Eszteri Dániel*

Elosztott adatbázisok, okoseszközök, automatikus döntések és a GDPR: adatvédelmi kapcsolódási pontok néhány új technológia vizsgálata kapcsán[1]

1. Bevezetés

A mesterséges intelligencia (MI), a dolgok internete (internet-of-things, röviden: IoT) és a blokklánc a technológiai fejlődés olyan területei, amelyek napjainkban egyre több jogi elemzés tárgyát képezik. Jelenleg a jogi szakirodalom hajlamos ezeket a témákat egymástól elkülönítve vizsgálni. Ezek a technológiai megoldások akár közösen alkalmazhatóak, és valószínűleg a jövőben együttesen is meg fognak jelenni a piacon.

Az IoT környezetre csatlakoztatott eszközök egy olyan elosztott típusú hálózaton is csatlakozhatnak egymáshoz, mint amilyen egy blokklánc alapú hálózat. Az egyik lehetséges kapcsolat például a technológiák között, hogy az IoT és a blokklánc biztosítja az adatkezelés és adatfeldolgozás infrastruktúráját és hozza létre annak közös technikai szabályozó közegét, míg az MI pedig próbálja optimalizálni az adatkezelési folyamatokat. A személyes adatokat a felhasználóktól az IoT-eszközök gyűjtik össze és töltik fel a rendszerbe.[2]

Tanulmányomban szeretném azonosítani és megvizsgálni ezeknek a látszólag távoli témáknak az összefüggéseit az Európai Unió általános adatvédelmi rendeletével[3] (GDPR) kapcsolatban. Az elemzésben előfeltételnek tekintem, hogy a személyes adatok kerüljenek kezelésre az IoT rendszerben és a blokkláncban, továbbá valamilyen emberi beavatkozás nélküli automatizált döntéshozatali mechanizmusnak is jelen kell lennie velük kapcsolatban. Egy ilyen rendszer létrehozása, vagyis a blokklánc-alapú MI koncepciója nagymértékben befolyásolhatja az érintettek alapvető jogait és szabadságait, magánszféráját.

Az MI-vel felszerelt blokklánc-alapú adatfeldolgozó rendszerek kockázatot jelenthetnek az egyének jogaira és szabadságaira, mivel még kevésbé kiforrott technológiák köré épülnek. A tanulmány első részében a vizsgált technológiák természetét mutatom be adatvédelmi szempontból, majd a második részben megpróbálom bemutatni a technológiák összekapcsolásából eredő problémákat.

2. A blokklánc technológián alapuló adatkezelés jellemzői

A blokkláncot tulajdonképpen egy adatok tárolására és mozgatására szolgáló rendszerként lehet leírni, amely az úgynevezett „elosztott főkönyvi technológiák” *(distributed ledger technologies)* egyik gyakorlatban is megvalósított, leggyakrabban előforduló képviselője. Az

* daniel.eszteri@outlook.com, jogász, a Nemzeti Adatvédelmi és Információszabadság Hatóság Incidensbejelentési Osztályának vezetője, az Eötvös Loránd Tudományegyetem Jogi Továbbképző Intézet és a Nemzeti Közszolgálati Egyetem megbízott oktatója adatvédelmi jogból.

[1] A kutatás a Társadalomtudományi Kutatóközpont Jogtudományi Intézetében valósult meg. A tanulmány a 138965. számú NKFIH pályázat és a Mesterséges Intelligencia Nemzeti Laboratórium keretében készült, az Innovációs és Technológiai Minisztérium, valamint a Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal támogatásával.

[2] Sandner P. et. al. (2020) Convergence of Blockchain, IoT, and AI, Front. Blockchain 3:522600, Online: https://doi.org/10.3389/fbloc.2020.522600, pp. 1-2.

[3] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet). *Az Európai Unió Hivatalos Lapja* (2016/L-119/1). Online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

elosztott főkönyv olyan tranzakciós adatbázis, amely több számítógépből álló hálózaton oszlik el, nem pedig központi helyen tárolják.[4] A hálózaton nincs alá-fölé rendeltségi viszony az egyes számítógépek között. Az elosztott hálózatra kapcsolódó gépek úgynevezett csomópontokként (angolul: *node*-okként) funkcionálnak és így 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.[5] A blokkláncban kezelt adatcsomagok bármilyen információ tárolására, kezelésre alkalmasak lehetnek, így maga a technológia univerzálisan használható szinte bármilyen adatkezelési célra.[6]

A blokklánc-technológiát használó hálózatokon az adatok tárolása az úgynevezett blokkokban történik. Ezekben az adattárolási egységekben bármilyen információ eltárolható, az adott blokklánc létrehozásának céljától függően. Az információkat tartalmazó blokkok láncszerűen, utólag megváltoztathatatlanul kapcsolódnak egymáshoz, ami annyit jelent, hogy az újabb blokkokat és a bennük lévő új adatokat mindig csak a lánc végére lehet felfűzni. 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 csak hozzárendeli az egyes adatokhoz 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, vagy hozzáférés joga kit illet meg.[8]

A láncszerűen felépülő és így egyre növekvő adatbázishoz az újabb adatokat újabb blokkokban adják hozzá. A blokkokban tárolt adatokkal végzett valamennyi művelet naplóját is az egyes blokkokban tárolják, a tranzakciók összefoglalása pedig az úgynevezett Merkle-fát eredményezi.[9] Ezen műveletek naplóját nevezzük összefoglaló néven „blokktörténetnek".

A hálózatra kapcsolódott számítógépek (az úgynevezett csomópontok) feladata az, hogy a blokkokban tárolt adatokkal végzett adatkezelési műveletek hitelességét algoritmikus úton ellenőrizzék.[10] A művelet jóváhagyása során azt ellenőrzik, hogy a tranzakció digitálisan megfelelően alá van-e írva a műveletet indítványozó felhasználó által, és van-e bármilyen hiteles előzménye a blokkláncon.

Amennyiben a csomópontok (vagy előre meghatározott számú csomópont) jóváhagyják a műveletet, úgy az rögzítésre kerül a blokkban, ami ezentúl megmásíthatatlanul hozzákapcsolódik a teljes lánchoz.[11]

A blokkláncot legegyszerűbben egy olyan adatkezelési technológiának írhatjuk le a fentiek alapján, amely az adatok kezelését egy közös, elosztott hálózaton teszi lehetővé, amely központi

---

[4] Európai Központi Bank. (2017) *How could new technology transform financial markets? 19th April 2017.* Online: www.ecb.europa.eu/explainers/tell-me-more/html/distributed_ledger_technology.en.html

[5] Győrfi András et .al.: *Kriptopénz ABC.* Budapest, HVG Könyvek, 2019., pp. 57–59.

[6] Például a blokklánc egyes szerzők szerint jó eszközként használható identitáskezelési célokra. In: Shraddha, K. (2018) Building-Blocks of a Data Protection Revolution. The Uneasy Case for Blockchain Technology to Secure Privacy and Identity, Munich Intellectual Property Law Center - MIPLC Studies, Vol. 35., 1. Auflage 2018, Online: doi.org/10.5771/9783845294025. pp. 31–33.

[7] Győrfi et. al., 2019., p. 61.

