DOI 10.26521/Profuturo/2020/1/7554

Jog- és államtudomány

Eszteri Dániel*

Elosztott mesterséges-intelligencia-fejlesztés blokklánc alapon az adatvédelem érvényesülése érdekében

Developing Blockchain-Based Distributed AI for Personal Data Protection

Absztrakt

A tanulmány célja bemutatni néhány olyan alapvető adatvédelmi jogi elvet, amelyek alkalmazásával a blokkláncban kezelt személyes adatok és az azokkal végzett automatikus döntéshozatal technológiája megfeleltethető lehet az Európai Unió általános adatvédelmi rendelete (GDPR) előírásainak. Az ilyen típusú rendszerek fejlesztése során az elemzés a „beépített adatvédelem" elvére helyezi a hangsúlyt. Feltevésem, hogy mivel a blokklánc elosztott alapú adatkezelést lehetővé tévő hálózat, ezért az abban részt vevő minden egyes csomópont adatkezelése vagy adatfeldolgozása során érvényesülnie kell bizonyos előre meghatározott, már a fejlesztés során kollektívan beépített és jelen lévő, absztrakt adatkezelési mintázatoknak. A jobb megértés érdekében az emberi tudatot és annak tudatos és tudattalan tartalmakkal való „feltöltését" hoztam analógiaként. Fő célom ezáltal rávilágítani arra, hogy a blokklánc és a gépi tanuláson alapuló mesterséges intelligencia két olyan technológia, amelyek összekapcsolása alkalmas komoly automatikus döntéshozó rendszerek (ún. „elosztott MI") fejlesztésére. Ezen elosztott MI-t használó rendszerek adatvédelmi jogi megfelelése a nagyon komoly kockázatok miatt olyan kulcskérdés, amivel – a technológia fejlődési irányait szem előtt tartva – érdemes komolyabban is foglalkozni.

Kulcsszavak: *általános adatvédelmi rendelet, GDPR, blokklánc, mesterséges intelligencia, gépi tanulás, automatikus döntéshozatal, beépített adatvédelem*

Abstract

The aim of the paper is to present some of the general principles of data protection law that can be applied to automated decision-making built on blockchain-based data processing in order to comply with the provision of the European Union's General Data Protection Regulation (GDPR). The analysis focuses on the applicability of the 'data protection by design' principle during the development of such systems. My hypothesis is that because blockchain-based networks are built on distributed data processing operations, therefore data controlling or processing of participating

* Dr. Eszteri Dániel, osztályvezető, Nemzeti Adatvédelmi és Információszabadság Hatóság, e-mail: daniel.eszteri@outlook.com.

nodes should comply with some abstract data protection patterns predetermined and collectively built-in during the system's development phase. For the sake of better understanding, I presented the human mind and its 'uploading' with conscious and unconscious content as an analogy to blockchain-based AI systems. My goal is to highlight that the fusion of blockchain and machine learning-based AI can be a suitable technology to develop serious automated decision-making systems (so-called 'distributed AI'). The compliance of these distributed AI systems with data protection law principles is a key issue regarding the very serious risks posed by them.

Keywords: *General Data Protection Regulation, GDPR, blockchain, artificial intelligence, machine learning, automated decision making, data protection by design*

A blokklánc és a mesterséges intelligencia (röviden: MI) két olyan ágazata a technológiai fejlesztéseknek, amelyek jogi értékeléséről napjainkban egyre több szó esik a vonatkozó szakirodalomban. Egyelőre azonban a jogi szakirodalom még jellemzően külön-külön vizsgálja ezek lehetséges értékelését. Tanulmányomban ezért szeretnék kísérletet tenni e látszólag távoli jelenségek közötti összefüggések azonosítására és vizsgálatára. A továbbiakban egy – alapvetően elméleti – gondolatkísérletet szeretnék bemutatni, amelynek nem titkolt célja a diskurzus erősítése e témában, az Európai Unió 2018-ban alkalmazandóvá vált általános adatvédelmi rendeletében (*General Data Protection Regulation,* a továbbiakban: GDPR)[1] foglalt előírások szempontjából. Ennek természetesen előfeltétele, hogy a blokkláncot – mint elosztott hálózati alapon működő adatkezelési technológiát – használva személyes adatok kezelése (is) történjen, továbbá megvalósuljon a személyes adatok kezelése tekintetében valamilyen automatikus, nem ember által vezérelt döntéshozatal. Az ilyen rendszerrel végső soron megalkotható az elosztott MI koncepciója, amely befolyással lehet az emberek mint adatalanyok alapvető jogaira.

Az elosztott MI-t használó rendszerek nagyon komoly adatvédelmi kockázatokat jelentenek az érintettek jogaira és szabadságaira nézve, mivel két új, még kevésbé kiforrott technológiáról van szó. Ezek vizsgálata a technológia fejlődési irányait is figyelembe véve véleményem szerint igencsak időszerű és indokolt.

A tanulmány első részében ismertetem a két különálló technológia sajátosságait adatvédelmi szempontból, majd kísérletet teszek az összekapcsolásukkal létrejövő elosztott MI által jelentett problémák ismertetésére.

1. A blokklánc használatán alapuló adatkezelés sajátosságai

A két technológia közül a blokklánc adatkezelési és adatvédelmi szempontú bemutatásával kezdem, mivel ez mint elosztott adatkezelést lehetővé tévő technológia képezi az általam vizsgált problémák alapját és kiindulópontját.

[1] Az Európai Parlament és a Tanács (EU) 679/2016 számú 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 (általános adatvédelmi rendelet). HL L 119., 2016.5.4., 1–88.

1.1. A blokklánc mint adatok kezelésére szolgáló számítógépes hálózat

A blokklánc-technológia az ún. „elosztott főkönyvi technológiák” *(distributed ledger technologies)* egyik, a gyakorlatban is megvalósított, leggyakrabban előforduló képviselője. Az elosztott főkönyv olyan tranzakciós adatbázis, amely több számítógépből álló hálózaton oszlik el, nem pedig központi helyen tárolják. A blokklánc megnevezés onnan ered, hogy a tranzakciók csoportonként, azaz blokkonként időrendi sorrendben egymáshoz kapcsolva láncot alkotnak.[2]

A blokkláncot – szándékosan leegyszerűsítve – tulajdonképpen egy adatok tárolására és mozgatására szolgáló rendszerként lehet leírni. Az adatok blokkláncon belüli tárolásának és mozgatásának előfeltétele egy számítógépekből álló, elosztott típusú hálózat, amelyben nincs alá-fölé rendeltségi viszony az egyes számítógépek között. Az elosztott hálózatra kapcsolódó gépek ún. csomópontokként (*node*-okként) funkcionálnak, amelyek egymáshoz kapcsolódnak. Végeredményben mindegyik csomópont összeköttetésben áll az összes többivel. Az ilyen típusú hálózat előnye, hogy egy csomópont kiesése semmilyen fennakadást nem okoz a rendszer működésében, feladatait azonnal át tudják venni más csomópontok.[3] A blokkláncban kezelt adatcsomagok bármilyen információ tárolására, kezelésére alkalmasak lehetnek, így maga a technológia univerzálisan használható szinte bármilyen adatkezelési célra.

1.2. A blokk mint adattárolási egység

A blokklánc-technológiát használó hálózatokon az adatok tárolása az ún. blokkokban történik. Bizonyos felfogások szerint a blokkokat úgy képzelhetjük el, mint egy üres dokumentumot, papírlapot vagy táblát, amire bármilyen információt leírhatunk.[4] E hasonlat alapján egy blokk születésének pillanatában az empirista gondolkodók által használt *tabula rasa* fogalmának feleltethető meg. E fogalommal az empirikus iskolát képviselő filozófusok azt kívánták érzékeltetni, hogy véleményük szerint az emberi elme – mint egyfajta információhordozó és feldolgozó közeg – a megszületés pillanatában még nem tartalmaz semmiféle veleszületett tudást.[5] Ehhez képest a racionalizmus filozófiai iskola képviselői szerint minden ember elméje rendelkezik bizonyos előre meghatározott ideákkal, mintázatokkal, amelyek az elme mélyebb rétegeiben a születés pillanatától jelen vannak.[6] Ezen két koncepció összevetésének a tanulmány konklúziója szempontjából később még lesz jelentősége.

