többi ügyféltől eltérő bánásmódra is lehetőséget adhatnak, diszkriminációt eredményezhetnek az egyes fogyasztóknak nyújtott szolgáltatás minőségében vagy árában.

Ennek kapcsán szükséges kiemelni, hogy a GDPR 22. cikke alapján 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 jelentős mértékben érintené. Figyelemmel arra, hogy ez a rendelkezés csupán a kizárólag automatizált adatkezelésen alapuló döntésekre terjed ki, és nem érinti azokat, amelyekben – bármilyen csekély mértékben is, de – emberi közreműködés is megjelenik, a későbbiekben problémát jelenthetnek azok az esetek, amikor a jogszabályi rendelkezések megkerülése érdekében az adatkezelők csupán látszólagosan alkalmaznak emberi beavatkozást a döntéshozatal során.⁴⁴ Fontos megemlíteni, hogy az ilyen eljárások a legtöbb esetben olyan nagy mértékű tényező mérlegelésével zajlanak, ami a folyamatot emberek számára átláthatatlanná vagy legalábbis nehezen értelmezhetővé teszi, ennek megfelelően nem lenne életszerű a hétköznapi felhasználóktól elvárni, hogy e kockázatokat önállóan kiszűrjék, azokat mérlegeljék, így

⁴³ GDPR 4. cikk 4.

⁴⁴ Tal ZARSKY: *Incompatible: The GDPR in the Age of Big Data*. Seton Hall Law Review, Vol. 47, No. 4(2), 2017. 1016-1017.

álláspontom szerint bírói gyakorlatnak szükséges kimunkálnia azokat a jogelveket, amelyek irányadóak lehetnek ebben a problémakörben is, rendezve az ezzel kapcsolatban felmerülő kérdéseket is.

Míg a GDPR a fentiekben rögzítetteknek megfelelően rendelkezik a profilalkotásról, az AI Act sem tartalmaz teljes körű tilalmat erre vonatkozóan, csupán meghatároz olyan gyakorlatokat, amelyek elfogadhatatlan kockázatokat jelentenek, mint a természetes személyek értékelésének vagy osztályozásának céljából történő, diszkriminációhoz vezető profilalkotás. Noha ez a megközelítés egyensúlyt tükröz az MI hasznos célú alkalmazásának lehetővé tétele és az egyének alapvető jogainak védelme között, a rendelkezésekkel kapcsolatban kérdéses, hogy azok hogyan érvényesülnek majd a gyakorlatban. Ebben a vonatkozásban különös figyelmet szükséges szentelni annak is, hogy jelenleg meglehetősen körülményes ellenőrizni az algoritmusok működését. Mindezekre tekintettel álláspontom szerint olyan európai, illetve tagállami szintű hatóságokra lenne szükség, amelyek hatékonyan felügyelik a normák betartását.

4.2. Predikciók, „nudging”

A vállalatok által végzett adatgyűjtés és elemzés lehetőséget biztosít olyan, akár alaptalan predikciókra, melyek számos, mélyen gyökerező adatvédelmi és etikai kockázatot hordoznak magukban. Példaként említendő, hogy 2012-ben a Target nevű amerikai üzletlánc a fogyasztók vásárlási adatainak elemzése révén képes volt „megjósolni”, hogy egyes nők terhesek-e, még mielőtt ezt az információt ők maguk nyilvánossá tették volna.⁴⁵ A Target adatkutatói a vásárlói viselkedés mintázatait vizsgálták, különösen azokat az árucikkeket, amelyeket a nők gyakran vásárolnak a terhesség korai szakaszában, így például vitaminkészítményeket vagy illatanyagmentes termékeket. A személyre szabott marketingstratégia kialakítása céljából megvalósított ilyen jellegű adatgyűjtés sok esetben súlyosan sérti az egyének magánélethez való jogát, ami rávilágít arra, hogy a Big Data predikciók alkalmazása során elengedhetetlen a szigorú jogi szabályozás, amely biztosítja a diszkriminációmentességet minden érintett számára.

A szakirodalom lényeges problémaként említi továbbá a predikciókkal kapcsolatban, hogy az ezeken alapuló eljárások bizonyos helyzetekben gyakorlatilag megfosztják az egyént önálló

⁴⁵ Charles DUHIGG: *Psst, You In Aisle 5*. New York Times, 2012. február 19., 30.

döntési képességétől.⁴⁶ RICHARDS és KING is rámutat a Big Data morális vetülete kapcsán, hogy szükségszerű figyelembe venni az identitás veszélyeztetésének eshetőségét. A szerzők által „*identitás paradoxonnak*” nevezett jelenség szerint noha a Big Data célja éppen az identifikáció, fenyegetést is jelent az identitásra, hiszen a predikciók, következtetések magukban hordozzák azt a veszélyt, hogy átveszik az uralmat az egyén felett irányított ajánlások, személyre szabott szűrők, egyéniesett javaslatok révén.⁴⁷

ZÖDI Zsolt szerint a helyes predikciót csak egyetlen hajszál választja el a manipulációtól,⁴⁸ amely állítást tökéletesen alátámasztják a közösségi portálok algoritmusai, melyek a felhasználók korábbi preferenciái alapján képesek a számukra vonzó tartalmakat kínálni nekik, lehetőségük van azonban ezzel az egyéni döntéseket is befolyásolni. Noha a felhasználók efféle „terelgetése” – melyet a külföldi szakirodalom „*nudging*”-nak nevez⁴⁹ – a legtöbbször csupán bizonyos opciók kizárásból áll, könnyedén alkalmas lehet egyebek mellett arra, hogy egyfajta monotonitást kialakítva kizárja a kritikus gondolkodást és jelentősen leszűkítse az egyének látásmódját. Amennyiben például a közösségi médiában egy felhasználó korábbi keresései és interakció alapján az algoritmus egyoldalúan jeleníti meg számára a politikai tartalmakat, így különösen egy adott politikai ideológia vagy konkrét párt által közzétett bejegyzéseket, az a felhasználó meglévő politikai nézeteinek elmélyüléséhez vezethet, elzárva őt az ellenkező véleményekkel való találkozás lehetőségétől. A szerző álláspontjával egyetértve lényegesnek tartom kiemelni, hogy az említett befolyásolás hosszú távon komoly társadalmi hatásokat eredményezhet, hiszen nemcsak az egyéni döntéseket terelheti egy meghatározott irányba, hanem a kritikus gondolkodást kollektív szinten is jelentősen gyengítheti.

Meg kell jegyezni, hogy a 3.4. pontban tárgyalt AI Act tilalmazza az olyan manipulatív, megtévesztő magatartásokat, melyek azt eredményezik, hogy egyes személyek olyan döntést hozzanak, amelyet egyébként nem hoztak volna meg, és oly módon, hogy az az érintett személyeknek jelentős károsodást okoz vagy ésszerű valószínűséggel okozhat.⁵⁰ Álláspontom szerint a Rendelet megfogalmazása nem pontos, különös tekintettel a bizonyítási nehézségekre annak vonatkozásában, hogy a felhasználó az adott döntést az adott helyzetben ténylegesen meghozta-e, vagy arra őt az algoritmus által kínált opciók készítették. A jelenlegi technológiai

⁴⁶ Lokke MOEREL - Corien PRINS: *Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things*, 2016. 30.

⁴⁷ Neil M. RICHARDS – Jonathan KING: *Three Paradoxes of Big Data*. Stanford Law Review Online, 2013. 43.

⁴⁸ ZÖDI, i. m., 92.

⁴⁹ Cass R. SUNSTEIN: *The Ethics of Nudging*, 2014. 2.