[8] A Nemzeti Adatvédelmi és Információszabadság Hatóság állásfoglalása a blokklánc („blockchain") technológia adatvédelmi összefüggéseivel kapcsolatban, Online: https://naih.hu/files/Adatved_allasfoglalas_naih-2017-3495-2-V.pdf, p. 3.

[9] Frankenfield, J. (2021) Merkle Root (Cryptocurrency). Online: https://www.investopedia.com/terms/m/merkle-root-cryptocurrency.asp

[10] Hossein Kakavand – Nicolette Sevres De Kost – Bart Chilton: The blockchain revolution: An analysis of regulation and technology related to distributed ledger technologies. *SSRN Electronic Journal,* (2017). Online: http://dx.doi.org/10.2139/ssrn.2849251. pp. 4–7.

[11] Győrfi et al. 2019., pp. 63., 68.

ellenőrző szerv felügyelete nélkül is működőképes. Az adatokkal végzett műveletek hitelesítése a hálózaton algoritmikus alapú önellenőrző mechanizmusokkal biztosított.

3. Az internet-of-things, avagy dolgok internete a személyes adatok kezelése szempontjából

A dolgok internete, avagy internet-of-things (röviden: IoT) fogalma a Massachusettsi Műszaki Egyetemen (Massachusetts Institute of Technology, MIT) született meg, és alapvetően egy teljesen összekapcsolt eszközökkel teli világot takar, ahol a különböző interoperábilis folyamatok együttesen automatizálhatóak.[12]

Az Európai Adatvédelmi Testület elődjének tekinthető ún. 29. cikk szerint működő Adatvédelmi Munkacsoport (angol rövidítéssel: WP29) 2014-ben tett közzé egy véleményt az IoT jelenséghez kapcsolódóan. A jelentés szerint IoT-nak nevezzük az olyan infrastruktúrát, amelyben a szenzorokkal felszerelt használati eszközök, tárgyak más tárgyakkal vagy emberekkel vannak összekapcsolva, és a szenzorok adatokat rögzítenek, kezelnek, tárolnak és közvetítenek, és a hálózati kapacitások használatával az egyedi azonosítókkal való társítás révén más eszközökkel és rendszerekkel lépnek interakcióba.[13]

Az OECD szerint az IoT egy olyan ökoszisztéma, amelyben a fizikai világot észlelő vagy azzal érintkező eszközök által gyűjtött adatok irányítják az alkalmazásokat és a szolgáltatásokat.[14] Az amerikai megközelítés szerint az IoT általában olyan technológiákra és eszközökre utal, amelyek lehetővé teszik különböző eszközök vagy dolgok hálózati kapcsolódását és interakcióját olyan helyeken, mint épületek, járművek, közlekedési infrastruktúrák, vagy otthonok.[15]

Az IoT legjelentősebb alapeleme, szolgáltatási rétege a „dolgok” összekapcsolását, az adatátvitelt, a gép-gép közti kommunikációt biztosító technikai megoldás, átviteli csatorna, melyet a távközlési szaknyelv az M2M (machine-to-machine) megnevezéssel jelöl. Az M2M így az IoT szükséges előfeltételének, részelemének tekinthető.[16]

Az IoT a kiterjedt adatkezelés elvén működik, amely technológia során az eszközökben a szenzorokat arra tervezték, hogy akadálytalanul kommunikáljanak egymással és váltsanak egymás között adatokat. Több szereplő vesz részt egy ilyen rendszer felépítésében, így különösen az eszközök gyártói, az applikációk tervezői, az adatok feldolgozásában résztvevők, az adatok elemzői. Az adatok útja az IoT világában könnyen teljesen követhetetlenné válik az adatalany számára. Minél több tárgy kapcsolódik be a hálózatba, annál részletesebb adatokat lehet gyűjteni az egyénről, és ilyen módon pedig részletes személyiségprofil alkotható róla. Ennek segítségével egyrészt az érintett teljesen átláthatóvá válhat harmadik személyek számára, másrészt a legmodernebb adatbányász programokkal sok olyan új információ is kinyerhető a rögzített adatokból, amelyek jelentős hatást gyakorolhatnak az egyénekre.[17]

---

[12] Az Európai Gazdasági és Szociális Bizottság véleménye – Bizalom, a magánélet tiszteletben tartása és biztonság a fogyasztók és a vállalkozások számára a dolgok internetén. 2018. https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52018IE1038&from=DA

[13] A 29. cikk szerint működő Adatvédelmi Munkacsoport 8/2014. számú véleménye az Internet-of-Things technológiáról (WP223). 2014. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf, p. 4.

[14] OECD: Consumer Product Safety in the Internet of Things, OECD Digital Economy Papers, 2018.

[15] Consumer Product Safety Commission, USA: Status Report on the Internet of Things (IoT) and Consumer Product Safety, 2019.

[16] Bocsok Viktor – Boldizs Péter Ferenc – Loós Csaba – Major Tamás: A dolgok internete: technologiai háttér, információbiztonsági és adatvédelmi aspektusok. https://fornax.hu/wp-content/uploads/2016/09/Informa%CC%81cio%CC%81biztonsa%CC%81g-e%CC%81s-adatve%CC%81delem-az-IoT-vila%CC%81ga%CC%81banv02jav.pdf, p. 3.

[17] Szabó Endre Győző – Bojnár Katinka – Buzás Péter: Új globális technológiák kihívásai a magyar jogban. In: Tóth András (szerk.): *Technológia jog – Új globális technológiák jogi kihívásai*. Patrocinium Kiadó, 2016., p. 56.

Az Európai Gazdasági és Szociális Bizottság véleménye szerint, mivel az IoT az emberi beavatkozás nélküli automatikus döntéshozatal elvén alapul, garantálni kell, hogy ezek a döntések ne veszélyeztessék a fogyasztók jogait, ne járjanak etikai jellegű kockázatokkal, illetve ne sértsék az alapvető emberi jogokat és elveket.[18]

A IoT-hoz tartozó adatgyűjtő eszközök, szenzorok működésük során több adatforrásból gyűjthetnek adatokat. Ezen adatok lehetnek passzív és aktív gépi, ezen belül is ember üzemeltette, vagy autonóm működésű gépek, illetve közvetlenül ember által generált adatok.[19]

Az IoT jelenségéről elmondható, hogy a technológiával összekötött eszközökön rögzített szenzorok az azokat tartalmazó tárgyak révén javarészt természetes személyekhez kötődnek, ilyen módon pedig a magánszféra érintettsége tetten érhető. Ha pedig a tárgyakhoz kötődő információk egyszersmind a természetes személlyel is kapcsolatba hozhatók, akkor személyes adatoknak minősülnek.[20] Ezért a GDPR 4. cikk 2. pontja szerinti fogalom[21] alapján az IoT-ba kapcsolt eszközök révén a személyes adatok érintettsége miatt adatkezelés történik, többek között azok gyűjtése, rendszerezése, tárolása és felhasználása miatt.

A háztartásban lévő IoT technológiát is felhasználó eszközök adatokat gyűjthetnek arról, hogy az érintett személy mikor tartózkodik otthon, így hogyan alakul a heti rutinja, vagy milyen fogyasztási szokásai vannak. Például az okoshűtője érzékeli milyen ételből mennyit vásárol, az okotévéje pedig, hogy milyen és mennyi multimédiás tartalmat ér el.