---

[2] Európai Központi Bank: Hogyan formálják át a technológiai újítások a pénzügyi piacokat? 2017. április 19. https:// www.ecb.europa.eu/explainers/tell-me-more/html/distributed_ledger_technology.hu.html (2020. 05. 09.).

[3] Győrfi András–Léderer András–Paluska Ferenc–Pataki Gábor–Tuan, Trinh Anh: *Kriptopénz ABC.* HVG Könyvek, Budapest, 2019, 57–59.

[4] Győrfi–Léderer–Paluska–Pataki–Truan: i. m., 60.

[5] Lásd erről legkorábban *Arisztotelész* („A lélekről”), majd később a felvilágosodás során *John Locke* („Értekezés az emberi értelemről”) írásait. Andrássy György: *Filozófia és jogászi etika.* Dialóg Campus, Pécs, 2008.

[6] Lásd legkorábban *Platón* gondolatait az ideák világáról (a „Parmenidész”-ben), majd később például *Descartes* foglal állást a racionalizmus mellett a *tabula rasa* koncepciójával szemben (az „Értekezés a módszerről” című műben). Andrássy: i. m.

A blokkokban mint adattárolási egységekben bármilyen információ eltárolható, az adott blokklánc létrehozásának céljától függően. A blokkláncot alkotó blokkokat először – a Bitcoin-rendszer kapcsán – ún. kriptopénzekkel kapcsolatos tranzakciók adatainak tárolására használták, de azok tulajdonképpen bármilyen más adat és azokkal végzett művelet tárolására alkalmasak lehetnek. Az információkat tartalmazó blokkok láncszerűen, utólag megváltoztathatatlanul kapcsolódnak egymáshoz, ami annyit jelent, hogy az újabb blokkok és a bennük lévő új adatok mindig csak a lánc végére kerülhetnek. A lánc kezdetén lévő első létrejött blokkot nevezzük „genezis-blokknak".[7]

Az egyes blokkokban tárolt adatokon végzett műveletek kivitelezésére nem úgy kerül sor, hogy tényleges adatmozgás valósul meg az egyes blokkok között, hanem a rendszer az egyes adatokhoz csak hozzárendeli az azokat tároló blokkban, hogy afelett például épp melyik felhasználó jogosult rendelkezni. A rendszer az egyes felhasználók „digitális aláírásaival" látja el a blokkokban tárolt adatokat, és ez alapján ítéli meg, hogy adott blokkban tárolt adathalmaz feletti rendelkezés, hozzáférés joga kit illet meg.[8]

A láncszerűen felépülő és így egyre növekvő adatbázishoz az újabb adatok újabb blokkokban kerülnek hozzáadásra. A blokkokban tárolt adatokkal végzett valamenynyi művelet naplója is az egyes blokkokban van tárolva. A blokkláncot alkotó blokkokban tárolt adatokkal végzett műveletek naplóját nevezzük összefoglaló néven „blokktörténetnek".

A hálózatra kapcsolódott számítógépek (az ún. csomópontok) feladata az, hogy a blokkokban tárolt adatokkal végzett adatkezelési műveletek hitelességét algoritmikus úton ellenőrizzék.[9] A művelet jóváhagyása során azt ellenőrzik, hogy a tranzakció digitálisan megfelelően alá van-e írva a műveletet indítványozó felhasználó által, és van-e annak bármilyen hiteles előzménye a blokkláncon.

Amennyiben a csomópontok (vagy előre meghatározott számú csomópont) jóváhagyják a műveletet, az rögzítésre kerül a blokkban, ami ezentúl megmásíthatatlanul hozzákapcsolódik a teljes lánchoz. A hitelesség további garanciáját nyújtja, hogy minden egyes csomópont letölt egy másolatot ezek után a friss blokkláncból, hogy egymást is tudják folyamatosan ellenőrizni, és meg tudják osztani egymás között a blokklánc legfrissebb kópiáját.[10]

A fentiek alapján a blokkláncot legegyszerűbben egy olyan adatkezelési technológiaként írhatjuk le, amely az adatok kezelését egy közös, elosztott hálózaton teszi lehetővé, és amely központi ellenőrző szerv felügyelete nélkül is működőképes. Az adatokkal végzett műveletek hitelesítése a hálózaton algoritmikus alapú önellenőrző mechanizmusokkal biztosított.

[7] Győrfi–Léderer–Paluska–Pataki–Truan: i. m., 61.

[8] Nemzeti Adatvédelmi és Információszabadság Hatóság: Állásfoglalás a blokklánc („blockchain") technológia adatvédelmi összefüggéseivel kapcsolatban, 2017. július 24. https://naih.hu/files/Adatved_allasfoglalas_naih-2017-3495-2-V.pdf; 3. (2020. 05. 09.).

[9] Kakavand, Hossein–De Kost, Sevres–Nicolette, Bart–Chilton, Bart: The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies. *SSRN,* 1 January 2017, 4–7. (DOI: 10.2139/ssrn.2849251).

[10] Győrfi–Léderer–Paluska–Pataki–Truan: i. m., 63, 68.

1.3. Út az elosztott MI felé: az okosszerződés mint a blokkláncon futó automatizált alkalmazás

A blokkláncon különböző algoritmusok futtatását az abban kezelt adatokkal végzett műveletek bizonyos fokú automatizálása érdekében már viszonylag régen leírták a témával foglalkozók. A blokklánc alapú műveletek automatizálásáról először az ún. okosszerződések *(smart contracts)* koncepciójához kapcsolódóan *Nick Szabó* írt, 1996-ban megjelent tanulmányában. Szabó szerint az okosszerződés olyan szerződés, amely az előre meghatározott feltételek bekövetkezése esetén automatikusan megvalósul, a szerződés ezért megszeghetetlen. A feltételek megvalósulása esetén a szerződés teljesítését, biztonságát és megszeghetetlenségét az a számítógépes hálózat biztosítja, amelyikben a felek azt elkészítették, ezért nincs szükség a hitelesítéshez harmadik fél (például ügyvéd) közreműködésére.[11] A blokklánc alapú rendszer az okosszerződések megkötésére és teljesítésére teljes mértékben alkalmassá tehető technológia, amelyet a gyakorlatban is megvalósítottak már.

Az okosszerződések kötésének lehetőségét a *Vitalik Buterin* által megalkotott koncepció alapján létrehozott, *Ethereum* nevű blokklánc-technológiát alkalmazó platform vezette be először. Lényege, hogy a blokklánc alapú hálózaton olyan programokat futtatnak, amelyek az előre kikötött szerződéses feltételek megvalósulása esetén végrehajtanak bizonyos műveleteket a hálózaton az ott kezelt adatokkal.[12] A hálózaton futó program így automatikusan végrehajt egy döntést, ha annak feltételei teljesülnek.

Az okosszerződések esetében is a csomópontok hitelesítik a folyamatot és az azzal összefüggésben kezelt adatokat, így a szerződő felek számlaszámait, az összeget, az időpontokat (például határidő) és egyéb feltételeket, de rögzíthetnek akár más személyes adatokat (például név) vagy egyéb szöveges információkat (például közlemény) is. A szerződés létrejöttével összefüggésben kezelt adatok és mozgásuk naplója megváltoztathatatlanul rögzül a blokkláncban.