⁵⁰ AI Act 5. cikk (1)

és jogi keretek között hiányoznak azok az eszközök és módszerek, amelyek objektíven és egyértelműen bizonyítani tudnák, hogy az algoritmus milyen mértékben hatott a felhasználói döntéshozatalra.

Ki kell emelni továbbá, hogy a jogforrás szövegének pontatlanságából adódóan közel sem egyértelmű a különbségtétel a tiltott technikák és a tilalom alá nem tartozó reklámok között, ami jelentős mértékben megnehezítheti mind a jogkövetést, mind annak felügyeletét. Emellett a jogszabályi rendelkezéseken túl szükségszerű a tilalom érvényesülését a gyakorlatban is hatékonyan biztosítani, melynek érdekében elsődleges jelentőségű egyebek mellett a megfelelő hatóságok létrehozása, illetve az adatkezelők tájékoztatása kötelezettségeikről.

4.3. A visszanevesíthetőség problémája

A fentiekén túl kiemelendő, hogy jelentős aggályt jelent az ún. visszanevesíthetőség vagy re-identifikáció. A fogalom arra utal, hogy az eredetileg anonimként gyűjtött adatokból később az egyének személyazonossága visszafejthetővé válik, hiszen az egyes adathalmazok hiába tartalmazzanak anonim jellegű adatokat, ha más, nyilvános adatbázisokkal összevetve az adatkezelőknek lehetőségük nyílik az érzékeny adatokhoz való hozzáférésre.⁵¹ Ennek vonatkozásában számottevő problémát jelent, hogy az érintetteknek gyakran nincs tudomásuk ennek a lehetőségéről.

Ebből a nehezen elkerülhető jelenségből következik, hogy újra kell gondolnunk a célhoz kötöttséget, mint az adatvédelem egyik fő alapelvét,⁵² különös tekintettel arra, hogy sok esetben az adatgyűjtéskor még nem is ismertek a célok, amelyek érdekében az adatok felhasználásra kerülnek majd.⁵³

4.4. Transzparencia hiánya

A gépi tanulással kapcsolatos aggodalmak között gyakran felmerülő, és nem kizárólag az adatvédelem terén jelentős kérdés az a „fekete doboz effektusnak” is nevezett dilemma,⁵⁴ mely

⁵¹ Paul Ohm: *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*. UCLA Law Review, Vol. 57., 2010. 1701-1706.

⁵² ZARSKY, i. m., 1007.

⁵³ KESERŰ, i. m., 22.

⁵⁴ Fontos megjegyezni, hogy téves az a feltételezés, miszerint az MI működési mechanizmusát lehetetlen átlátni. Sokkal inkább arról van szó, hogy a kérdés vizsgálata beláthatatlanul sok időbe telne és hatalmas anyagi költségekkel járna, így tulajdonképpen nem átláthatatlanságról, mindössze a transzparencia kapcsán tapasztalt rendkívüli nehézségekről beszélhetünk.

szerint rendkívül nehéz átlátni, miért és hogyan jutott egy adott eredményre egy gépi tanulást alkalmazó modell.⁵⁵

4.4.1. Érintettek tájékoztatása

A transzparencia efféle hiánya az adatvédelemmel kapcsolatban azért különösen aggályos, mert a GDPR 5. cikk (1) bekezdése kifejezetten előírja, hogy az adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni. Nehezen teljesíthetők továbbá a GDPR 15. cikk (1) bekezdés h) pontjában foglalt kötelezettségek, amelyek az alkalmazott logikáról való tájékoztatást írják elő.⁵⁶ Emellett az AI Act 13. cikke írja elő az MI-rendszerek fejlesztői számára, hogy a felhasználókat olyan módon kell tájékoztatni a rendszerek működéséről, hogy számukra is értelmezhető legyen a rendszer kimenete, így biztosítható legyen annak használata. Figyelemmel arra, hogy algoritmusok komplexitása miatt gyakran maguk a fejlesztők sem képesek teljes mértékben átlátni a döntéshozatal minden lépését, felvetül a kérdés, hogy hogyan várható el az érintett megfelelő tájékoztatása.

Szükséges felismerni továbbá, hogy nem elvárható a hétköznapi felhasználóktól, hogy a neurális hálózatok működését átlássák, ezen ismeretek hiányában pedig semmilyen egyéb tájékoztatás nem lehet teljes körű. ESZTERI Dániel ezzel kapcsolatban kiemeli, hogy egyfajta köztes megoldásra kell törekedni az érintettek tájékoztatása kapcsán, ugyanis nem elegendő, ha az adatkezelő csupán általánosságban jelzi, hogy egy neurális hálózaton alapuló rendszert alkalmaz, hiszen ez az érintett számára aligha teszi világossá, hogy személyes adatait hogyan kezelik. Ezzel szemben ESZTERI rámutat arra is, hogy az érintett rendelkezésére bocsátott magyarázat túl részletes volta a legtöbb esetben lerontja a tájékoztatás közérthetőségét és hátráltatja annak befogadását.⁵⁷

Ira S. RUBINSTEIN utal ezzel összefüggésben azon dilemmára is, hogy az adatbányászatot alkalmazó vállalkozások gyakran képtelenek előzetes és kielégítő tájékoztatást nyújtani az

⁵⁵ Yavar BATHAE: *The Artificial Intelligence Black Box and the Failure of Intent and Causation*. Harvard Journal of Law & Technology Volume 31, Number 2, 2018. 906-921.; Jarek GRYZ - Marcin ROJSZCZAK: *Black box algorithms and the rights of individuals: no easy solution to the "explainability" problem*. Internet Policy Review, 10(2), 2021.

⁵⁶ Bryan CASEY - Ashkan FARHANGI - Roland VOGL: *Rethinking Explainable Machines: The GDPR's „Right to Explanation” Debate and the Rise of Algorithmic Audits in Enterprise*. Berkeley Technology Law Journal, 2019.

⁵⁷ ESZTERI, i. m., 680.

érintetteknek, mivel maguk sem rendelkeznek pontos ismeretekkel arról, hogy milyen összefüggéseket tárhatnak fel.⁵⁸

A jelenséggel kapcsolatban több szerző is megjegyzi ugyanakkor, hogy az emberi agy működése hasonlóképpen titokzatos, sőt, jelenleg csupán felületes ismereteink vannak az emberi elme működési mechanizmusairól. Ezzel szemben az általunk létrehozott MI algoritmusok esetében legalább tisztában vagyunk azok működési elveivel, még ha nem is mindig tudjuk megmagyarázni az egyes döntések pontos indokait.⁵⁹ Ennek megfelelően egyes szerzők arra az álláspontra helyezkednek, hogy a megfelelő garanciák megléte mellett tulajdonképpen nem problémás az efféle átláthatatlanság.

4.4.2. Szerzői jogi kérdések

A technológiai korlátokon túl szükséges rámutatni a téma szerzői jogi vetületére. A szoftverek működésébe való betekintés biztosítása ugyanis a rájuk kiterjedő szerzői jogi szabályozás értelmében gyakran nem valósítható meg jogszerűen. A mesterséges intelligencia tanítása során felhasznált adatkészletek szerzői jogi védelem alatt álló szövegeket vagy egyéb fájlokat tartalmazhatnak, így azok jogszerű felhasználása érdekében a jogtulajdonosok engedélye szükséges, vagy törvénynek kell kifejezetten engedélyeznie a felhasználást.⁶⁰

Ennek megfelelően a szabályozás ezen iránya jelentős kihívások elé állítja azokat a vállalkozásokat, amelyek bonyolult algoritmusokon alapuló szoftvereket működtetnek. Ennek kapcsán tekintettel kell lenni arra a tényre is, hogy a működési mechanizmusra vonatkozó részletek szerzői jogi védelemtől függetlenül üzleti titoknak minősülhetnek, illetve nyilvánosságra hozataluk korlátozhatja ezen vállalkozások versenyelőnyét a piacon.