Az IoT eszközök, kiváltképp a hordozható típusok (okostelefonok, -órák, -szemüvegek) természetükből adódóan folyamatosan bekapcsolt állapotban vannak, állandóan érzékelnek, adatot gyűjtenek és küldenek, kommunikálnak.[22]

A 29-es Munkacsoport a 05/2014 számú véleményében fejezte ki aggályait az IoT rendszerek elterjedésével kapcsolatban, mely oka többek az, hogy az IoT eszközök esetében az adatelosztás jellegéből adódóan a felhasználó könnyen kerülhet abba a helyzetbe, hogy elveszti a kontrollt az adatai terjedése felett. A biztonsági szempontokon túl azonban megállapításra került, hogy az IoT eszközök által termelt adatok jelenlegi környezetben önmagukban sem elég áttekinthetők a felhasználó vagy az érintettek számára, létrehozva ezzel egy állapotot melyet „információs aszimmetriának" nevezünk, amiben a felhasználónak nincs tudomása arról mely adatai kerültek elosztásra harmadik féllel.[23]

Kitér a 29-es Munkacsoport véleménye továbbá arra a feltételezésre miszerint az IoT felépítéséből adódóan jelenleg nem állnak rendelkezésre megfelelő biztosítékok arra vonatkozóan, hogy az adatkezelés céljának felhasználóval történő tájékoztatásakor eredetileg közölt indok megegyezik azzal az indokkal, mint amelyre az érzékeny személyes adatok gyűjtése valójában megtörtént. Már a 29-es Munkacsoport is felhívta arra a figyelmet, hogy a gyártóknak a tájékoztatók és adatkezelési nyilatkozatok megtartása mellett azok „jogi szöveg" hatású jellegét csökkenteniük kell, hogy a felhasználók felvilágosítása hatékonyabbá váljon, így az egyes eljárások szabványosításával és egységesítésével csökkenthetők a kockázatok, anélkül hogy mindezzel az innováció útjába állnánk.[24] Igaz, a fenti munkacsoporti vélemény

---

[18] Európai Gazdasági és Szociális Bizottság, 2018. op. cit.
[19] Bocsok et. al., op. cit., p. 11.
[20] Szabó – Bojnár – Buzás, 2016., op. cit., p. 56.
[21] GDPR 4. cikk 2. pont: „adatkezelés": a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés.
[22] Ars Boni: Az IoT eszközök térnyerése az adatvédelem tükrében. 2018. https://arsboni.hu/az-iot-eszkozok-ternyerese-az-adatvedelem-tukreben/
[23] Ibid.
[24] Ibid.

még a GDPR alkalmazhatósága előtt jelent meg, annak aktualitása az elmúlt időszakban sem változott.

4. A gépi tanulás általános technológiai háttere

A mesterséges intelligencia és a gépi tanulás technológiai hátterét olyan mértékben szeretném bemutatni, amely szükséges ahhoz, hogy adatvédelmi jogi szempontból megértsük és elemezzük a blokklánc-alapú MI és gépi tanulás modelljét.

A Norvég Adatvédelmi Hatóság (Datatilsynet) jelentése szerint a mesterséges intelligencia olyan rendszer, amely képes saját tapasztalatai alapján tanulni és a különböző helyzetekben szerzett ismereteket összetett problémák megoldására alkalmazni. A koncepció lényege, hogy az MI tanul az általa „látott" személyes adatokból (a gyakorlatban a bemeneti adatokból), és döntéseket vagy „előrejelzéseket" hoz.[25]

A gépi tanulás 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.[26]

A gépi tanulás során az MI-rendszer által végzett adatkezelést három lépcsőre lehet bontani, amelyek a következők: [27]

(1) Először a rendszerbe betáplálnak nagy mennyiségű tesztadatot, 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 úgynevezett *modellt* generál. A rendszer a modell segítségével, a már azonosított minták alapján képes feldolgozni a később általa „látott" (a gyakorlatban betáplált, betöltött) éles adatokat.

(2) Ezek után a rendszerbe újabb adatokat töltenek fel, amelyek hasonlóak a tanuláshoz használt adatokhoz. A korábban generált 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 belétáplált új adatokkal kapcsolatban.

Fontos azt is megjegyezni, hogy a gépi tanulás során létrejövő modell nem feltétlenül tartalmazza a forrásadatokat, amelyek a tanulásának alapjául szolgáltak. A tanulás alapjául szolgáló adatoktól függetlenül is tud működni a legtöbb esetben a gépi tanulás során létrejött MI-rendszer.[28]

A kizárólag automatizált döntéshozatalban tehát nincs emberi részvétel a döntési folyamatban. A gépi tanulás tulajdonképpen az automatizált döntéshozatal előszobájának tekinthető. E szerint a kizárólag automatizált, tehát a gép által meghozott döntést a legtöbb esetben az adatok valamilyen fajta automatikus értékelésének kell megelőznie. Ez az értékelés nagyon sok esetben a rendszer gépi tanulás során elsajátított és beazonosított mintázatai alapján történik.

---

[25] Datatilsynet. (2018) Artificial intelligence and privacy. Online: https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf

[26] Szepesvári Csaba: Gépi tanulás – rövid bevezetés. Előadás, MTA SZTAKI, 2005. március 22. Online: http://old.sztaki.hu/~szcsaba/talks/lecture1.pdf

[27] Datatilsynet, 2018. op. cit., p. 7.

[28] Ibid., p. 10.

5. Automatizált adatkezelés blokklánc-alapon

5. 1. Első megközelítés: okosszerződések

Az elosztott főkönyvi rendszerekkel foglalkozó kutatók már leírták a blokklánc adatkezelési műveleteinek automatizálási lehetőségét algoritmusok futtatásával a hálózaton.

Nick Szabo volt az, aki először – az „okos szerződés" koncepcióját és kifejezését használva 1996-ban az elosztott hálózat adatfeldolgozási műveleteinek automatizálását írta le. Szabó szerint az okos szerződés olyan szerződés, amely automatikusan megvalósul, ha a korábban meghatározott feltételek teljesülnek, így a szerződés gyakorlatilag „önmagát teljesíti" és ezért megszeghetetlen. A feltételek érvényesülése esetén a szerződés teljesítését, biztonságát és megszeghetetlenségét az a számítógépes hálózat biztosítja, amelyikben a felek azt elkészítették, ezért nincs szükség a hitelesítéshez harmadik fél (pl. ügyvéd) közreműködésére.[29]

Amint az a gyakorlatban már látható, a blokklánc egy teljesen életképes technológia az okosszerződéses alkalmazások futtatásához: a felhasználók részére automatikus szerződések megkötésének lehetőségét a blokklánc-alapú platform, az Ethereum vezette be először. Lényegében a hálózaton futó program automatikusan végrehajt egy bizonyos döntést, ha a szükséges feltételek teljesülnek.[30]