Az okosszerződéses alkalmazás a hálózat valamennyi csomópontján fut, így annak funkcióit lehetőségük van kihasználni a felhasználóknak. Az okosszerződés kódja és az automatizálásért felelős algoritmus valamennyi résztvevő számára látható, hozzáférhető és felhasználható.[13]

1.4. A blokkláncon futtatható automatizált algoritmusok és a GDPR kapcsolata

A fentiek alapján könnyen elképzelhető, hogy a blokkláncon nem csupán olyan automatikus műveletek végrehajtására alkalmas algoritmus futtatható, amely szer-

[11] Szabó, Nick: Smart Contracts: Building Blocks for Digital Markets. 1996. https://www.truevaluemetrics.org/DBpdfs/BlockChain/Nick-Szabo-Smart-Contracts-Building-Blocks-for-Digital-Markets-1996-14591.pdf; 1–5, 8. (2020. 05. 09.).

[12] Buterin, Vitalik: A Next-Generation Smart Contract and Decentralized Application Platform. Ethereum White Paper, 2013. https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf (2020. 05. 09.).

[13] Bacon, Jean–Michels, Johan David–Millard, Christopher–Singh, Jatinder: Blockchain Demystified. *Queen Mary School of Law Legal Studies Research Paper,* 268/2017, 29.

ződések megkötésére használhatja fel a blokkláncban kezelt adatokat. A blokkláncban lévő adatokon futtatható lehet bármilyen más, automatizált döntéshozatalra alkalmas algoritmus, szoftver. Ilyen lehet például egy profilalkotásra alkalmas program, vagy bármilyen más, a kezelt adatok alapján mintákat kereső, és ezek alapján döntéseket hozó alkalmazás.[14]

Már itt utalnék arra, hogy témánk szempontjából kulcsfontosságú az automatizált döntéshozatal fogalma, mivel a vizsgált probléma szempontjából alapvetőnek tekintjük, hogy a blokkláncban kezelt személyes adatokat felhasználva automatikusan, emberi beavatkozás nélkül szülessenek döntések. A GDPR mint európai uniós adatvédelmi norma, nem határozza meg, hogy mi tekinthető *automatizált döntéshozatalnak,* holott több helyen is használja ezt a fogalmat. A *profilalkotás* fogalma viszont szerepel a rendelet értelmező rendelkezései között. Eszerint ilyennek minősül, ha a személyes adatokat automatizált módszerekkel az egyén tulajdonságainak, jellemzőinek értékelésére, elemzésére vagy előrejelzésére használják.[15]

Az Európai Unió 1995-ös adatvédelmi irányelvének[16] 29. cikke szerint működő Adatvédelmi Munkacsoport (*Article 29 Working Party,* a továbbiakban: WP29) vonatkozó iránymutatása szerint az automatizált döntéshozatal az a képesség, hogy technológiai eszközök segítségével, emberi beavatkozás nélkül hoznak döntéseket.[17] A kizárólag automatizált döntéshozatalban tehát nincs emberi részvétel a döntési folyamatban.

A GDPR megfogalmazása több helyen együtt utal a profilalkotásra és az automatizált döntéshozatalra, és közös szabályokat állapít meg velük kapcsolatban. Fontos megjegyezni, hogy ettől függetlenül a két fogalom nem teljes mértékben azonos. Létezhet olyan automatizált döntéshozatali eljárás, amely nem minősül egyben profilalkotásnak, illetve profilalkotást is lehet végezni automatizált döntéshozatali mechanizmusok beépítése nélkül. A legtöbb esetben azonban a két fogalom kéz a kézben járnak, és kiegészítik egymást, így adatvédelmi szempontból indokolható az együttes tárgyalásuk.

Az automatizált döntéshozatalra (beleértve adott esetben a profilalkotást is) képes, blokkláncon futó alkalmazásoknak közös sajátossága, hogy az általuk elemzett, a blokkláncban kezelt adatok alapján, emberi beavatkozás nélkül hoznak dön-

[14] Lásd például az alábbi tanulmányt az energiagazdálkodási célokból végzett blokklánc alapú profilalkotás koncepciójáról: Sankaran, Sriram–Sanju, Sonam–Achuthan, Krishnashree: Towards Realistic Energy Profiling of Blockchains for Securing Internet of Things. IEEE 38th International Conference on Distributed Computing Systems (ICDCS), Vienna, 2018, 1454–1459.

[15] GDPR 4. cikk 4. pont: *„'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."*

[16] Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról. HL L 281., 1995.11.23., 31–50.

[17] A 29. cikk szerint működő Adatvédelmi Munkacsoport: Iránymutatás az automatizált döntéshozatallal és a profilalkotással kapcsolatban a 2016/679 rendelet alkalmazásához. https://naih.hu/files/wp251rev01_hu.pdf; 8. (2020. 05. 09.) [a továbbiakban: WP29 (2017)].

téseket. Mielőtt rátérnénk az ezáltal felvetett, adatvédelmi jogi problémákra, röviden be kell mutatni az ún. adatalapú gépi tanulás és döntéshozatal általános jellemzőit, amire a következő pontban kerítek sort.

2. Az adatalapú gépi tanulás és döntéshozatal sajátosságai és adatvédelmi kérdései

2.1. A gépi tanulás általános technológiai háttere

A gépi tanulás technológiai hátterével és GDPR-megfelelésével kapcsolatban ehelyütt csupán annak lényegét emelem ki, és csak olyan mértékben ismertetem, amennyire mindenképpen szükséges a blokklánc alapú elosztott MI modelljének megértéséhez, és további jogi elemzéséhez.

A Norvég Adatvédelmi Hatóságnak *(Datatilsynet)* a gépi tanulás adatvédelmi jogi aspektusait taglaló jelentése úgy írja le az öntanuló MI-t, mint egy olyan rendszert, amely képes a saját tapasztalatai alapján tanulni, és képes a megszerzett tudást különböző helyzetekben összetett problémák megoldására alkalmazni. A koncepció lényege, hogy az MI az általa „látott" (a gyakorlatban tulajdonképpen beletöltött) személyes adatokból tanul és dönt.[18]

A gépi tanulás tehát az MI-fejlesztés egyik ágát jelenti. Ennek lényege, hogy a rendszer tapasztalatokból generál önálló tudást. A rendszer példaadatokban, adatbázisokban keresett minták alapján képes önállóan vagy emberi segítséggel szabályszerűségeket, szabályokat felismerni és meghatározni, majd az elsajátított tudásbázisban felfedezett szabályszerűségek alapján – immár automatikusan – döntéseket hozni.[19]

A gépi tanulás során az MI-rendszer által végzett adatkezelést három lépcsőre lehet bontani:

1. Először a rendszerbe betáplálnak nagy mennyiségű adatot, ebben az adathalmazban pedig az algoritmus megpróbál mintákat, hasonlóságokat keresni. Amennyiben az algoritmus talál ilyen azonosítható mintákat, úgy azokat megjegyzi és elmenti későbbi használat céljából. A megjegyzett és elmentett minták alapján ezek után a rendszer egy ún. *modellt* generál. A rendszer a modell segítségével, a már azonosított minták alapján képes feldolgozni a később általa „látott" (betáplált) adatokat.

2. Ezek után a rendszerbe újabb adatokat töltenek fel, amelyek hasonlóak a tanuláshoz használt adatokhoz. A modell alapján az MI eldönti, hogy az új adat mely megtanult mintázathoz hasonlít a leginkább.

3. A rendszer végül informál arról, hogy milyen döntést hozott az elsajátított mintázatok alapján a beletáplált új adatokkal kapcsolatban.[20]

---

[18] Datatilsynet: Artificial intelligence and privacy. Report, January 2018. https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf (2020. 05. 09.).

[19] Szepesvári Csaba: Gépi tanulás – rövid bevezetés. *MTA SZTAKI,* 2005. március 22. http://old.sztaki.hu/~szcsaba/talks/lecture1.pdf (2020. 05. 09.).

[20] Datatilsynet: i. m., 7.