4.4.3. A felelősséggel kapcsolatos dilemma

A fekete doboz-effektusból adódóan kérdésként merülhet fel az is, hogy egy esetleges adatvédelmi incidens esetén kit terhel a felelősség figyelemmel arra, hogy a fentiekben kifejtetteknek megfelelően gyakran nehéz meghatározni, hogy az adatgyűjtés, az adatkezelés,

⁵⁸ Ira S. RUBINSTEIN: *Big Data: The End of Privacy or a New Beginning?* International Data Privacy Law, Volume 3, Issue 2, May 2013. 78.

⁵⁹ Bartosz BROŻEK - Michał FURMAN - Marek JAKUBIEC - Bartłomiej KUCHARZYK: *The black box problem revisited. Real and imaginary challenges for automated legal decision making.* Artificial Intelligence and Law, 2024. 430.; Andrea BONEZZI – Massimiliano OSTINELLI - Johann MELZNER: *The human black-box: the illusion of understanding human better than algorithmic decision-making.* Journal of Experimental Psychology: General 151(9), 2022. 2250–2258.

⁶⁰ Giovanni SARTOR - Francesca LAGIOIA - Giuseppe CONTISSA: *The Use of Copyrighted Works by AI Systems: Art Works in the Data Mill*, 2018. 13-14.

illetve az MI-szoftverek működtetése a jogszabályoknak megfelelően történt-e. Ezekben az esetekben az adatvédelmi incidens során keletkező károk felmérése és az érintettek tájékoztatása is összetett feladat, hiszen amennyiben az adatkezelési folyamatok átláthatatlanok, az adatkezelők nem feltétlenül rendelkeznek elegendő információval ahhoz, hogy pontosan meghatározzák, milyen mértékben sérült az érintettek magánélete és milyen lépéseket kell tenniük a kár enyhítése érdekében.

4.4.4. Kockázatelemzés, biztonsági intézkedések

A fentiekén túl kötelezettséggént jelentkezik az adatkezelővel és az adatfeldolgozóval szemben, hogy az adatkezelés sajátosságai és egyéb körülmények figyelembevétele mellett megfelelő technikai és szervezési intézkedéseket hajtson végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja.⁶¹ Fontos azonban megjegyezni, hogy az algoritmusok működésének átláthatatlansága sok esetben korlátozhatja a kockázatok felmérését és a megfelelő biztonsági intézkedések foganatosítását, ami nem csupán az adatkezeléssel érintettek jogainak megsértéséhez vezethet, de a vállalkozásokra is olyan terheket róhat, mint különféle költséges eljárások lebonyolítása, vagy valamely mulasztás miatt az esetlegesen kiszabott bírságok megfizetése.

4.5. Diszkriminatív gyakorlatok

Nem elhanyagolható kockázata a Big Data és az MI együttes hasznosításának a megkülönböztetés alkalmazása. Az MI-technológia egyre szorosabban integrálódik mindennapi életünkbe, így az elsődlegesen a prediktív analitikában és a fogyasztói reklámokban megjelenő elfogultság egyre nagyobb teret kap.⁶² Halmozottan igaz ez abban az esetben, amikor az algoritmusok bizonyos, a valóságban jelentéktelen tényezők kiemelésével hoznak döntéseket. KESERŰ Barna Arnold a következő példával élt ennek kapcsán: egy hipotetikus MI-nak egy olyan adathalmazt adunk, ahol 1000 hitelbírálati kérelemből 450-et elutasítanak, ebből a 450 jelentkezőből pedig 200 szemüveges. Ebből az adathalmazból a szoftver azt a következtetést vonhatja le, hogy a szemüveg kockázati tényezőnek minősül, ezért elkezdi negatívumként értékelni, így kialakulhat egy olyan gyakorlat, ahol a szemüvegesek nehezebben kaphatnak hitelt, mint azok, akik nem viselnek szemüveget.⁶³

⁶¹ GDPR 32. cikk

⁶² Bita AMANI: *AI and Equality by Design*. Artificial Intelligence and the Law in Canada, 2021. 3-4.

⁶³ KESERŰ, i. m., 20.

Egy másik példa, hogy a hitelhez való hozzáférés lehetőségét korlátozza az a gyakorlat, mely során a pénzügyi szolgáltatást kínáló vállalkozások hirdetéseikkel jobb anyagi helyzetben lévő fogyasztókat célozzák meg a kockázatok elkerülése érdekében, míg a kisebb jövedelműek nem értesülnek ugyanezen hitelajánlatokról.⁶⁴

Ezzel kapcsolatban megjegyzendő, hogy az MI szoftverek a gépi tanulás működési mechanizmusából adódóan könnyedén kerülhetnek egyfajta spirálba, amely felerősítheti a meglévő társadalmi előítéleteket és diszkriminatív mintázatokat.⁶⁵ Amennyiben ugyanis az algoritmusok olyan adatokat használnak fel a tanulási folyamat során, amelyek már tartalmazznak előítéleteket, ezen előítéletek továbbra is fennmaradnak és gyarapodnak, súlyosbítva a társadalmi egyenlőtlenségeket.⁶⁶

Noha az Európai Unió Mesterséges Intelligencia Rendelete jelentős előrelépést hozott ezen a területen,⁶⁷ említést kell tenni az olyan hiányosságokról, mint a szenzitív biometrikus adatok kezelése vagy az emberi érzelmek monitorozásának kérdése, melyek bizonyos esetekben, így például orvosi alkalmazás céljából engedélyezettek. A Rendeletben megjelenő szigorú tilalmak ellenére nem zárhatóak ki teljesen a visszaélések, ami további szabályozást tesz szükségessé az Európai Unió részéről annak érdekében, hogy az adatkezelők és az adatkezeléssel érintett személyek teljes körű védelmet élvezhessenek.

4.6. Adattípusok összemosódása

Noha a GDPR 9. cikke szerint főszabály szerint bizonyos, így többek között a faji vagy etnikai származásra, vallási vagy világnézeti meggyőződésre, vagy a szexuális irányultságra vonatkozó személyes adatok kezelése tilos meghatározott kivételek mellett, KESERŰ Barna Arnold rámutat, hogy a Big Data alapú adatelemzés révén ezen különleges személyes adatok könnyedén vegyülhetnek az általános személyes adatokkal. A szerző példája alapján pusztán GPS-adatokról szinte teljes bizonyossággal tehetünk megállapítást egy adott személy vallási meggyőződését illetően, ha minden vasárnap templomban tartózkodik.⁶⁸ Emellett érdemes megemlíteni, hogy a vásárlási szokásokból könnyedén következtethetünk egészségügyi

⁶⁴ Kate CRAWFORD – Jason SCHULTZ: *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*. Boston College Law Review, Vol. 55, No. 93, 2014. 99.

⁶⁵ Ld. még: LUKÁCS Adrienn: *Digitális diszkrimináció és automatizált döntéshozatal, különös tekintettel a munka világára*. MJSZ, 2023/2. 110-111.

⁶⁶ Solon BAROCAS - Andrew D. SELBST: *Big Data's Disparate Impact*. California Law Review Vol. 104, No. 2. 681.

⁶⁷ Lásd: 3.4. pont

⁶⁸ KESERŰ, i. m., 24.

adatokra, kijelenthető például, hogy a laktózmentes termékek vásárlása laktózintoleranciára utal.