Az okosszerződések esetében is a csomópontok hitelesítik a folyamatot és az azzal összefüggésben kezelt adatokat, így a fenti példánál maradva a szerződő felek számlaszámait, az összeget, az időpontokat (pl. határidő), egyéb feltételeket, de akár más személyes adatokat (pl. név) vagy szöveges egyéb információkat (pl. közlemény) is rögzíteni lehet. A szerződés létrejöttét ugyanúgy a csomópontok hitelesítik algoritmikus módon, az adatok és mozgásuk naplója pedig megváltoztathatatlanul rögzül a blokkláncban.[31] Például egy fájlról készített hashkulcs és a tulajdonos neve párokként tárolhatók a hálózaton pl. a tulajdonjog igazolásának céljából. A fájl hash értéke és a blokk időbélyege együtt bizonyítják a szerződés és a tulajdonjog létezését.[32]

Az okosszerződéses alkalmazás az elosztott hálózat minden csomópontján fut, így minden felhasználó használhatja a funkcióit. Az automatizálásért felelős intelligens szerződési alkalmazás kódja és algoritmusa a hálózat minden résztvevője számára elérhető, hozzáférhető és használható.[33]

Az okosszerződéses alkalmazásokat azonban nem szabad összetéveszteni az MI-technikákkal. Az intelligens szerződés alkalmazások önmagukban nem tekinthetők egyszerre MI-alkalmazásoknak is, mivel nem hoznak egyedi döntéseket a blokkláncban kezelt adatok alapján. Az okosszerződések fő célja a legtöbb helyzetben csak a blokkláncon lévő tranzakciók automatizálása és hitelesítése, ha bizonyos feltételek teljesülnek. A legtöbb esetben nem jellemző rájuk túl nagy komplexitás. A fentiek alapján az MI és a gépi tanulás növelheti az

---

[29] Nick Szabó: „Smart Contracts: Building Blocks for Digital Markets" 1996 (részlegesen átdolgozva: 2018), *www.truevaluemetrics.org/DBpdfs/BlockChain/Nick-Szabo-Smart-Contracts-Building-Blocks-for-Digital-Markets-1996-14591.pdf*, p. 8.

[30] Buterin V. (2013): A Next-Generation Smart Contract and Decentralized Application Platform. Online: https://ethereum.org/en/whitepaper

[31] Filatova, N. (2020) Smart contracts from the contract law perspective: outlining new regulative strategies, *International Journal of Law and Information Technology*, Volume 28, Issue 3, Autumn 2020, Online: https://doi.org/10.1093/ijlit/eaaa015, pp. 220–222.

[32] Xing, B. és Marwala T. (2018): The Synergy of Blockchain and Artificial Intelligence. Online: http://dx.doi.org/10.2139/ssrn.3225357, p. 3.

[33] Bacon, J. et. al. (2017) Blockchain Demystified. *Queen Mary School of Law Legal Studies Research Paper* No. 268/2017., p. 29.

intelligens szerződéskötési alkalmazások hatékonyságát, de az alkalmazásuk maguk még nem tekinthetők mesterséges intelligenciának.[34]

5.2. Második megközelítés: az elosztott MI

Visszatérve az MI és a blokklánc kapcsolatára, mint témánk egyik kiindulópontjára: Elképzelhető olyan elemző szoftverek futtatása a blokkláncon, amely képes gépi tanulási technikákkal azonosítani az ott tárolt adatok mintáit. Ebben az esetben a rendszer alkalmassá tehető arra is, hogy az azonosított mintázatok mentén automatikus döntések szülessenek.

A blokklánc-alapú adatkezelést – ahogy azt már a vonatkozó szakirodalom is lefedte – különböző MI technikákkal lehet segíteni vagy továbbfejleszteni.[35]

Véleményem szerint két lehetőség van az MI-alapú alkalmazások futtatására a blokkláncon:

(1) *A blokklánc-alapú gépi tanulási megközelítés:* Az MI elemzi az adatokat a blokkláncban, és megpróbál azokban mintázatokat azonosítani. Ebben az esetben a blokklánc azon adatok tárolási formáját és forrását jelenti, amelyből az MI „tanul", tehát a blokklánc ún. „tanító adatbázist" képez. Később az azonosított minták egy olyan modellt fognak alkotni, amely felhasználható lesz automatikus döntéshozásra. Ebben az esetben a blokkláncban tárolt adatok „csupán" az MI-alapú automatizált adatkezelés tanító adatbázisát szolgáltatják.

(2) *Blokklánc-alapú automatizált döntéshozatali megközelítés:* Az MI ebben az esetben magán a blokkláncban tárolt adatokon fog automatizált adatkezelési műveleteket végre hajtani, valamint megpróbálja optimalizálni is az így születő döntéseket. Ebben a megközelítésben az MI döntései magában a blokkláncban is naplózásra kerülnek (valójában: a blokktörténetben és a Merkle fában), amint azt a tanulmány 2. pontja is jelezte. Véleményem szerint a döntések naplóinak egy példányát külön (nem feltétlenül blokklánc alapú) adatbázisban is lehetne tárolni, de ez alapvetően nem szükséges az ilyen rendszerek működési mechanizmusaihoz.

A blokkláncban kezelt adatokkal automatizált döntéshozó applikációkkal vagy szoftverekkel kapcsolatos projektek gyűjteménye megtalálható a terület legújabb kutatási dokumentumaiban[36] (így pl. Vasco Lopes és Luís A. Alexandre témába vágó tanulmányában is[37]). Ezek szerint a blokklánc-alapú automatizált döntéshozatali alkalmazások mintákat keresnek az adatbázisban, és az azonosított modell alapján hoznak döntéseket.

Jelen tanulmányomban előfeltételnek kívánom a továbbiakban tekinteni, hogy tisztán automatizált (algoritmus-alapú) döntéseket hozzanak a blokkláncban tárolt személyes adatokkal, emberi beavatkozás nélkül.

6. Példák az IoT, a blokklánc és az MI összefonódására

Egy jó példa található Sandner et. al. tanulmányában a blokklánc és az MI összekapcsolásáról IoT környezetben: a hipotetikus példában egy okosvárosban az utcai

---

[34] Schrepel, T. (2021): Smart Contracts and the Digital Single Market Through the Lens of "Law + Technology" Approach. European Commission. Online: https://ssrn.com/abstract=3947174

[35] Xing, B. és Marwala, T. (2018) op. cit., pp. 6-8.

[36] Lásd például a következő tanulmányt a blokklánc-alapú profilalkotás koncepciójáról energiagazdálkodási célokból: Sankaran, S. et. al. (2018) Towards Realistic Energy Profiling of Blockchains for Securing Internet of Things. *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)* Vienna.