Fontos azt is megjegyezni, hogy a gépi tanulás során létrejövő modell nem feltétlenül tartalmazza a forrásadatokat, amelyek a tanulásának az alapjául szolgáltak. A gépi tanulás során létrejött MI-rendszer a legtöbb esetben a tanulás alapjául szolgáló adatoktól függetlenül is tud működni.[21]

Visszakanyarodva egy gondolat erejéig a blokklánchoz mint kiindulóponthoz: egy ilyen, gépi tanulással elsajátított mintázatokat (a modellt) felhasználó elemzőszoftver a blokkláncon futtatva képessé válhat arra, hogy ott automatikusan hozzon döntéseket. A blokklánc tehát ebben az esetben azon adatok tárolási formáját és forrását jelenti, amely adatokat felhasználva az MI-szoftver valamilyen döntést fog hozni. Ezen szoftvereket fel lehet így használni blokklánc alapú profilalkotásra, de bármilyen más automatizált döntés meghozatalára is, az abban kezelt adatokkal kapcsolatban. Az automatikus döntéshozó szoftver valamennyi csomóponton fut, így működése és az általa hozott döntések egy elosztott alapú MI-rendszert eredményeznek.

2.2. A gépi tanulás néhány adatvédelmi kérdése

Az alábbiakban az automatizált döntéshozatalra képes rendszerek működése kapcsán felmerülő adatvédelmi problémák közül annak különös szabályait, illetve ehhez kapcsolódva három, szorosan összefüggő elv érvényesülését szeretném röviden és általánosságban ismertetni, a GDPR kontextusában. Ezek az elvek a célhoz kötöttség és az adattakarékosság elvei, valamint az átláthatóság követelménye.

Azért esett ezekre az elvekre a választásom, mert a blokklánc és gépi tanulás alkalmazásán alapuló automatikus döntéshozatali rendszerek fejlesztése során ezen elvek érvényesülésére a kezdetek óta oda kell figyelni a beépített adatvédelem követelményének érvényesülése érdekében is, továbbá ezek az elvek speciális sajátosságokat mutatnak a blokklánc alkalmazása kapcsán. Míg a célhoz kötöttség és adattakarékosság elvének való megfelelés látszólag lehetetlen vállalkozásnak tűnik egy blokklánc alapú adatkezelés esetén, addig az átláthatóság követelménye annál egyszerűbbnek tűnhet. Ezek bemutatása előtt azonban tekintsük át általánosságban az automatizált döntéshozatal különös szabályait a rendeletben.

2.3. Az automatizált döntéshozatalra vonatkozó szabályok a GDPR-ban

A GDPR 22. cikk (1) bekezdése 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 *hasonlóképpen jelentős mértékben érintené*. Ez a rendelkezés általános tilalmat állapít meg a kizárólag automatizált adatkezelésen alapuló döntéshozatal tekintetében. A rendelet ideérti az olyan profilalkotást is, amely ilyen döntési folyamatokon alapul. Ez a tilalom attól függetlenül fennáll, hogy az érintett tesz-e intézkedést a személyes ada-

[21] Datatilsynet: i. m., 10.

tai kezelésével kapcsolatban. Főszabályként tehát a GDPR általános tilalmat állít fel a joghatással vagy hasonlóképpen jelentős hatással járó, kizárólag automatizált egyedi döntéshozatalra vonatkozóan.[22]

Ahhoz, hogy a döntés tekintetében emberi részvételnek minősüljön egy tevékenység, és ezért ne kelljen rá alkalmazni a 22. cikk általános tilalmát, az adatkezelőnek biztosítania kell, hogy a döntést érintő emberi áttekintés érdemi, és nem csak jelképes gesztus. Embernek kell tehát a tilalom feloldásához a végső döntést meghoznia, vagy az algoritmus által felajánlott döntést mérlegelnie és jóváhagynia.[23]

A tisztán automatizált döntéshozatalra vonatkozó szabályokat továbbá csak azokban az esetekben kell alkalmazni, amikor az *joghatással* vagy *hasonló jelentős hatással* jár az érintett természetes személyre nézve. A GDPR nem határozza meg a „joghatás" vagy a „hasonlóképpen jelentős hatás" fogalmakat, azonban a rendelet ezen megfogalmazása egyértelművé teszi, hogy a 22. cikk csak a súlyos következményt jelentő hatásokra terjed ki.[24]

A joghatás megköveteli, hogy a gépi döntés befolyásolja valaki törvényes jogait. Joghatás lehet olyasmi is, ami befolyásolja a személy jogállását vagy szerződésen alapuló jogait. Emellett megjelenik a homályosabban megfogalmazott „hasonlóképpen jelentős hatás" fogalma is. Nehéz pontosan meghatározni, hogy mit kell *jelentős mértékűnek* tekinteni ahhoz, hogy elérje a küszöböt. A WP29 vonatkozó iránymutatása szerint ebbe a kategóriába tartozhatnak az egyén anyagi körülményeit befolyásoló döntések, például a hitelre való jogosultságát illetően; az olyan döntések, amelyek befolyásolják az egyén egészségügyi szolgáltatásokhoz való hozzáférését; vagy amelyek befolyásolják az oktatáshoz való hozzáférését (például: egyetemi felvétel).[25]

Léteznek azonban kivételek ezen általános tilalom alól, amelyeket a 22. cikk (2) bekezdése nevesít. Ezek szerint a tilalom nem alkalmazható az alábbi esetekben:

1. Ha a döntés az érintett és az adatkezelő közötti *szerződés* megkötése vagy teljesítése érdekében szükséges. Ebben az esetben az adatkezelőnek be kell tudnia mutatni, hogy az automatizált döntéshozatal alkalmazása a legmegfelelőbb adatkezelési módszer a szerződésben meghatározott célok eléréséhez. Ha a szerződéssel elérni kívánt célt más módszerrel is el lehet érni, az már nem minősül szükségesnek.[26]

2. Ha a döntés 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

3. Ha a döntés az érintett kifejezett *hozzájárulásán* alapul. A hozzájárulás kifejezett voltáról való meggyőződés legegyértelműbb módja a hozzájárulás írásbeli nyilatkozattal történő megerősítése. A WP29 szerint digitális vagy online kontextusban

[22] Veale, Michael–Edwards, Lilian: Clarity, surprises and further questions in the Article 29 Working Party draft guidence on automated decision making and profiling. *Computer, Law and Security Review,* 2018/2, 400. (DOI: 10.1016/j.clsr.2017.12.002).

[23] WP29 (2017): i. m., 22.

[24] Veale–Edwards: i. m., 401.

[25] WP29 (2017): i. m., 23.

[26] WP29 (2017): i. m., 25.

például előfordulhat, hogy az érintett elektronikus űrlap kitöltésével, elektronikus levél küldésével, az aláírását tartalmazó, szkennelt dokumentum feltöltésével, vagy elektronikus aláírás használatával is ki tudja állítani az előírt nyilatkozatot. Végül a hozzájárulás kétlépcsős ellenőrzésével is meg lehet győződni a kifejezett hozzájárulás érvényességéről (kétfaktoros autentikáció használata).[27]

Amennyiben tehát az automatikus döntéshozatalhoz blokkláncban kezelt személyes adatokat dolgoznak fel, úgy az adatkezelőnek meg kell felelnie a GDPR fenti előírásainak, az ilyen célú rendszer üzemeltetésével kapcsolatban. Természetesen mindig a kezelt adatok, az adott adatkezelési cél, és annak az érintettre jelentett hatása fogja meghatározni, hogy a 22. cikkben foglalt általános tilalom érvényesül-e. Amennyiben igen, úgy az automatizált döntéshozatalt is alkalmazó adatkezelés kizárólag a tilalom alól nevesített kivételek igazolásával lehetséges a blokkláncon.

2.4. A blokkláncon alapuló gépi tanulás a célhoz kötöttség és adattakarékosság alapelveinek való megfelelés szempontjából

A blokklánc alapú adatkezelés és az egymással szorosan összefüggő célhoz kötöttség és adattakarékosság elveinek összeegyeztetése komoly fejtörést okozhat. A célhoz kötöttség elve alapján a személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet, és fontos, hogy azokat nem kezelhetik ezekkel a célokkal össze nem egyeztethető módon.[28] Az adattakarékosság elve alapján a kezelt személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell hogy legyenek, és csak a szükséges mennyiségre kell korlátozódniuk.[29] Mindkét elvből levezethető a túlzó, készletező, feleslegesen kezelt és tárolt adatok kezelésének tilalma.