Ez a jelenség jelentős terhet ró az adatkezeléssel érintett vállalkozásokra, hiszen a jogszabályi megfelelés érdekében különös figyelmet kell fordítaniuk e speciális adatok kezelésének elkerülésére, ami sokszor problémás, hiszen a fenti példa alapján azok sokszor általános, jogszerűen kezelhető személyes adatokból származnak.

Mindezeken túl szólni kell arról is, hogy idővel egyre több adat esik ebbe a speciális kategóriába, ezzel pedig elhalványul annak relevanciája, hogy kiemelt figyelmet szenteljünk ezeknek. Ez azt jelenti, hogy végső soron valójában nem tudunk majd különbséget tenni a különleges és az általános adatok kezelése között,⁶⁹ így a szabályozás célja, amely a különleges kategóriák különleges bánásmódját hivatott biztosítani, megghiúsul.⁷⁰

⁶⁹ ZARSKY, i. m., 2015.

⁷⁰ MOEREL - PRINS, i. m., 11.

5. Jövőbeli irányok

A fentiekben megfogalmazott dilemmák egyrészt a meghaladott jogszabályi keretek, másrészt az etikátlan adatkezelői és fejlesztői gyakorlatok közé szerveződnek.

Korábban igyekeztem rámutatni, hogy az MI és Big Data összekapcsolása révén megvalósított adatgyűjtés és -felhasználás során realizált előnyök jelentőségét gyakran alábecsülik a potenciális veszélyekkel szemben, így szükséges a jogszabályi háttér olyan irányú módosítása, mely lehetőséget biztosít az esetleges visszaélések kiküszöbölésére. A mesterséges intelligencia és a nagy adathalmazok kezelésével kapcsolatos fenti kockázatok enyhítésére és a felmerülő etikai kihívások kezelésére sajátos, technológiaorientált szabályozásra van szükség, lehetővé téve az egyediesítést a tagállami technológia-használat specifikumait figyelembe véve. Gyakori jelenség ugyanis, hogy az új adattípusok vagy adatkezelési gyakorlatok miatt betarthatatlanná vagy szükségtelenné válnak a jogi normák. Az Európai Unió adatvédelmi dokumentumai nem nyújtanak egyértelmű választ a Big Data és az MI alkalmazásának vonatkozásában felmerült kérdésekre, és véleményem szerint a szabályozás több ponton mellőzi a gyakorlatiasságot. E probléma feloldását az Európai Unió megkísérelte ugyan az AI Act keretei között, de álláspontom szerint további szegmensek vonatkozásában is indokolt lenne a szabályozás kiterjesztése. Ennek a szemléltetésére önmagában elegendő példa, hogy a GDPR azon rendelkezése, hogy „*az adatok körét pedig a célhoz szükséges minimumra kell korlátozni*”,⁷¹ nehezen értelmezhető a Big Data kontextusában.⁷²

Mivel a Big Data és az MI használata számos, a fentiekben kifejtett erkölcsi kérdést is felvet, így különösen a profilalkotás vagy a diszkrimináció problémáját, elvi jelentőségű lenne továbbá a morális irányok meghatározása, a határok meghúzása e technológiák alkalmazása vonatkozásában.⁷³ Noha erre az Európai Unió már a GDPR megalkotásával kísérletet tett, a jelenlegi szabályozás összeférhetetlen a Big Data által teremtett adatkörnyezettel.⁷⁴ Ezt követően, még az AI Act elfogadásával is számtalan olyan fontos terület maradt érdemi szabályozás nélkül, mint például a „*nudging*”, illetve a legtöbb esetben tisztázatlan a felelősség kérdése a dolgozatom 4.4.3. pontjában meghatározott esetkörök tekintetében. E kérdések

⁷¹ GDPR Preambulum (39)

⁷² RUBINSTEIN, i. m., 78.

⁷³ A mesterséges intelligencia szabályozásával kapcsolatos erkölcsi-etikai iránymutatások kidolgozásával összefüggésben ld. bővebben Stefán Ibolya: *A mesterséges intelligencia jogi szabályozásának egyes kérdései*. MJSZ, 2020. 3. Különszám, 184-191.

⁷⁴ ZARSKY, i. m., 996.; Alexandr KESA - Tanel KERIKMÄE: *Artificial Intelligence and the GDPR: Inevitable Nemeses?*, TalTech Journal of European Studies 10, no. 3, 2020. 71.

kapcsán olyan szabályozásra lenne szükség, mely sem az adatkezelők, sem az adatkezeléssel érintettek számára nem okoz kárt, és betartása sem jár aránytalanul nagy költségekkel.

A fentiek alapján az erkölcsi irányok meghatározásának egyik ága a természetes személyek védelmét célozza. Annak ellenére, hogy egyes nézőpontok szerint a Big Data korában a személyes adatok áramlásának korlátozhatatlan volta miatt egyre kevésbé lehet felügyelni a privát szféra védelmét,⁷⁵ Neil M. RICHARDS és Jonathan KING szerint elsődlegesen éppen ez a kontrollálhatatlanság ad okot arra, hogy az adatvédelem területe gyökeres változáson menjen keresztül.⁷⁶ Ugyan a dolgozatom 3. fejezetében megvizsgált jogforrásokban elsősorban elvi szinten körvonalazódnak a témával kapcsolatos olyan erkölcsi kérdések, mint az egyének magánéletének tiszteletben tartása,⁷⁷ álláspontom szerint szükségeszerű e dimenziók részletesebb kidolgozása, különös tekintettel arra, hogy az adatgyűjtés és elemzés mértéke exponenciálisan gyarapszik. Mindezek mellett, valamint ezzel párhuzamosan szükségeszerű a magánszféra védelmének megerősítése is.

Mindez, ahogyan arra RICHARDS és KING is utal, együtt jár az információ bizalmas jellegének tiszteletben tartásával, hiszen az elmúlt évtizedekben a magánélet egyfajta „bináris” jelleget öltött, és sokakban tévesen az az elképzelés alakult ki, hogy az adatok vagy privát jellegűek maradnak, vagy megosztás által nyilvánossá válnak. A szerzők rámutatnak arra, hogy egyes információk egyfajta köztes állapotban vannak, azaz annak ellenére, hogy az adat tulajdonosán kívül más számára is elérhető, nem lehet azt korlátlanul felhasználni, mert ettől függetlenül nem veszti el bizalmi jellegét.⁷⁸ Ennek rögzítése és a tudatosság növelése mind az adatkezelők, mind a felhasználók tekintetében létfontosságú, ennek érdekében pedig elengedhetetlen a jogalkotó szervek és a piaci szereplők közreműködése.

Ezen túlmenően a magánélet védelme érdekében olyan jogintézmények bevezetésére van szükség, amelyek effektíven segítik elő többek között a visszanevesíthetőséggel kapcsolatos dilemmák megoldását vagy a diszkriminatív gyakorlatok kizárását. Fontos megjegyezni, hogy a visszaélések sokszor nehezen kiszűrhetőek, ezáltal szankcionálásuk sem mentes a

⁷⁵ KESERŐ, i. m., 15.

⁷⁶ Neil M. RICHARDS – Jonathan KING: *Big Data Ethics*. Wake Forest Law Review, 2014. 395. o.

⁷⁷ Ezzel kapcsolatban megjegyzendő, hogy az Európai Unió magas szintű független szakértői csoportja 2019 áprilisában publikálta a „Etikai iránymutatás a megbízható mesterséges intelligenciára vonatkozóan” című dokumentumát, melyben megfogalmazta, hogy az MI megbízhatósága, így a jogsértések elkerülése a jogszerűség, az etikusság és a stabilitás egyidejű érvényesülése esetén biztosítható. Forrás: European Commission: Directorate-General for Communications Networks, Content and Technology, *Etikai iránymutatás a megbízható mesterséges intelligenciára vonatkozóan*, Publications Office, 2019, <https://data.europa.eu/doi/10.2759/428483>

⁷⁸ RICHARDS – KING, i. m. 2014, 396.

nehézségektől, erre figyelemmel még inkább indokolt egy olyan szabályozás kialakítása, amelynek betartása az adatkezelők érdekeit is szolgálja.