[37] Lopes, V. és Alexandre, L. A. (2019) An Overview of Blockchain Integration with Robotics and Artificial Intelligence. *Ledger Journal Vol. 4, Supplement 1 (2019): Proceedings of the First Symposium on Blockchain and Robotics,* MIT Media Lab, Cambridge, MA, 5 December 2018, USA. Online: https://doi.org/10.5195/ledger.2019.171

lámpák hálózata alkotja a blokkláncot, amelyen minden lámpa saját blokkal rendelkezik a hálózaton. Minden lámpa tehát ugyanahhoz a blokklánchoz csatlakozik, a blokkok pedig adatokat tárolnak a lámpák használatáról és teljesítményükről. A hálózaton egy MI-szoftver elemezheti ezeket az adatokat, és optimalizálhatja a lámpahálózat időszakos karbantartását. Javasolhatja azt is például fenntartó felé, hogy a gyakrabban használt lámpákat rendszeresebben tartsák karban.[38]

Ezt a példát alkalmazhatjuk egy olyan rendszerre is, amely már személyes adatokat is kezel: A 29. cikk szerinti munkacsoport egy korábbi véleményében például már elemezte az az intelligens fogyasztásmérő rendszerek adatvédelmi szempontjait. A vélemény előzménye az Európai Bizottság ajánlása volt az intelligens fogyasztásmérő rendszerek bevezetésének előkészítéséről. Az ajánlással összefüggésben az intelligens hálózat[39] „olyan továbbfejlesztett energiahálózatot jelent, amelyhez a szolgáltató és a fogyasztó közötti kétirányú digitális kommunikáció, az intelligens fogyasztásmérő, valamint a monitoring és ellenőrző rendszerek is hozzátartoznak."

Az „okosmérő" továbbá egyben egy olyan elektronikus rendszert is jelent, amely képes mérni az energiafogyasztást, viszont ezen felül több információt is kezel egy hagyományos mérőnél és elektronikus kommunikáción keresztül képes adatokat továbbítani és fogadni. Az intelligens fogyasztásmérők valójában a hagyományos fogyasztásmérők digitális változatának tekinthetők, azzal a különbséggel, hogy az intelligens fogyasztásmérők kétirányú kommunikációs csatornaként működnek a fogyasztók és a szolgáltatók között (pl. villamos energia-, víz-, gázszolgáltatók). Az intelligens fogyasztásmérők előnye, hogy egyszerű és közvetlen módon továbbítják a részletes és valós idejű fogyasztási információkat a szolgáltatónak. A fogyasztók valós idejű mennyiségi adatok alapján nagyon részletes kimutatást kapnak energiafogyasztásukról, ami így könnyen optimalizálhatóvá teszi fogyasztásukat.[40]

Már az ajánlás és a vélemény is nagy figyelmet fordított a tervezéssel és üzemeltetéssel összefüggésben a „beépített és alapértelmezett adatvédelem" elvének követelményeire és érvényesítésére, mivel az ilyen rendszerekben hatalmas mennyiségű, a fogyasztókra vonatkozó személyes adatot dolgoznak fel az egyes szolgáltatók.[41]

Ha Sandner et. al. (blokklánc-alapú utcai lámpák) fent említett hipotetikus példáját alkalmazzuk egy intelligens hálózatra és okosmérőrendszerre, azt mondhatjuk, hogy az egyes háztartások (illetve az ide telepített mérőeszközök) képezhetik a hálózat blokkjait. Ezek a mérőeszközök tárolhatják a fogyasztók víz-, gáz-, villamosenergia-fogyasztására vonatkozó adatokat, és valós időben elküldhetik azokat a szolgáltatóknak. Másrészt egyben MI technológiák elemezhetik a háztartások fogyasztási adatait, és azonosíthatják azokat a fogyasztási mintákat, amelyek segíthetik a fogyasztók közötti energiaelosztás optimalizálását. Az egyes szolgáltatók megoszthatják egymással az azonosított adatfelkezelési mintákat is, hogy szinkronizálják szolgáltatásaikat a jobb minőségű hozzáférés érdekében.

Az ilyen rendszerekben a fogyasztási adatok előzményeit a blokkokban (háztartásokban) is rögzítik, és így azok történetileg nyomon követhetők. Az MI fogyasztás-optimalizálásának hatékonysága a blokkokban is nyomon követhető az egyes háztartások fogyasztási adatainak nyomon követésével. Ez átláthatóbbá teheti a rendszert, és segíthet tovább fejleszteni az

---

[38] Sandner P. et. al. (2020) op. cit., p. 4.

[39] 29. cikk szerinti Adatvédelmi Munkacsoport. (2013) Opinion 07/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force). Online: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp209_en.pdf

[40] Európai Bizottság. (2012) Recommendation on preparations for the roll-out of smart metering systems (2012/148/EU) 9 March 2012. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32012H0148&, 3. pont a)-b) alpontjai

[41] Ibid., 3. pont d)-e) alpontjai

alkalmazott MI- és gépi tanulási-technikákat a jobban működő intelligens hálózat és intelligens fogyasztásmérő rendszer kialakítása érdekében. Az IoT környezetbe összekapcsolt merők, a blokklánc és az MI összefonódása így jól kitűnik ebből a példából.

Az Európai Bizottság és az Európai Beruházási Bank számára készített legutóbbi jelentés azt is megjegyezte egyébként, hogy az energetikában alkalmazható lehet e technológiák összekapcsolása: MI az épületek energiafelhasználásának optimalizálására és blokklánc, hogy megosszák az adatokat az energiaipar egészével a hálózathasználat optimalizálása érdekében.[42]

7. A blokklánc – MI összefonódás egyes adatvédelmi kérdései

7.1. Az automatizált döntéshozatal szabályai a GDPR-ban

A GDPR nem határozza meg az *automatizált döntéshozatal* fogalmát, de ezt a kifejezést többször is használja a normatív szövegben. A *profilalkotás* fogalma viszont szerepel a 4. cikk fogalommeghatározásainak listáján.

E rendelkezés szerint a profilalkotás a személyes adatok automatizált kezelésének bármely olyan formáját jelenti, amely során a természetes személyhez fűződő bizonyos személyes jellemzők értékelése a cél. A profilalkotás célja lehet különösen a természetes személy munkahelyi teljesítményének, gazdasági helyzetének, egészségi állapotának, személyes preferenciáinak, érdeklődésének, megbízhatóságának, viselkedésének, tartózkodási helyének vagy mozgásának elemzése vagy előrejelzése.[43]

A 29. cikk szerinti adatvédelmi munkacsoport (WP29) vonatkozó iránymutatása szerint az automatizált döntéshozatal olyan eljárás, amely során emberi beavatkozás nélkül technológiai eszközök segítségével hoznak meg a személyes adatok kezelése során döntéseket. Ez azt jelenti, hogy a kizárólag automatizált döntéshozatal esetében nincs emberi részvétel a döntéshozatalban.[44]

A GDPR 22. cikkének (1) bekezdése értelmében az érintettnek jogában áll az olyan kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya alól kivonnia magát, amely rá nézve joghatással járna, vagy hasonlóan jelentős hatással lenne rá nézve. Ez a rendelkezés a kizárólag automatizált adatkezelésen alapuló döntéshozatal általános tilalmát jelenti. A rendelet magában foglalja az ilyen döntéshozatali folyamaton alapuló profilalkotást. Ez a tilalom attól függetlenül érvényes, hogy az érintett tesz-e bármilyen intézkedést személyes adatainak kezelésével kapcsolatban. Ezért a GDPR főszabályként általános tilalmat állapít meg a kizárólag automatizált egyedi döntéshozatalra vonatkozóan, amely joghatással vagy hasonlóan jelentős hatással járna az érintett magánéletére, magánszférájára nézve.[45]

Annak érdekében, hogy egy tevékenységet a meghozott döntés tekintetében emberi beavatkozásnak minősítsenek, és ezért a 22. cikk szerinti tilalom ne vonatkozzon rá, az adatkezelőnek gondoskodnia kell arról, hogy a döntés emberi felülvizsgálata érdemleges legyen, és ne csak szimbolikus gesztus. Ezt olyan személynek kell megtennie, aki rendelkezik a döntés megváltoztatására vonatkozó jogkörrel. Más szóval, ahhoz, hogy mentesüljön a tilalom

---

[42] Verbeek A. és Lundquist M. (2021): Artificial intelligence, blockchain and the future of Europe: How disruptive technologies create opportunities for a green and digital economy. Online: https://op.europa.eu/en/publication-detail/-/publication/8730fef5-315c-11ec-bd8e-01aa75ed71a1/language-en, p. 109.