A blokklánc alapvető működési elve, hogy az adatok a velük végzett tranzakciós műveletek kivitelezése után is tárolódnak az adatbázisban, sőt ezekre kerülnek felfűzésre a további műveletek is, az integritás és biztonság garantálása érdekében. Egyszerűbben: az adatok és az azokkal végzett tranzakciós naplók elvileg a végtelenségig tárolódnak a rendszerben, és ezen keresztül pontosan visszakövethetőek az egyes adatkezelési műveletek. Az adatbázis folyamatosan növekszik, tartalmazva a valaha elvégzett valamennyi adatkezelési műveletet. A blokklánc azon, „replikatív" természete szintén problematikus, hogy valamennyi csomópont eltárolja az adatbázis teljes másolatát, önellenőrzési célokból.[30] Első ránézésre ezen tulajdonságok ellentmondanak a GDPR fentiekben hivatkozott elveinek.

[27] A 29. cikk szerinti Adatvédelmi Munkacsoport: Iránymutatás az (EU) 2016/679 rendelet szerinti hozzájárulásról, 2018. április 10. WP259 rev 01. http://naih.hu/files/wp259-rev-0_1_HU.PDF; 20–22. (2020. 05. 09.).

[28] GDPR 5. cikk (1) bekezdés *b)* pont.

[29] GDPR 5. cikk (1) bekezdés *c)* pont.

[30] Finck, Michèle: *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?* European Parliamentary Research Service, July 2019. https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf; 68.

Nagyon fontos előkérdés a blokkláncon alapuló adatkezelés jogszerűségének megítélése szempontjából azonban, hogy a fenti, látszólag készletező jellegű adatkezelések vajon mennyire egyeztethetők össze az eredeti adatkezelési céllal.[31]

Egy blokkláncos adatkezelés csak akkor felelhet meg a célhoz kötött adatkezelés és adattakarékosság elveinek, ha az adatkezelési céllal összeegyeztethető az ilyen jellegű tárolás. Vannak olyan adatkezelések, amelyek alapvetően nem alkalmasak erre. Például egy, az érintett hozzájárulásán alapuló adatkezelés szinte soha, hiszen a hozzájárulás visszavonása esetén a GDPR által előírt törlési kötelezettség[32] teljesítése első ránézésre lehetetlen. De olyan jogszabályi felhatalmazáson alapuló adatkezeléseknél, mint például az ingatlan-nyilvántartás vezetése,[33] vagy a levéltári adatkezelések, már könnyebb a helyzet, hiszen ezeknél a cél valamennyi adat megőrzése, és az azokkal végzett műveletek pontos és részletes vezetése. Világos tehát, hogy egy adott blokklánc alapú adatkezelés GDPR-megfelelősége a célhoz kötöttség és adattakarékosság szempontjából csak esetről esetre ítélhető meg teljes bizonyossággal, és különös figyelmet kell fordítani a megfelelő adatkezelési jogalap kiválasztására is. Amennyiben a blokklánc-technológia adattárolással kapcsolatos sajátosságai összeegyeztethetőek az előre meghatározott legitim céllal, úgy az adattakarékosság elvének való megfelelés sem lesz többé problematikus.

Amennyiben a blokkláncon alapuló adatkezeléshez automatikus döntéshozó algoritmusokat is igénybe kíván venni az adatkezelő, úgy természetesen ezen adatkezelési műveletnek is vizsgálni kell a fenti alapelveknek való megfelelését. Véleményem szerint, amennyiben a blokkláncon alapuló adatkezelés célja összeegyeztethető a technológia adattárolási sajátosságaival, úgy az abban kezelt adatokat használó automatikus döntéshozó alkalmazás működése is általában összeegyeztethető lesz vele. Ennek oka, hogy az adatok tárolásának alapja maga a blokklánc alapú adatbázis, arra csupán „ráépül" az automatikus döntéshozatal. Ettől függetlenül persze indokolt vizsgálni a rendszer megfelelését a GDPR automatikus döntéshozatalra vonatkozó, különös szabályainak is (lásd a 2.3. pontban írtakat).

Hangsúlyozom azonban, hogy az adatok rendszerbe történő betöltése előtt tisztázni kell, hogy pontosan milyen feladat elvégzése céljából használjuk az adatokat, és a használt adatok körét a cél szempontjából relevánsakra szükséges korlátozni.[34] Ez a későbbiekben ismertetett, beépített adatvédelem elvének érvényesülése szempontjából is kulcsfontosságú követelmény (lásd a 3. pontban).

[31] Finck: i. m., 65.

[32] GDPR 17. cikk (1) bekezdés *b)* pontja: *„Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, az adatkezelő pedig köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje, ha (…) az érintett visszavonja a 6. cikk (1) bekezdésének a) pontja vagy a 9. cikk (2) bekezdésének a) pontja értelmében az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja."*

[33] McMurren, Juliet–Young, Andrew–Verhulst, Stefaan: Addressing Transaction Costs Through Blockchain and Identity in Swedish Land Transfers. *GovLab,* October 2018. https://blockchan.ge/blockchange-land-registry.pdf (2020. 05. 09.).

[34] Datatilsynet: i. m., 11.

2.5. Az átláthatóság követelménye a blokkláncon alapuló gépi tanulással kapcsolatban

A gépi tanulással kapcsolatban az egyik legtöbbször hangoztatott (nem csak adatvédelmi) aggály, hogy gyakran lehetetlen előre megjósolni, hogy milyen eredményt fog produkálni a rendszer. A használt modell produkálhat olyan eredményt is, amelyre látszólag semmilyen magyarázat nem létezik. Ezt a jelenséget „fekete doboznak" nevezzük.[35]

Tudományos és műszaki területen a fekete doboz olyan készülék, rendszer vagy tárgy, amely kizárólag csak a bemenete, kimenete és átviteli jellemzői alapján vizsgálható, konkrét belső működése ismeretlen, azaz megvalósítása „átlátszatlan" (fekete). Szinte bármire lehet hivatkozni fekete dobozként: tranzisztorra, algoritmusra vagy az emberi elmére. A jelenség leírása *Wilhelm Cauertől* eredeztethető, aki 1941-ben dolgozta ki ezzel kapcsolatos elméletét, de a fogalmat még nem használta. Későbbi követői írták le a jelenséget úgy, mint „fekete doboz" analízis.[36]

Az adatvédelem alapelvei között régóta szerepel a követelmény, hogy az érintett természetes személy számára, akinek az adatait kezelik, az adatkezelésnek átláthatónak kell lennie. Ezt az elvet a GDPR is kifejezetten nevesíti az 5. cikk (1) bekezdés *a)* pontjában. Ezek szerint a személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni. A GDPR tehát a jogszerűség, a tisztességes eljárás és az átláthatóság alapelveit egyszerre nevesíti, így azoknak minden adatkezeléssel kapcsolatban, egymásra tekintettel, és egyszerre kell érvényesülniük.

A kérdés ezért, hogy hogyan lehet úgy adatalapú gépi tanuláson alapuló automatikus döntéshozó rendszereket létrehozni, hogy azok az érintett számára kellően átláthatóan működjenek az általuk produkált eredmények szempontjából, így a kezelt személyes adatok tekintetében megfeleljenek az átláthatóság követelményének. A fekete doboz problémája az átláthatóság kapcsán első ránézésre szinte megoldhatatlan problémának tűnhet az adatkezelők számára.

A GDPR tájékoztatási kötelezettséget ír elő az adatkezelő részére a kizárólag automatizált adatkezelésen alapuló, joghatással vagy hasonlóan jelentős hatással járó döntéshozatallal kapcsolatban.[37] Ennek keretében a következő három információt kell közölni az érintettel: tájékoztatni kell az ilyen típusú adatkezelés tényéről, érdemi tájékoztatást kell adni az alkalmazott logikáról, és arról is, hogy az adatkezelés milyen jelentőséggel, és milyen várható következményekkel bír az érintettre nézve.[38]

A GDPR szerint az adatkezelőknek *érdemi információt* kell adniuk az alkalmazott logikáról. Önmagában így például nem lehet elég az, ha az adatkezelő csak általánosságban közli, hogy például neurális hálózaton alapuló rendszert üzemeltet, mivel az érintett így érdemben vajmi keveset fog megtudni arról, hogy mi történik

[35] Datatilsynet: i. m., 12.