A fentiekkel kapcsolatban megjegyzendő azonban, hogy a túlszabályozás elkerülése érdekében szem előtt kell tartani, hogy az adatgyűjtés a felhasználókra nézve gyakran valós kockázatokat nem tartogat magában, illetve az azok hasznosításával elérhető előnyök esetlegesen ellensúlyozhatják a felmerülő hátrányokat. Ez jelentős kihívások elé állítja a jogalkotót, ugyanis széles körű lehetőséget kínál annak vonatkozásában, hogy „merre billenjen a mérleg”. E folyamat központi kérdése, hogy a szabályozás miként támogathatja az innovációt, miközben biztosítja az átláthatóságot és az érintett adatvédelemhez való jogának tiszteletben tartását egyaránt.

Nem elhanyagolható kockázatot jelent továbbá, hogy az adatkezelés számos esetben a magánélethez való jog előmozdítására és az identitás védelmére való tekintet nélkül, mindössze a jogszabályoknak való megfelelést szem előtt tartva történik. Erre figyelemmel álláspontom szerint mind az MI-szoftverek fejlesztőinek, mind az adatkezelést végző gazdasági társaságoknak fokozott felelősséget kell vállalniuk adatkezelési gyakorlataik etikusabbá tételéért. Az adatvédelem nem merülhet ki a jogszabályi előírásoknak való megfelelésben, az adatkezelés során proaktív megközelítést kell alkalmazni, mely magában foglalja az adatkezelés átláthatóságát, a felhasználók jogainak tiszteletben tartását és az adatkezelési folyamatok ellenőrizhetőségét biztosító belső irányelvek kialakítását.

5.1. Adatok megfontoltabb szelektálása, validálása

A fenti kockázatok kezelésének érdekében megvalósítandó stratégia egyik alappillére a felhasznált adatok minőségének javítása, ideértve mind a mesterséges intelligencia-modellek tanításánál alkalmazott, mind a konkrét adatkezelési folyamatok során igénybe vett adathalmazokat. Figyelemmel arra ugyanis, hogy a döntéshozatal teljes egészében ezen adatokra épül, egyértelmű, hogy a bemeneti adatok hibái, hiányosságai vagy torzításai közvetlenül befolyásolják az *output*-ot. Az adatminőség ellenőrzése növelheti egyrészt a modellek döntéseinek megbízhatóságát és pontosságát, másrészt hozzájárulhat a GDPR és az AI Act adattakarékosságra⁷⁹ és transzparenciára⁸⁰ vonatkozó előírásai betartásához.

⁷⁹ GDPR 5. cikk (1) bekezdés c) pont; AI Act (69) preambulumbekzdés

⁸⁰ GDPR 12. cikk

Emellett a szelektálás, valamint annak esetleges jogszabályi előírások általi ösztönzése elősegítheti a diszkriminatív minták kiszűrését. Ahogyan ugyanis a 4.5. pontban arra rámutattam, gyakori problémaként jelentkeznek a diszkriminatív gyakorlatok, amelyek a különféle nézőpontok alulreprezentáltságából, az adatok változatosságának hiányából adódnak. Ezekre tekintettel szükségesű figyelmet fordítani arra, hogy az algoritmusok minél sokszínűbb, a valóságot tükröző adatkészletekkel dolgozzanak. A reprezentatív adathalmazok alkalmazása nem csupán a vállalkozások érdekét szolgálja, az erre vonatkozó jogszabályi rendelkezések bevezetése alkalmas lenne a diszkrimináció kizárásából adódóan az érintettek jogainak védelmére is. Emellett a megfelelően validált adatok által minimalizálható az adathalmazokba betáplált előítéletek fennmaradásának kockázata, ezzel elkerülve azok „begyűrűződését” a belső szervezetrendszerbe, amely jelenségről szintén szó esett a jelen dolgozatom 4.5. pontjában.

Fontos kiemelni a téma vonatkozásában az adatok hitelességét is, amelynek biztosítása elsősorban olyan technológiai eszközöket igényel, mint például a blokklánc-mechanizmus, illetve már az adatgyűjtési folyamatok során is fontos tekintettel lenni a transzparenciára a visszaélések elkerülése érdekében. Noha a pontosság elvéből adódóan szükségesű biztosítani az adatok naprakészségét és helytállóságát,⁸¹ álláspontom szerint a gyakorlatban nem létesültek megfelelő jogintézmények ezen rendelkezés biztosítására.

Annak ellenére, hogy az AI Act 10. cikkében foglalt, meglehetősen absztrakt rendelkezései jelentős mértékben összezsengenek a fentiekben összegzett irányokkal, meg kell jegyezni, hogy ez a dokumentum elsősorban a nagy kockázatú MI-rendszerekre vonatkozó szabályozást tartalmaz. Figyelemmel arra, hogy a nagy kockázatú MI-rendszerek csoportja viszonylag szűk körű, szükségesű lenne az adatok minőségére vonatkozó kritériumokat további kategóriákra kiterjeszteni.

5.2. Adatvédelmi hatásvizsgálatok

Az adatvédelmi hatásvizsgálat kulcsfontosságú eszköz azon adatkezelések vonatkozásában, amelyek *„valószínűsíthetően magas kockázattal járnak a természetes személyek jogaira és szabadságaira nézve”*.⁸² Ezen esetekben az adatkezelőnek kötelezettsége egy olyan hatásvizsgálat lefolytatása, melynek során körvonalazódik, hogy a tervezett adatkezelési műveletek hogyan érintik a személyes adatok védelmét. A hatásvizsgálatok mélyebb elemzésre

⁸¹ GDPR 5. cikk (1) bekezdés d) pont

⁸² GDPR 35. cikk (1) bekezdés

ösztönözhetik az MI alkalmazóit és fejlesztőit egyaránt, akik így alaposan feltérképezhetik a lehetséges hibákat.⁸³ Az MI és a Big Data fejlődésének köszönhetően azonban szükségessé válhat az adatvédelmi hatásvizsgálatokkal kapcsolatos szabályozás kereteinek kiterjesztése, illetve azok módosítása az alább részletezettek figyelembevételével. A hatásvizsgálatokkal kapcsolatos szemléletváltozás, a jogintézmény rugalmasabb megközelítése mind a jogalkotó, mind az alkalmazók szempontjából alkalmas lehet arra, hogy elmozdítsa az említett szereplők fókuszát a pusztá megfelelésről a problémamegoldás és a fejlesztés irányába.⁸⁴

A hatásvizsgálatokra irányuló javaslat relevanciáját mutatja azt is, hogy az elmúlt években az Egyesült Államok Kongresszusa is tárgyalta az ún. *Algorithmic Accountability Act* (*Algoritmikus Elszámoltathatóság Rendelet*) megalkotásáról, amely az átláthatóság és a felelősségre vonhatóság erősítését szolgálja.⁸⁵ Az *Algorithmic Accountability Act*-javaslatban megjelenik a hatásvizsgálatok (*impact assessment*-ek), azaz a jelenlegi vagy javasolt intézkedések jövőbeli következményeinek azonosítására irányuló vizsgálatok⁸⁶ lefolytatásának előírása.