[43] GDPR 4. cikk 4. pont

[44] 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, p. 8.

[45] Veale, M. és Edwards, L. (2018) Clarity, surprises and further questions in the Article 29 Working Party draft guidance on automated decision making and profiling. *Computer, Law and Security Review 34*., p. 400.

alól, a végső döntést egy embernek kell meghoznia, vagy az algoritmus által javasolt döntést felül kell vizsgálnia és jóvá kell hagynia.[46]

Ezenkívül a kizárólag automatizált döntéshozatalra vonatkozó szabályokat csak abban az esetben kell alkalmazni, ha a döntésnek joghatása vagy hasonlóan jelentős mértékű hatása van a természetes személyre nézve. A GDPR nem határozza meg a „joghatás" vagy a „hasonlóan jelentős hatás" fogalmát, de a rendeletnek ez a megfogalmazása egyértelművé teszi, hogy a 22. cikk csak az egyén magánszférájára nézve jelentős következményekkel járó esetekre terjed ki.[47]

A joghatás fogalma megköveteli, hogy a döntés befolyásolja egy személy törvényes jogait, például őt jogszabály alapján megillető vagy egy szerződésen alapuló jogait. A WP29 szerint az ilyen hatások közé tartoznak például a természetes személyekre vonatkozó olyan automatizált döntések, amelyek eredményeként: a szerződéseket felmondják, a törvény által garantált jóléti juttatásokat (például gyermekekkel kapcsolatos juttatásokat vagy lakhatási támogatást) biztosítják vagy elutasítják, az országba való belépést megtagadják, az állampolgárságot megtagadják stb.[48]

Az automatizált döntéshozatalnak az emberek jogaira gyakorolt hatása a törvényben vagy szerződésben meghatározott jogok olyan eseteire vonatkozik tehát, amelyek így viszonylag egyértelműen körülhatárolhatók. Ezenkívül azonban a 22. cikk a homályosabban megfogalmazott „hasonlóan jelentős mértékű hatás" fogalmát is használja, amely szintén a tilalom hatálya alá tartozik. A GDPR (71) preambulumbekezdése tartalmazhat némi iránymutatást ezzel a fogalommal kapcsolatban, mivel a következő példákat sorolja fel: online hitelkérelem elutasítása vagy egyetemi felvételi emberi beavatkozás nélkül.

A 22. cikk (2) bekezdésében meghatározott általános tilalom alól azonban vannak kivételek. Ennek megfelelően a tilalom nem alkalmazható, ha a tisztán automatikus döntés:

(1) az érintett és az adatkezelő közötti szerződés megkötéséhez vagy teljesítéséhez szükséges;
(2) olyan európai uniós vagy tagállami jogszabályi előírás engedélyezi, amely az adatkezelőre vonatkozik, és amely megfelelő intézkedéseket is határoz meg az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében;
(3) az érintett kifejezett hozzájárulásán alapul: A hozzájárulás kifejezésének legvilágosabb módja az érintett írásbeli nyilatkozata. Az Európai Adatvédelmi Testület szerint digitális vagy online kontextusban megfelelő lehet, ha az érintett elektronikus űrlap kitöltésével, e-mail küldésével, az aláírását tartalmazó beszkennelt dokumentum feltöltésével vagy elektronikus aláírással adja meg a hozzájáruló nyilatkozatot. Végül a hozzájárulás kétlépcsős ellenőrzésével is bizonyosságot szerezhetünk annak a GDPR szerinti megfelelőségéről.[49]

7.2. Blokklánc-alapú automatizált döntéshozatal és a GDPR

Ha a személyes adatokat a blokkláncban automatikus döntéshozatali célokkal összefüggésben is kezelik, az adatkezelőnek meg kell felelnie a GDPR fenti követelményeinek. Természetesen mindig a kezelt adatok, az adatkezelés konkrét célja és az érintettre gyakorolt hatása határozza meg, hogy a 22. cikk szabályai alkalmazandók-e vagy sem. Ha igen, az automatizált döntéshozatalt alkalmazó adatkezelés csak akkor lehetséges a blokkláncon, ha az adatkezelő bizonyítani tudja a felsorolt kivételeknek való megfelelést.

[46] 29. cikk Adatvédelmi munkacsoport. (2017) op. cit., p. 22.
[47] Veale, M. és Edwards, L. (2018) op. cit., p. 401.
[48] 29. cikk Adatvédelmi munkacsoport. (2017) op. cit., p. 22.
[49] Európai Adatvédelmi Testület. (2020) Iránymutatás az (EU) 2016/679 rendelet szerinti hozzájárulásról. Online: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf, pp. 20–22.

Az automatizált döntéshozatalra képes blokkláncon futó alkalmazások általános funkciója (beleértve a profilalkotást is bizonyos esetekben) az, hogy a meghozott döntéseik az elosztott hálózatban feldolgozott adatokon alapulnak, és mentesek minden emberi beavatkozástól. Ezekben az esetekben az ilyen rendszerekre a GDPR 22. cikke vonatkozik.

Ha a blokklánc- és IoT-alapú intelligens fogyasztásmérés hipotetikus példáját vesszük a tanulmány 6. pontjából, véleményem szerint az ilyen adatkezelés a 22. cikk hatálya alá tartozik, mivel az automatikus döntések befolyásolják a személyek törvényes jogait (pl. a villamosenergia-ellátáshoz való jogot), és az adatkezelés az érintett (ügyfél) és az adatkezelő (pl. villamosenergia-szolgáltató) közötti szerződésen alapul a legtöbb esetben.

7.3. A célhoz kötöttség és az adattakarékosság elveinek való megfelelés kérdése

A blokklánc-alapú adatkezelés komoly kihívást okozhat a GDPR az adatkezelés célhoz kötöttségét és adatok minimalizálásának (adattakarékosság) elvét kimondó rendelkezéseinek való megfelelést illetően. A célhoz kötöttség elve alapján a személyes adatokat csak meghatározott, egyértelmű és jogszerű célból szabad gyűjteni, és azokat nem szabad az említett célokkal összeegyeztethetetlen módon kezelni.[50] Az adattakarékosság elve szerint a kezelt személyes adatoknak megfelelőnek és relevánsnak kell lenniük az adatkezelés céljai szempontjából, és az e célokkal kapcsolatban szükségesre kell korlátozódniuk.[51] Mindkét elv tiltja a túlzott, felhalmozott, szükségtelenül kezelt és tárolt adatok kezelését.