[36] Cauer, Emil–Mathis, Wolfgang–Pauli, Rainer: Life and Work of Wilhelm Cauer (1900–1945). *Proceedings of the Fourteenth International Symposium of Mathematical Theory of Networks and Systems (MTNS2000)*, Perpignan, June 2000, 4.

[37] GDPR 15. cikk (1) bekezdés *h)* pont.

[38] GDPR 13. cikk (2) bekezdés *f)* pont.

az adatkezelés során a személyes adataival. Az érdemi információ viszont azt sem jelenti, hogy az adatkezelőnek feltétlenül bonyolult magyarázatot kell nyújtania az alkalmazott algoritmusokról, vagy hogy az algoritmust teljes egészében fel kellene tárnia. A technológia részletes bemutatása ugyanis a legtöbb esetben lerontaná a tájékoztatás közérthetőségét és hátráltatná a befogadását.[39]

A fentieken túl meg kell még említeni, hogy az adatkezelőnek az adatkezelés *jelentőségéről* és a *várható következményeiről* is tájékoztatnia kell az érintettet. A WP29 vonatkozó iránymutatása szerint ahhoz, hogy ez az információ érdemi és érthető legyen, a lehetséges hatásokra vonatkozó, valós és kézzelfogható példákat kell megadni. Digitális kontextusban az adatkezelők további eszközöket is használhatnak az ilyen hatások bemutatására, és vizuális technikákat vehetnek igénybe egy korábbi döntésük meghozatalának magyarázatához is. Az iránymutatás ebben az esetben összehasonlító alkalmazás biztosítását hozza fel példaként.[40] Ezt a megközelítést az *Oxford Internet Institute* és a londoni *Alan Turing Institute* közös kutatása is kiemeli, megállapítva, hogy az adatkezelők számára egy nyilvános tesztrendszer üzemeltetése lehet a megfelelés kulcsa, mind az alkalmazott logikáról, mind az adatkezelés jelentőségéről és várható következményeiről való tájékoztatás során.[41] Így az adatkezelőnek nem kell kinyitnia a fekete dobozt az érintett előtt, elég, ha megérteti vele, hogy a döntés meghozatala hogyan történt, és ő mit tehet annak érdekében, hogy ügyében más (kedvezőbb) döntés születhessen.[42]

Az átláthatóságnak és tájékoztatási kötelezettségnek való megfelelés kapcsán egy blokklánc alapú rendszer üzemeltetése akár kívánatos is lehet. Ennek oka, hogy a blokkláncban az ott kezelt adatokkal végzett, valamennyi művelet naplózásra és tárolása került az adatbázisban, az pedig valamennyi csomópont számára hozzáférhető. A blokkláncban eltárolt műveletek naplója természetesen csupán a döntések eredményeit tartalmazza; azt, hogy maga a döntés hogyan született meg az automatikus döntéshozó szoftver által, nem feltétlenül. Viszont az adatokon végzett valamennyi művelet tanulmányozható és könnyebben átlátható a felhasználók számára, amelyből akár az algoritmus által hozott döntés mögötti logikára is könnyebben lehet következtetni, illetve könnyebben lehet azt megismerni.

3. A beépített adatvédelem elvének alkalmazása a blokkláncon alapuló, automatikus döntéshozatallal kapcsolatban

3.1. Kollektív adatkezelési mintázatok

A GDPR az adatkezelő és az adatfeldolgozó általános kötelezettségei között említi, hogy az adatvédelmi alapelveknek és a rendelet előírásainak való megfelelés,

[39] Péterfalvi Attila–Révész Balázs–Buzás Péter (szerk.): *Magyarázat a GDPR-ról.* Wolters Kluwer, Budapest, 2018, 158.

[40] WP29 (2017): i. m., 28.

[41] Wachter, Sandra–Mittelstadt, Brent–Russell, Chris: Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR. *Harvard Journal of Law & Technology,* 2018/2, 863–871.

[42] Datatilsynet: i. m., 21–22.

valamint az érintettek jogainak érvényesülése érdekében különböző *garanciákat* kell beépíteniük az adatkezelés folyamatába. Ezek a garanciák olyan megfelelő technikai és szervezési intézkedéseket kell hogy takarjanak, amelyek figyelembe veszik a tudomány és technológia mindenkori állását és a megvalósítás költségeit, továbbá az adatkezelés jellegét, hatókörét, körülményeit és céljait, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázatokat.[43] Az adatkezelőnek megfelelő technikai és szervezési intézkedéseket kell végrehajtania annak biztosítására, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott, konkrét adatkezelési cél szempontjából szükségesek. Ez a kötelezettség vonatkozik a gyűjtött személyes adatok mennyiségére, kezelésük mértékére, tárolásuk időtartamára és hozzáférhetőségükre. Ezek az intézkedések különösen azt kell hogy biztosítsák, hogy a személyes adatok alapértelmezés szerint a természetes személy beavatkozása nélkül ne válhassanak hozzáférhetővé meghatározatlan számú személy számára.[44] A GDPR ezen előírásait nevezik a *beépített és alapértelmezett adatvédelem elvének,* melynek funkciója, hogy az adatkezelésre szolgáló rendszerek kialakítása során már alapértelmezetten figyelembe vegyék a rendeletnek való megfelelést, mind a technikai, mind a szervezési intézkedések szintjén.

Az elvnek való megfelelés természetesen a blokklánc alapú személyes adatkezelés és az erre épülő, automatizált döntéshozó alkalmazások tekintetében is szükséges, így a fejlesztés során mindig alaposan át kell tekinteni, hogy milyen naprakész, az alkalmazott technológiákra alkalmazható technika és szervezési megoldások érhetők el a piacon.

A blokklánc és az erre épülő automatizált döntéshozó rendszerek fejlesztése során egy általános elvet fogalmazhatunk meg, amelynek már a konkrét adatkezelés megkezdése, így a rendszer üzembe helyezése előtt érvényesülnie kell az adatvédelmi megfelelés érdekében. Ezt az elvet a *kollektív adatkezelési mintázatok elvének* neveztem el, amelyet ehelyütt megkísérlek a blokklánc alapú automatizált döntéshozó rendszerekre és az azokban kezelt személyes adatokra alkalmazni.

A blokk mint adattárolási egység bármilyen (digitalizálható) személyes adatot, információt tartalmazhat a lánchoz való hozzáadásának pillanatában. A kezelt adat, információ jellegének csak a meghatározott cél szabhat határt. A blokkláncban végzett adatkezelés működési elveinek kialakítása azonban már jóval az adatok hozzáadása előtt elkezdődik. Az adatkezelő és az adatfeldolgozó feladata, hogy már a működés kialakítása, tehát a rendszer megtervezése és kifejlesztése során figyelemmel legyen az adatvédelmi megfelelésre, a fentiekben ismertetett beépített adatvédelem elve alapján.

Ennek során természetesen vizsgálni kell többek között a fentiekben kifejtett célhoz kötöttség, korlátozott tárolhatóság vagy átláthatóság követelményét, továbbá az érintettnek nyújtott tájékoztatás formáját és az automatizált döntéshozatalhoz szükséges jogalap meglétét is. Ezek azonban csak lépcsőfokok a GDPR-megfelelés útján (amelyekre a fentiekben a téma szempontjából vett jelentőségük miatt tértem

[43] GDPR 25. cikk (1) bekezdés.

[44] GDPR 25. cikk (2) bekezdés.

ki részletesen), az adatkezelőnek ugyanis szem előtt kell tartania a rendelet további előírásainak való megfelelést is.