5.2.1. Eredmények nyilvánossá tétele

NAHMIAS és PEREL kiemelik, hogy bár az adatvédelmi hatásvizsgálatok lefolytatásának kötelezettsége az amerikai törvényjavaslat szabályozásához hasonlóan az adatkezelési tevékenység megkezdése előtti időszakra vonatkozik, a hatásvizsgálat eredményeinek nyilvánosságra hozatala a GDPR szerint nem kötelező, így a szervezetek mérlegelésére van bízva.⁸⁷ Ez a szabályozási hiányosság nem csupán jelentősen korlátozhatja a nyilvánosság számára a fontos információkhoz való hozzáférést, a vizsgálatok formálissá válását is eredményezheti, ezzel gyengítve a GDPR által kitűzött, az elszámoltathatóságra irányuló célt.

5.2.2. Független szakértők bevonása

Az adatvédelmi hatásvizsgálatok során az adatkezelő szervén kívül álló, független szakértők bevonásának előírása effektíven segíthetné elő az adatvédelmi kockázatok elemzéséhez szükséges objektivitás és szakmaiság biztosítását. A kvalifikált szakértők véleményének integrálása az adatgyűjtésbe lehetővé teszi, hogy a hatásvizsgálati folyamat ne csak a szabályozási megfelelésre összpontosítson, hanem a technológiai innováció által generált

⁸³ Sonia KATYAL: *Private Accountability in the Age of Artificial Intelligence*. 66 UCLA L. REV. 54, 2019. 112.

⁸⁴ Yifat NAHMIAS - Maayan PEREL: *The Oversight of Content Moderation by AI: Impact Assessments and Their Limitations*. Harvard Journal on Legislation, Vol. 58, No. 1, 2021. 15.

⁸⁵ NAHMIAS – PEREL, i. m., 20-23.

⁸⁶ www.iaia.org

⁸⁷ NAHMIAS – PEREL, i. m., 21.; KATYAL, 2019. 115-116.

adatkezelési kihívásokra is kiterjedjen. Mindezek által pontosabb kép kapható arról, hogy az adatkezelés során mely tevékenységek, területek lehetnek aggályosak a felhasználók jogaira nézve.

5.3. Automatikus hatásvizsgálat

Hosszútávon figyelemreméltó előrelépést jelenthet az adatkezelés terén az automatikus hatásvizsgálati szoftverek alkalmazása. Ezen eszközök bevezetése nem csupán a hatékonyság növelését szolgálná, hanem hozzájárulna a pontosság és megbízhatóság fokozásához is, valamint az adatvédelmi gyakorlatok egységesítéséhez, csökkentve ezzel az emberi hibák előfordulásának valószínűségét. Ezen felül a folyamatos monitorozás lehetősége, amit ezek az automatizált rendszerek kínálnak, alapvetően fontos az adatvédelmi kockázatok azonnali kezelése és a szükséges korrekciók gyors végrehajtása szempontjából, így ilyen téren is forradalmi változást hozhatna az adatkezelés minőségében. Mindezek alapján az automatizált hatásvizsgálati szoftverek és egyéb eszközök bevezetése elengedhetetlen lépés lenne az adatvédelmi gyakorlatok modernizálása felé vezető úton.

5.4. Átláthatóság növelése

Álláspontom szerint a legfontosabb célkitűzések egyike a transzparencia biztosítása, hiszen ez elengedhetetlenül szükséges a felhasználók védelmének biztosításához és az adatkezelésbe vetett bizalom fenntartásához. Fontos kiemelni, hogy az átláthatóság nagymértékben szolgálja az adatkezelők érdekét is, hiszen ha a felhasználók meg vannak győződve az adatgyűjtés biztonságáról, hajlamosabbak több adatot megosztani, ami előmozdíthatja a fogyasztói igények és preferenciák pontosabb megértését és kielégítését, ezáltal a versenyképesség növelését.

Az átláthatóság növelését célzó egyik legjelentősebb tendencia napjainkban az *Explainable AI* (XAI), vagyis a magyarázható mesterséges intelligencia, melynek alapvető célja, hogy az MI által hozott döntések, a modell belső működése és a döntési folyamatok logikája könnyen érthető legyen.⁸⁸ A felhasználók, adatkezelők és fejlesztők számára egyaránt átlátható MI-rendszerek alkalmazására irányuló megközelítés a *black box*-effektusból fakadó kockázatok

⁸⁸ A magyarázható MI-modellekről ld. bővebben Dang MINH - H. Xiang WANG - Y. Fen LI - Tan N. NGUYEN: *Explainable Artificial Intelligence: A Comprehensive Review*. Artificial Intelligence Review, 2022 55:3503–3568.; Roberto CONFALONIERI - Ludovik COBA - Benedikt WAGNER - Tarek R. BESOLD: *A Historical Perspective of Explainable Artificial Intelligence*. WIREs Data Mining and Knowledge Discovery, Volume 11, Issue 1

csökkentését célozza. Jelenleg azonban nincs egyetértés a szakirodalomban annak vonatkozásában, hogy ez az átláthatóság hogyan biztosítható effektíven.

5.4.1. Átláthatósági tesztek

Figyelemmel a dolgozatom 4.4.1. pontjában kifejtettekre, a *black box*-effektusnak nevezett jelenségből adódóan problémás lehet az érintettek tájékoztatása az alkalmazott logikáról, erre tekintettel ESZTERI Dániel az Oxford Internet Institute és a londoni Alan Turing Institute közös kutatásaira támaszkodva egyfajta tesztrendszer bevezetését szorgalmazza.⁸⁹ A kutatás eredményeit prezentáló tanulmány alapján ez a módszer azért lenne sikeres, mert az érintettek számára gyakran nem a logika működése a legfontosabb, hanem az, hogy hogyan javíthatnak az algoritmus által megállapított eredményeken. Így a szerzők példaként hozzák azt az esetet, ha hitelkérelmek benyújtása esetén rendelkezésre állna egy nyilvános tesztrendszer, amit fiktív adatokkal kitöltve a felhasználók megérthetnék, hogy különféle paraméterek esetén milyen következtetésekre jut a szoftver.⁹⁰ Ez a megoldás álláspontom szerint nem csak a közérthető tájékoztatást segítheti elő, de védi az MI-fejlesztők szellemi tulajdonát és versenyképességét is.

5.4.2. Eleve megmagyarázható modellek

A szakirodalomban a *XAI*-val kapcsolatban egyre inkább megjelenik az az álláspont, hogy az efféle átláthatóságot az eleve értelmezhető modellek alkalmazása biztosíthatja.⁹¹

Lawrence LESSIG hangsúlyozza, hogy az új technológiák nem csak a jogon, de magába a technológiába épített korlátozásokon keresztül is szabályozhatók. Bár a szerző a mű első kiadásakor még az internet, illetve a robotok vonatkozásában kereste a választ a megfelelő szabályozás kérdésére, az általa felvázolt nézetek ma is relevánsak, alkalmazhatóak lehetnek az új kihívások kezelésére. A LESSIG által meghatározott négy alapvető kategória – jog, társadalmi normák, piac és architektúra, mint a szabályozás eszközei – olyan átfogó keretrendszert nyújt, amely képes adaptálódni az MI és a Big Data technológiák által felvetett adatvédelmi kérdésekhez is.⁹²

⁸⁹ ESZTERI, i. m., 680.

⁹⁰ Sandra WACHTER - Brent MITTELSTADT - Chris RUSSELL: *Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR*. Harvard Journal of Law & Technology, 31 (2), 2018. 863-871.

⁹¹ Cynthia RUDIN: *Stop Explaining Black Box Machine Learning Models for High Stakes Decisions and Use Interpretable Models Instead*, 2019. 1-5.

⁹² Lawrence LESSIG: *Code and Other Laws of Cyberspace*. Basic Books, 1999.