A blokklánc működésének egyik alapelve az, hogy az összes adat megőrzési időkorlát nélkül tárolódik az adatbázisban, a rajtuk eszközölt műveletek naplójával együtt. Az adatok és azokon végzett adatkezelési műveletek naplója felfűződik a régebbiekre az integritás és a biztonság garantálása érdekében. Az adatokat és tranzakciónaplókat határozatlan ideig tárolják a rendszerben, abból a célból, hogy pontosan nyomon lehessen követni az egyes adatkezelési műveletek és az adatok sorsát. Minden csomópont továbbá az adatbázis teljes másolatát tárolja önellenőrzési célokból. Első látásra ezek a jellemzők ellentétben állnak a GDPR fent említett alapelveivel.[52]

A blokklánc-alapú adatkezelés jogszerűségének megítéléséhez azonban egy fontos előkérdés, hogy az ilyen típusú technológia alkalmazása egyáltalán kompatibilissé tehető-e az bármiféle adatkezelési céllal.[53] Az alapelveknek való megfelelés szempontjából tehát meg kell vizsgálni, hogy a személyes adatok ilyen típusú kezelése (pl. adatok határozatlan ideig történő tárolása a láncban) összeegyeztethető-e az eredeti céllal. Vannak olyan típusú adatkezelések, amelyek alapvetően nem alkalmasak erre. Például az érintett hozzájárulásán alapuló adatkezelés szinte soha sem lesz ilyen, mivel (első látásra) a személyes adatok törlésére vonatkozó kötelezettség teljesítése a hozzájárulás visszavonása esetén nem teljesíthető.[54]

A jogszabályi kötelezettség teljesítésén alapuló adatkezelés, például ingatlan-nyilvántartások[55,56] vagy állami levéltárak vezetése esetén azonban könnyebb a helyzet, hiszen

---

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

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

[52] Finck, M. (2019) Blockchain and the General Data Protection Regulation. European Parliamentary Research Service, PE 634.445. p. 68.

[53] Finck, M. (2019) op. cit., p. 65.

[54] GDPR 17. cikk (1) bekezdés b) pont: 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.

[55] McMurren, J. et. al. (2018) Adressing Transaction Costs Through Blockchain and Identity in Swedish Land Transfers. Online: blockchan.ge/blockchange-land-registry.pdf

[56] Kachorowska, M. (2019) Blockchain-based land registration: Possibilities and challenges. *Masaryk University Journal of Law and Technology, Vol. 13. No. 2*. Online: https://doi.org/10.5817/MUJLT2019-2-8

ezeknek az adatbázisoknak a célja az összes személyes adat és az azokkal végzett valamennyi művelet megőrzése és eltárolása, archiválása. A közérdekű archiválási cél tehát könnyebben állhatja ki az alapelvi megfelelés próbáját blokklánc alkalmazása esetén.

Egy adott blokklánc-alapú adatkezelés ezért csak eseti alapon értékelhető a jogszerűség és a GDPR-megfelelés szempontjából. Tekintettel a célhoz kötöttségre és az adattakarékosságra, különös figyelmet kell fordítani az adatkezelés megfelelő jogalapjának kiválasztására. Ha az adatkezelés előre meghatározott törvényes célja megfelel a blokklánc technológia sajátosságainak, az alapelvi megfelelés már nem lesz véleményem szerint nagyon problémás.

Ha az adatkezelő automatikus döntéshozatali algoritmusokat kíván használni a blokklánc alapú adatkezeléshez, természetesen ezt a műveletet is meg kell vizsgálni a fent említett elveknek és a GDPR 22. cikkének való megfelelés szempontjából.

Véleményem szerint, ha az adatkezelés célja összeegyeztethető az alkalmazott technológia jellemzőivel, akkor a kezelt adatok felhasználásával működő automatikus döntéshozatali alkalmazás működtetése is összeegyeztethető lesz vele a legtöbb esetben. Az adatokat magában a blokkláncban tárolják, az automatikus döntéshozatal pedig az adatbázisra „épül rá". Mindazonáltal azt is fontos megvizsgálni, hogy a rendszer megfelel-e a GDPR automatikus döntéshozatalra vonatkozó különös szabályainak.

Hangsúlyozom azonban, hogy mielőtt adatokat töltenének be a rendszerbe, pontosan tisztázni kell, hogy milyen feladatra használják fel az adatokat, és ezért korlátozni kell a felhasznált adatok körét a cél szempontjából releváns adatokra. Ez a beépített adatvédelem elvének alkalmazása szempontjából is kulcsfontosságú követelmény, amelyet később ismertetek.[57]

7.4. Az átláthatóság elvének való megfelelés kérdése

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 kérdés ezért az, hogyan lehet úgy a gépi tanulást használó 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. Az adatkezelés átláthatóságának jogi követelménye ezért komoly problémák elé állíthatja az MI-megoldásokon alapuló adatkezelést fejlesztő vállalkozásokat.

A GDPR a fenti problémát úgy próbálja meg áthidalni, hogy tájékoztatási kötelezettséget ír elő az adatkezelő részére a kizárólag automatizált adatkezelésen alapuló, joghatással vagy hasonlóan jelentős hatással járó döntéshozatallal kapcsolatban, amelyet személyes adatok kezelésével hoznak. A rendelet beleérti ebbe a körbe az ilyen adatkezelésen alapuló profilalkotást is.[58] Ennek keretében a következő három információt kell közölni az érintettel:

(1) tájékoztatni kell az ilyen típusú személyes adatkezelés tényéről;

(2) érdemi tájékoztatást kell adni az alkalmazott logikáról;

(3) és végül arról is, hogy az adatkezelés milyen jelentőséggel és milyen várható következményekkel bír az érintettre nézve.[59]

---

[57] Európai Unió Alapjogi Ügynöksége (2019) Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights. Online: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-data-quality-and-ai_en.pdf, p. 10. Lásd továbbá: Datatilsynet. (2018) op. cit., p. 11.

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

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

Az automatizált egyedi döntéshozatal tényének közlése viszonylag egyszerű követelmény, ennek keretében elég, ha az adatkezelő arról tájékoztat, hogy ilyen típusú adatkezelésre kerül sor. Fontos, hogy az érintett arról is tudomással bírjon, ha az automatizált egyedi döntéshozatal kapcsán egyben profilalkotásra is sor kerül.

Az alkalmazott logikáról való tájékoztatás miléntje már több kérdést vet fel. Ez főleg a gépi tanulási módszerek esetében jelenthet nagy kihívást az adatkezelő részére, mivel az sokszor rendkívül összetett, nagyon nehezen átlátható adatkezelési folyamatokon alapul.

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 pl. neurális hálózaton alapuló rendszert üzemeltet, mivel az érintett így érdemben vajmi keveset fog felfogni arról, hogy mi történik az adatkezelés során a személyes adataival.

Az érdemi információ viszont azt sem jelenti, hogy feltétlenül bonyolult magyarázatot kell nyújtania az alkalmazott algoritmusokról, vagy azt, hogy az algoritmust teljes egészében fel kellene tárnia az adatkezelőnek. A technológia részletes bemutatása ugyanis a legtöbb esetben lerontaná a tájékoztatás közérthetőségét, és hátráltatná a befogadását.[60] Emellett maga a GDPR is kimondja, hogy az alkalmazott logikáról való tájékoztatás nem érinti az üzleti titkokat vagy a szellemi tulajdont, így a szoftverek védelmét biztosító szerzői jogokat.[61] A technológia komplexitása természetesen nem lehet mentség a tájékoztatás teljes mellőzésére sem.