Az adatvédelmi megfelelésnek vissza kell köszönnie a már éles rendszer működésében. Ez azért is fontos, mivel a blokkláncban az adatok és a velük végzett műveletek megváltoztathatatlan tárolása egyfajta örökös lenyomatként szolgál a megfelelés ellenőrzésére. Az adatokkal végzett műveletek kitörölhetetlen lenyomata jelenti azokat a mintázatokat, amelyek vizsgálata kapcsán megállapítható az adatvédelmi jognak történő megfelelés. Hangsúlyozom, hogy ezek a mintázatok a blokklánc valamennyi, a csomópontok által kezelt kópiájában rendelkezésre állnak, ezért azokat „kollektív adatkezelési mintázatoknak" tekinthetjük. A mintázatok lenyomata akkor is rendelkezésre áll, ha egyébként maguknak a személyes adatoknak a kezelése egy elkülönült adatbázisban, ún. *off-chain*[45] megoldásokat alkalmazva történik.

Amennyiben a blokklánc alapú rendszerben az adatok kezelése során automatikus döntéshozó alkalmazásokat, algoritmusokat is igénybe vesznek, úgy az ilyen alkalmazások által végzett adatkezelési műveletek is visszaköszönnek a kollektív adatkezelési mintázatokban. A mintázatokat vizsgálva így kirajzolódhat előttünk az algoritmus által az adatokkal végzett döntések nagyképe. Az egyes döntések által összeálló mintázatok vizsgálata során jobban megérthetővé válhat az automatikus döntéshozatal háttere, az MI működése. Ez a fekete dobozban lévő folyamatok megértése szempontjából is kulcsfontosságú lehet, ami végső soron megkönnyítheti az egyén tájékoztatását is az automatizált döntéshozatal során alkalmazott logikáról, illetve annak jelentőségéről és várható következményeiről a GDPR 13. cikk (2) bekezdés *f)* pontjában és 22. cikkében foglaltak alapján.

A blokklánc alapon működő, elosztott MI viselkedésének rajzolata ott fog rögzülni a blokkláncot alkotó blokktörténetben, és kollektíven jelen lesz valamennyi csomópont által végzett adatkezelési műveletben. A következőkben egy hasonlattal szeretném megvilágítani a jelenséget, az egyéni emberi tudat és az öröklött társadalmi viselkedési formák példáján.

3.2. Egy hasonlat: Az emberi tudat és a blokklánc alapú elosztott MI közös vonásai

Az emberi tudat működésének kollektív mintázatait korábban már azonosították a pszichológia tudományán belül, ezért érdemes ezzel kezdeni a gondolatmenetet. A pszichoanalitikus iskola képviselői közül *Carl Gustav Jung* mutatott rá az emberi szellemtörténetben bizonyos archetipikus képek, metaforák azonosságára és ismétlődésére az egyes kultúrákban, amelyeket az emberiség „kollektív tudattalanjának" részeiként jellemez, és amelyek az egyéni gondolkodás- és viselkedésmintákban is visszaköszönhetnek. Jung így ír a kollektív tudattalanról:

[45] Az off-chain adatkezelés olyan blokklánc alapú technológiai megoldásokat takar, amely során maguk a személyes adatok nem magában a blokkláncban, hanem egy elkülönült adatbázisban vannak tárolva, de kezelésük hash-kulcsok használatával összeköttetésben áll a háttér-technológiát adó alapadatbázissal, amely már blokklánc alapon működik. Lásd: Mannan, Rosanna–Sethuram, Rahul–Younge, Lauryn: GDPR and Blockchain: A Compliance Approach. *European Data Protection Law Review,* 2019/3, 423–424. (DOI: 10.21552/edpl/2019/3/18).

> A kollektív tudattalan a psziché egy része, amely nemcsak a személyes tapasztalatoknak köszönheti létét, vagyis nem személyesen tettünk rá szert. A kollektív tudattalan tartalmai soha nem voltak tudatosak, és ezért soha nem az egyén tett szert rájuk, hanem teljes mértékben örökölte őket. Míg a személyes tudattalan jobbára komplexusokból áll, addig a kollektív tudattalan archetípusokat tartalmaz. Az archetípus fogalma azt fejezi ki, hogy vannak bizonyos formák a pszichében, amelyek mindig és mindenütt föllelhetőek. A kollektív tudattalan, mint egy második pszichés rendszer egyetemes és személytelen jellegű és mindenkiben azonos.[46]

A tanulmány elején már említett, empirikus és racionalista filozófiai iskolákba való besorolás szempontjából ezek a gondolatok inkább a racionalizmushoz állnak közel, amely szerint az emberi tudat rendelkezik veleszületett, örökölt gondolkodási, viselkedési mintázatokkal.

Az emberi tudatról és az emberiség kollektív tudattalanjáról áttérve az MI vizsgálatára, meg kell említeni *Pokol Béla* könyvét,[47] amely a mesterséges intelligencia társadalmának filozófiai és szociológiai problémáit dolgozza fel, és amelyben több neves szerző gondolatait összegzi a kollektív MI megjelenésének lehetőségéről. *Pokol* is említi az emberiség kollektív intelligenciájának társadalmi korokon átívelő fejlődését, azonban szerinte – és az általa hivatkozott szerzők *(Nick Bostrom, Kevin Kelly)* szerint – emellett a kollektív MI megjelenésével is számolni kell. Az elemzés szerint a mai emberi közösségek kollektív intelligenciájának az MI-be való integrálása révén jöhet létre a kollektív mesterséges intelligencia jelensége (az idézett szerzők ezt „szuperintelligenciának" nevezik). A szerző által hivatkozott *Kevin Kelly* például az MI által feljavított emberi gondolkodás révén az emberi értelem és a gépi értelem összeolvadásán alapuló társadalom kialakulását feltételezi.[48]

Pokol Nicolai Hartmann német filozófus létrétegekről szóló elméletét is bemutatja, amely alapján az emberi társadalom négy létréteg: a fizikai, a biológiai, a lelki és a szellemi létréteg alapján épül fel. Pokol szerint napjainkban a szellemi létrétegbe egyre jobban kezd belefonódni a mesterséges intelligencia. Ennek legjobb példája, hogy a hálózatokon keresztül áramló, emberek által hozzáadott és dinamikusan változó, változtatható adatok társadalmát éljük napjainkban, amely létrehozta az értelem felemelkedését a papíron létező, fizikai rögzítettségből az értelem állandó reflexív lebegésének állapotába. *Kelly* ezt *flowing*nak, a tudás folyékonnyá válásának nevezi, avagy a „folyékony osztott értelem" jelenségének az új adatalapú társadalomban (gondoljunk csak például a közösségi-média-felületeken történő kommunikáció sajátosságaira).[49]

A fentiek alapján az adatalapú társadalomban bárki hozzáadhatja a tudását, információit az emberiség kollektív adattárához, amely az emberiség kollektív gondolkodásának és intelligenciájának lenyomataként jelenik meg. Az algoritmusok által az elme kollektív lenyomatában keresett összefüggések megmutathatják nekünk a gondolkodásunk, tudatunk (beleértve akár a tudattalan tartalmakat is) működésének hasonló mintázatait, összefüggéseit.

[46] Jung, Carl Gustav: *Az archetípusok és a kollektív tudattalan.* Scolar, Budapest, 2017, 51–52.
[47] Pokol Béla: *A mesterséges intelligencia társadalma.* Kairosz, Budapest, 2018.
[48] Pokol: i. m., 71–72.
[49] Pokol: i. m., 111–114.