A fentiekre ZÖDI Zsolt mutat rá,⁹³ mindezeket tovább gondolva pedig megállapítható, hogy a jogalkotón túl magukat az MI-fejlesztőket is felelősség terheli annak tekintetében, hogy milyen változásokat hoznak ezen technológiák. Az algoritmusokba egyre inkább szükségessé válik ugyanis olyan korlátozásokat is beépíteni, amelyek révén megakadályozhatóak a visszaélések, a diszkriminatív gyakorlatok vagy akár a szerzői jogi jogsértések. Ez – a megfelelő jogszabályi háttér megléte mellett – elhanyagolhatatlan jelentőségű az Európai Unió adatvédelmi jogának szempontjából, hiszen a beépített védelmi mechanizmusok hatékonyabban szolgálhatják az adatvédelmi normák betartását, mint az adatkezelők által megvalósított intézkedések.

Amennyiben tehát a jogszabályok előírnák a fejlesztők számára egy olyan átlátható kritériumrendszer betartását és az MI-szoftverekbe való beépítését, mely az etikus és jogszerű felhasználást szolgálja, olyan MI-k jöhetnének létre, amelyek egyáltalán nem adnak lehetőséget visszaélésre. Ez magában foglalhatja az adatminimalizálást, mint alapértelmezett beállítást vagy a felhasználók számára átlátható adatkezelés biztosítását, de utalhat akár a differenciált adatvédelem⁹⁴ alkalmazására is.

Marco ALMADA restriktív megközelítésként hivatkozik arra a módszerre, melynek lényege, hogy már a rendszer tervezési szakaszában kezelik az átláthatatlanságot, ezzel biztosítva, hogy maga a rendszer kialakítása lehetővé tegye az abba való betekintést a fejlesztőkön kívüli kör számára is.⁹⁵ Az ilyen, eleve megmagyarázható módon felépített modellek természetüknél fogva értelmezhetőek, így az érintettek számára is közérthető módon tesznek eleget a GDPR-ban meghatározott tájékoztatási kötelezettségnek.

Ennek vonatkozásában ALMADA kiemeli ugyanakkor, hogy az átlátható rendszerekkel kapcsolatban számos, a hasznosságot érintő kérdés merül fel. Gyakran előforduló probléma, hogy ezek a modellek nem érik el a mélytanulási algoritmusok teljesítményét.⁹⁶ Erre figyelemmel a XAI fejlesztése során szükséges tekintettel lenni arra, hogy mely kontextusok igényelnek eleve értelmezhető modelleket, és hol lehet elfogadható kompromisszumot kötni más magyarázó technikák alkalmazásával.

⁹³ ZÖDI, i. m., 194.

⁹⁴ A differenciális adatvédelem (*differential privacy*) olyan matematikai keretrendszer, amely biztosítja, hogy a személyes adatok és az azokból nyert információk védelmet élvezzenek még akkor is, ha az adott adatbázisban lévő többi adat nagyrészt ismert. A Microsoft kutatója, Cynthia Dwork által kidolgozott eljárás a technológia eszközeivel járul hozzá az egyének magánéletének védelméhez. Forrás: Jane R. BAMBAUER - Krish MURALIDHAR - Rathindra SARATHY: *Fool's Gold: an Illustrated Critique of Differential Privacy*. Arizona Legal Studies Discussion Paper No. 13-47

⁹⁵ Marco ALMADA: *Governing The Black Box of Artificial Intelligence*, 2023. 12-15.

⁹⁶ ALMADA, i. 13-15.

6. Összegzés

Ahogy arra a jelen kutatásom során igyekeztem rámutatni, a Big Data és a mesterséges intelligencia alkalmazása alapjaiban véve formálja át az Európai Unió gazdasági szereplői által megvalósított adatkezelést. Számtalan olyan kihívásról tettem említést dolgozatom keretein belül, amelyek a vállalkozásokat a versenyképességre veszélyes mértékben is fenyegethetik, erre tekintettel álláspontom szerint szükséges különös figyelmet fordítani az adatvédelem területére.

A jelen dolgozatom elkészítése során lefolytatott kutatómunka során igazolást nyert azon felvetésem, miszerint az Európai Unió hatályos adatvédelmi szabályozása nem tud maradéktalanul lépést tartani a technológia fejlődés által előidézett kihívásokkal, így a jogszabályi keretek átdolgozása elkerülhetetlenné vált. Noha az Európai Unió olyan szabályozási környezet megalkotására törekszik, amely elősegíti az innovációt és nem hagyja figyelmen kívül az érintettek adatainak védelmét sem, felismerve azt, hogy a jelenlegi – nemzeti vagy akár nemzetközi – jogi keretek nem tudnak megbirkózni a gyors technológiai fejlődésből adódó komplex kihívásokkal. Bár a mesterséges intelligencia szabályozási környezete – azon belül is különösen az AI Act – az Európai Unió tagállamai vonatkozásában számtalan korábbi aggályra választ ad, álláspontom szerint szükséges tovább cizellálni a szabályozást annak érdekében, hogy a gyakorlatban megjelenő kihívások is leküzdhetőek legyenek: egyebek mellett a profilalkotás, a predikciós mechanizmusok és a visszanevesíthetőség olyan, különösen érzékeny kérdések, amelyek további szabályozást tesznek szükségessé.

A dolgozatom elején körvonalazott irányokon túlmenően kutatásom során arra is fény derült, hogy a megfelelő jogszabályi rendelkezések megalkotása és a technológiai transzparencia biztosítása nem csupán a jogalkotó kötelezettsége, hiszen az a mesterséges intelligencia fejlesztőinek és alkalmazóinak aktív közreműködését is megköveteli. Az MI felelős és fenntartható alkalmazása érdekében mind a szabályozás szintjén, mind a gyakorlatban kiemelt jelentőségű az érintettek jogainak tiszteletben tartása és az innováció társadalmi hatásainak figyelembevétele.

Összességében tehát álláspontom szerint elengedhetetlenül szükséges annak biztosítása, hogy a jogszabályok lépést tartsanak a gyorsan változó technológiai háttérrel, amely a jogalkotó szervek hatáskörébe tartozik, emellett azonban fontos, hogy a vállalati szektor is aktív szerepet vállaljon az adatvédelmi megoldások fejlesztésében, hiszen csak így biztosítható, hogy az új technológiák használata ne járjon együtt a felhasználók jogainak sérelmével.

7. Irodalomjegyzék

7.1. Szakcikkék, kiadványok

- A. M. TURING: Computing Machinery and Intelligence. Oxford University Press, 1950
- A. M. TURING: Intelligent Machinery. Oxford University Press, 1948
- Alexandr KESA - Tanel KERIKMÄE: Artificial Intelligence and the GDPR: Inevitable Nemeses?, TalTech Journal of European Studies 10, no. 3, 2020
- Andrea BONEZZI – Massimiliano OSTINELLI - Johann MELZNER: The human black-box: the illusion of understanding human better than algorithmic decision-making. Journal of Experimental Psychology: General 151(9), 2022
- Bartosz BROŻEK - Michał FURMAN - Marek JAKUBIEC - Bartłomiej KUCHARZYK: The black box problem revisited. Real and imaginary challenges for automated legal decision making. Artificial Intelligence and Law, 2024
- Bitu AMANI: AI and Equality by Design. Artificial Intelligence and the Law in Canada, 2021
- Bögel GYÖRGY: A Big Data ökoszisztémája. Typotex Elektronikus Kiadó Kft, Budapest, 2015
- Bryan CASEY - Ashkan FARHANGI - Roland VOGL: Rethinking Explainable Machines: The GDPR's „Right to Explanation” Debate and the Rise of Algorithmic Audits in Enterprise. Berkeley Technology Law Journal, 2019
- Cass R. SUNSTEIN: The Ethics of Nudging, 2014
- Charles DUHIGG: Psst, You In Aisle 5. New York Times, 2012. február 19.
- Cynthia RUDIN: Stop Explaining Black Box Machine Learning Models for High Stakes Decisions and Use Interpretable Models Instead, 2019
- Dang MINH - H. Xiang WANG - Y. Fen LI - Tan N. NGUYEN: Explainable Artificial Intelligence: A Comprehensive Review. Artificial Intelligence Review, 2022 55:3503–3568
- Daniel L. RUBINFELD - Michal S. GAL: Access Barriers to Big Data. Arizona Law Review, Vol. 59.
- Dimitra MARKOPOULOU - Vagelis PAPAKONSTANTINOU - Paul DE HERT: The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. Computer Law & Security Review, Volume 35, Issue 6, 2019.
- Douglas LANEY: 3D Data Management: Controlling Data Volume, Velocity and Variety. Gartner. Retrieved, 6, 2001.