Amennyiben a blokklánc alapú adatkezelést, és az ezen futó MI-szoftvereket, -algoritmusokat hasonlítjuk az emberi elméhez, azt mondhatjuk, hogy az egyes, konkrét személyes adatokat tároló blokkok jelenthetik az egyén személyes tudata által tárolt információkat. A blokklánc egyes felhasználói folyamatosan újabb adatokat adhatnak hozzá az elosztott adatbázishoz, amely így hasonlatos az emberi elme által élete során megtanult újabb és újabb információkhoz. Az előző pontban kifejtettek alapján az adatkezelés közös, kollektív mintázatai valamennyi blokkban az ember biológiai és társadalmi fejlődése során kialakult, közös pszichés formákhoz, és az ezekből fakadó gondolkodási és viselkedési mintázatokhoz hasonlíthatóak, amelyek valamennyi emberben megvannak, velünk születnek, emberi mivoltunkból fakadnak. Ezt *Jung* gondolatai alapján a kollektív tudattalan archetípusaihoz hasonlíthatjuk. A kollektív mesterséges intelligencia ily módon történő felépítése valóban hasonlatossá teheti annak működését az emberi gondolkodáshoz.

A blokkláncban lévő blokk mint adattárolási egység, így önmagában, megszületése pillanatában – az empirista filozófiai iskolából kölcsönzött fogalommal élve – egy *tabula rasa,* azonban abban csak az adatkezelő által megtervezett kollektív adatkezelési mintázatok alapján történhet a tényleges adatkezelés. Az adatkezelésnek és az adatok alapján az MI által hozott automatikus döntéseknek ezen szabályszerűségek alapján kell megszületniük.

Az adatkezelés kollektív mintázatait a blokklánc alapú adatkezelés tervezési folyamatai során a beépített és alapértelmezett adatvédelem elve alapján kell beépíteni a tervezett projektbe. Ezen követelményt ezért is nevezhetjük a kollektív adatkezelési mintázatok elvének. Az absztrakt, jogi megfelelőséget garantáló mintázatoknak az első blokk létrejöttekor már le kell képeződniük, hogy utána a lánc épülésével továbbterjedjen a szabályrendszer valamennyi blokkban és a blokklánc valamennyi – a csomópontok által kezelt – kópiájában. Talán nem véletlenül nevezik a blokklánc alapú rendszerekben az első blokkot „genezis-blokknak", hiszen ez teremti meg a rendszer működésének alapjait.

4. Összegzés: Az elosztott MI mint a következő nagy adatvédelmi kihívás?

> Kiderült, hogy létrehozni egy istent – ahogy azt az elődeid is tanúsíthatják –, nem egyszerű. Mindenekelőtt adatokra volt szükségünk. És ő volt a mi emberünk. Dempsey gazdag volt, arrogáns. Jó helyen volt, jó időben, az adatvédelmi törvények előtt. És a vállalata, az Incite rendelkezett a világ összes adatával.[50]

Az előzőekben láttuk, hogy a gépi tanuláson alapuló mesterséges intelligencia alkalmas olyan döntéshozó rendszerek kifejlesztésére, amelyek gyorsan és hatékonyan tudnak, az adatok alapján megtanult mintázatokat felhasználva döntéseket hozni. A blokklánc pedig egy olyan adatkezelési rendszert takar, amely az elosztott hálózati struktúrát használva, magas szintű adatbiztonságot garantál, és hatékonyan lehet képes kezelni az elosztott erőforrásokat.

[50] Westworld, 3. évad 5. rész.

Amennyiben a gépi tanulást használó, adatalapú döntéshozó rendszer egy blokklánc technológiát használó adatbázisban kezelt adatokat használ a döntések meghozatalára, úgy a két rendszer vegyítéséről beszélhetünk. Ilyen rendszerre jó példát szolgáltatnak a már korábban bemutatott okosszerződéses alkalmazások, de elképzelhető más adatkezelési célból írt ilyen alkalmazás is. Az adatvédelmi jogi védelem szempontjából természetesen elengedhetetlen, hogy a blokkláncban személyes adatok kezelése is történjen.

Egyes vélemények szerint a mesterséges intelligencia fejlesztése és a blokklánc alapvető működési elvei első ránézésre ellentmondásosnak tűnnek. Ennek oka, hogy az MI hatékony fejlesztése nagy mennyiségű, naprakész, jó minőségű adatállományt kíván meg az algoritmusok megfelelő tanítása, és ezáltal pontos döntések meghozatala érdekében. Ennek eredményeképpen azon adatkezelők járnak jól, akik a legjobb minőségű (naprakész, pontos) adatokkal, és a legfejlettebb technológiával rendelkeznek. A hatékony fejlesztés napjainkban ezért a számítási képesség és az adatok összegyűjtésével, majd egy kézben összpontosításával, centralizálásával történik. Ezzel szemben a blokklánc a centrális kontroll megszüntetésével az erőforrások és adatok elosztásán alapuló technológia, ahol az adatokhoz valamennyi, a hálózatban részt vevő szereplő hozzáférhet.[51] Az első ránézésre ellentmondásos technológiák vegyítése azonban az MI-ipar demokratizálódásához, a kisebb és nagyobb szereplők között az erőforrások és adatok igazságos elosztásához is vezethet.[52] A rendszer akár arra is alkalmas lehet, hogy decentralizált, egymástól független szervezetek ugyanazon mintázatok alapján kezeljenek jogszerűen adatokat, a jelen írás előző pontjában kifejtett elv mentén.

Ezek az elképzelések természetesen jelenleg merőben filozofikusak (és valljuk be, idealistának hatnak), azonban léteznek már a piacon ebbe az irányba mutató MI-fejlesztési projektek, például a decentralizált MI megalkotása céljából fejlesztett *SingularityNET*.[53]

Ahogy viszont arra a fenti – egyelőre csak fikciós forgatókönyvből vett – idézet is rávilágít, a technológia komoly, a társadalmat alapvetően befolyásoló intézmények kiépítésére is alkalmas lehet. A *Westworld* című sorozatban egy, a Föld valamennyi lakosának személyiségéről és szokásairól rendkívül pontos adatokkal rendelkező mesterséges intelligencia előre képes látni az emberi sorsokat, és emiatt az embereknek nyújtott információs társadalommal összefüggő szolgáltatásokon keresztül igyekszik láthatatlanul befolyásolni az életeket, gyakorlatilag megfosztva ezzel az

[51] AI and Blockchain: The intersection of top tech trends. *Skalex,* https://www.skalex.io/artificial-intelligence-blockchain/ (2020. 05. 09.).

[52] Banafa, Ahmed: Blockchain and AI: A Perfect Match? *Open Mind BBVA,* https://www.bbvaopenmind.com/en/technology/artificial-intelligence/blockchain-and-ai-a-perfect-match/ (2020. 05. 09.).

[53] A projekt egyik munkatársa, *Arif Khan* szerint: *„Gondoljunk úgy a blokkláncra, mint egy széles horizontális rétegre, amely átfog különböző kultúrákat, nemzeteket és földrajzi területeket. Mindenkinek hozzáférése lehet ehhez a horizontális réteghez, és kapcsolatba léphet a technológiával, amely így lehetővé teszi az embereknek, hogy nagyon különböző adathalmazokat adjanak ahhoz hozzá és dolgozzanak vele. A központosítottan kezelt adathalmazokhoz képest a blokklánc-alapú adatbázisokat nem kontrollálja semmilyen központi entitás."* Idézi: Wolfson, Rachel: Diversifying Data with Artificial Intelligence and Blockchain Technology. *Forbes,* 20 Nov. 2018. https://www.forbes.com/sites/rachelwolfson/2018/11/20/diversifying-data-with-artificial-intelligence-and-blockchain-technology/#407937894dad (2020. 05. 09.).

emberiséget a szabad akarattól. Igaz, a történet szerint ez az MI egy központi, centralizált rendszeren fut, így tevékenysége egy blokklánc alapú elosztott rendszerhez képest könnyen befolyásolható, vagy akár le is állítható. Egy elosztott alapon működő MI ehhez képest sokkal nehezebben lenne megállítható, így az érintettekre, tehát ránk, emberekre jelentett hatása is sokkal komolyabb lenne. Ezért is fontos már idejekorán elkezdeni az ilyen rendszerek adatvédelmi jogi megfeleléséről szóló tudományos diskurzust. Remélem, a tanulmánnyal hozzájárultam ehhez a párbeszédhez.