- ESZTERI Dániel: Hogyan tanítsuk jogszerűen a mesterséges intelligenciánkat? Magyar Jog, 2019/12.
- Francis X. DIEBOLD: On the Origin(s) and Development of the Term “Big Data”, 2012. PIER Working Paper No. 12-037
- Giovanni SARTOR - Francesca LAGIOIA - Giuseppe CONTISSA: The Use of Copyrighted Works by AI Systems: Art Works in the Data Mill, 2018
- Ira S. RUBINSTEIN: Big Data: The End of Privacy or a New Beginning? International Data Privacy Law, Volume 3, Issue 2, May 2013. 78.
- J. MINSKY: Steps Toward Artificial Intelligence. Proceeding of The Ire, 1961
- Jane R. BAMBAUER - Krish MURALIDHAR - Rathindra SARATHY: Fool's Gold: an Illustrated Critique of Differential Privacy. Arizona Legal Studies Discussion Paper No. 13-47
- Jane THOMASON: Big Tech, Big Data and the New World of Digital Health. Global Health Journal, Volume 5, Issue 4, 2021
- Jarek GRYZ - Marcin ROJSZCZAK: Black box algorithms and the rights of individuals: no easy solution to the “explainability” problem. Internet Policy Review, 10(2), 2021
- Jonas SCHUETT: Risk Management in the Artificial Intelligence Act. European Journal of Risk Regulation, 2023
- Kate CRAWFORD – Jason SCHULTZ: Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. Boston College Law Review, Vol. 55, No. 93, 2014
- KESERŰ Barna Arnold: A 21. századi technológiai változások hatása a jogalkotásra,. Dialóg Campus, Budapest, 2020
- Lawrence LESSIG: Code and Other Laws of Cyberspace. Basic Books, 1999
- Lilian MITROU: Data Protection, Artificial Intelligence and Cognitive Services: Is The General Data Protection Regulation (GDPR) "Artificial Intelligence-Proof"?
- Lokke MOEREL - Corien PRINS: Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things, 2016
- LUKÁCS Adrienn: Digitális diszkrimináció és automatizált döntéshozatal, különös tekintettel a munka világára. MJSZ, 2023/2.
- Marco ALMADA - Nicolas PETIT: The EU AI Act: a medley of product safety and fundamental rights? Robert Schuman Centre for Advanced Studies Research Paper No. 2023/59.

- Marco ALMADA: Governing The Black Box of Artificial Intelligence, 2023.
- Martin EBERS: Truly Risk-Based Regulation of Artificial Intelligence – How to Implement the EU’s AI Act, 2024
- MEZEI Kitti: A mesterséges intelligencia jogi szabályozásának aktuális kérdései az Európai Unióban. IMR, 2023/1.
- Neil M. RICHARDS – Jonathan KING: Big Data Ethics. Wake Forest Law Review, 2014
- Neil M. RICHARDS – Jonathan KING: Three Paradoxes of Big Data. Stanford Law Review Online, 2013
- Niels VANDEZANDE: Cybersecurity in the EU: How the Nis2-Directive Stacks Up Against its Predecessor, 2023
- Omer TENE - Jules POLONETSKY: Privacy in the Age of Big Data: A Time For Big Decisions. Stanford Law Review Online, 2012
- Paul DE HERT – Vagelis PAPAKONSTANTINOU: The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals, 2012. Computer Law and Security Review, Vol. 28, No. 2.
- Paul OHM: Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. UCLA Law Review, Vol. 57., 2010
- Philip RUSSOM: Big Data Analytics. TDWI Best Practices Report, 2011
- Richard KEMP: Legal Aspects of Managing Big Data. Computer Law & Security Review, Volume 30, Issue 5, 2014
- Roberto CONFALONIERI - Ludovik COBA - Benedikt WAGNER - Tarek R. BESOLD: A Historical Perspective of Explainable Artificial Intelligence. WIREs Data Mining and Knowledge Discovery, Volume 11, Issue 1
- Sandra WACHTER - Brent MITTELSTADT - Chris RUSSELL: Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR. Harvard Journal of Law & Technology, 31 (2), 2018
- Sara QUACH - Park THAICHON - Kelly D. MARTIN - Scott WEAVER - Robert W. PALMATIER: Digital Technologies: Tensions in Privacy and Data. Journal of the Academy of Marketing Science, 2022
- Solon BAROCAS - Andrew D. SELBST: Big Data's Disparate Impact. California Law Review Vol. 104, No. 2

- Sonia KATYAL: Private Accountability in the Age of Artificial Intelligence. 66 UCLA L. REV. 54, 2019
- STEFÁN Ibolya: A mesterséges intelligencia jogi szabályozásának egyes kérdései. MJSZ, 2020. 3. Különszám
- Tal ZARSKY: Incompatible: The GDPR in the Age of Big Data. Seton Hall Law Review, Vol. 47, No. 4(2), 2017.
- Toshinori MUNAKATA: Fundamentals of the New Artificial Intelligence. Springer, 2008
- TÓTH András: Az Európai Unió Mesterséges Intelligencia Törvényéről. GJ, 2024/5-6.
- Yavar BATHAEE: The Artificial Intelligence Black Box and the Failure of Intent and Causation. Harvard Journal of Law & Technology Volume 31, Number 2, 2018
- Yifat NAHMIAS - Maayan PEREL: The Oversight of Content Moderation by AI: Impact Assessments and Their Limitations. Harvard Journal on Legislation, Vol. 58, No. 1, 2021
- ZÖDI Zsolt: Jog és Jogtudomány a Big Data korában. Állam- és Jogtudomány, 58. évfolyam 1. szám, 2018

7.2. Jogsabályok és uniós kiadványok

- Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről
- Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv)
- Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete (2024. június 13.) a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról, valamint a 300/2008/EK, a 167/2013/EU, a 168/2013/EU, az (EU) 2018/858, az (EU) 2018/1139 és az (EU) 2019/2144 rendelet, továbbá a 2014/90/EU, az (EU) 2016/797 és az (EU) 2020/1828 irányelv módosításáról (a mesterséges intelligenciáról szóló rendelet)
- Az Európai Parlament és a Tanács 95/46/EK irányelv (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról
- European Commission (2010): Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the

Regions – A comprehensive approach on personal data protection in the European Union.
Brussels, 4. November. COM(2010) 609 final

- European Commission: Directorate-General for Communications Networks, Content and Technology, Etikai iránymutatás a megbízható mesterséges intelligenciára vonatkozóan, Publications Office, 2019
- Fehér Könyv a mesterséges intelligenciáról: a kiválóság és a bizalom európai megközelítése, Brüsszel, 2020.2.19. COM(2020) 65 final