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 letárolása került az adatbázisban, az pedig valamennyi csomópont számára hozzáférhető. A blokkláncban letárolt 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 azt megismerni.

8. A beépített adatvédelem érvényesülése az elosztott adatbázisokon alapuló automatikus döntéshozatalban

8.1. a blokkláncon végzett adatkezelési műveletek lenyomata

A GDPR az adatkezelő és az adatfeldolgozó általános kötelezettségei között megemlíti, hogy az adatvédelmi elveknek és a rendelet követelményeinek való megfelelés, továbbá az érintetti jogok védelme érdekében különböző garanciákat kell beépíteniük az adatkezelési folyamatokba. Ezeknek a garanciáknak ki kell terjedniük a megfelelő technikai és szervezési intézkedésekre, amelyek figyelembe veszik a tudomány és technika állását és a végrehajtás költségeit, az adatkezelés jellegét, hatókörét, körülményeit és céljait, valamint a különböző valószínűségű és súlyú, a természetes személyek jogait és szabadságait érintő kockázatokat. Az adatkezelő megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítása érdekében, hogy alapértelmezés szerint csak az adott adatkezelési célhoz szükséges személyes adatokat kezeljen. Ez a kötelezettség az összegyűjtött személyes adatok mennyiségére, feldolgozásának mértékére, tárolásának időtartamára és rendelkezésre állására vonatkozik. Ezeknek az intézkedéseknek különösen azt kell biztosítaniuk, hogy a személyes adatokhoz alapértelmezés szerint nem férnek hozzá meghatározatlan számú személyek az adatkezeléssel érintett természetes személy beavatkozása nélkül. A GDPR ezen rendelkezéseit a beépített és

[60] Péterfalvi Attila – Révész Balázs – Buzás Péter (szerk.): *Magyarázat a GDPR-ról*. Wolters Kluwer, Budapest, 2018., p. 158.
[61] GDPR (63) preambulumbekezdés

alapértelmezett adatvédelem elvének nevezik, amelynek feladata, hogy már adatkezelés tervezésekor figyelmet fordítsanak a rendelet előírásainak való megfelelésre.[62]

Ennek az elvnek a betartása is szükséges a blokklánc-alapú adatkezelés során és az azon alapuló automatizált döntéshozatali alkalmazásoknál. A fejlesztőknek ezért mindig alaposan meg kell vizsgálniuk az alkalmazott technológiával kapcsolatban a piacon elérhető naprakész technikai és szervezési megoldásokat.

Ez azt jelenti, hogy az IoT környezetre alkalmazott elosztott-alapú automatizált döntéshozatali rendszerek fejlesztési és tesztelési folyamata során is vizsgálni kell az adatvédelmi megfelelést, jóval az éles üzemelés megkezdése előtt. Ily módon az adatvédelmi megfelelés akkor is megjelenik, amikor majd az élő rendszer ténylegesen működni kezd.

A következő elmélet a fent említett elv követésére szolgál: IoT környezetben az egyes eszközöket (pl. okosmérő) és bennük tárolt adatokat az egyes blokkok jelenítik meg, amely így elosztott alapú hálózatot alkot. A blokkok adattároló egységként bármilyen (digitalizálható) személyes adatot vagy információt tartalmazhatnak a lánchoz való hozzáadásukkor. A kezelt adatok és információk jellegét csak a konkrét cél korlátozhatja.

A blokklánc-alapú adatkezelés működési elveit már azelőtt megtervezik, hogy élő személyes adatokat adnak hozzá a rendszerhez. Az adatkezelő és az adatfeldolgozó felelőssége, hogy a rendszer fejlődésének korai szakaszában is figyelembe vegye az adatvédelmi megfelelést, a fent leírt beépített adatvédelem elve alapján. Ennek során meg kell vizsgálni többek között a célhoz kötöttség és a korlátozott tárolhatóság elveinek érvényesülését, valamint az érintett tájékoztatásának formáját és az automatizált döntéshozatal jogalapjának meglétét. Ezek természetesen csak lépések a GDPR-megfelelés útján, mivel az adatkezelőnek értékelnie kell a rendelet további követelményeinek való megfelelést is.

Ez azért is fontos, mert az adatok megváltoztathatatlan tárolása és az összes adatkezelési művelet naplózása a blokkláncban egyfajta örökös lenyomatként szolgálhat a megfelelés ellenőrzéséhez. A blokkokban végzett adatkezelési műveletek kitörölhetetlen lenyomata olyan adatkezelési mintákat mutathat, amelyekben az adatvédelmi jogszabályoknak való megfelelés is vizsgálható. A minták a blokklánc összes csomópontja által letárolt másolatban elérhetőek. Véleményem szerint ezeknek a mintáknak a lenyomata akkor is tanulmányozható, ha a személyes adatokat egyébként külön adatbázisban kezelik, úgynevezett off-chain megoldásokkal.[63]

8.2. Az MI működésének lenyomata a blokkláncban?

Ha a személyes adatok kezelés során automatikus döntéshozatali alkalmazásokat és algoritmusokat használnak a blokklánc-alapú, elosztott rendszerben, az ilyen alkalmazások által végzett adatkezelési műveletek nyomon követhetők a rendszer naplójában is (a blokktörténetben és a Merkle-fában). Véleményem szerint az MI által hozott döntések lenyomata a személyes adatokkal nyomon követhető, amikor az MI adatkezelési műveleteket hajt végre a blokkláncon és megpróbálja optimalizálni a döntéseket a tanulmány 5.2. pontjában kifejtetteknek megfelelően („blokklánc-alapú automatizált döntéshozatali megközelítés"). Ebben a megközelítésben az MI algoritmus döntéseinek eredményei is eltárolásra kerülnek a blokklánc elosztott adatbázisában. Egy okosmérő-hálózatban így például naplózásra kerül az egyes blokkokban (tkp. magában a mérőeszközökben), hogy a hálózat működésének optimalizálás során milyen döntéseket hozott az MI.

---

[62] GDPR 25. cikk (1)-(2) bekezdései

[63] Az „off-chain" vagy adatok „láncon kívüli" kezelése egy olyan technológiai megoldás, amelyben a személyes adatokat egy külön adatbázisban tárolják, nem pedig magában a blokkláncban. Az off-chain adatbázis hash-kulcsokkal csatlakozik a „mag-adatbázishoz", amely már blokklánc-alapú. Lásd: Mannan, R. et. al. (2019) GDPR and Blockchain: A Compliance Approach. *European Data Protection Law Review 3/2019.*, pp. 423-424.

Az automatizált műveletek lenyomatának vizsgálatával láthatjuk a teljes képet azokról a döntésekről, amelyeket az algoritmus hoz az adatokkal. Az egyes döntések által követett minták vizsgálatával jobban megérthetjük az automatikus döntéshozatal hátterét és az MI működését. Ez döntő fontosságú lehet a rendszerben zajló folyamatok megértéséhez is, amelyek végső soron megkönnyíthetik az automatizált döntéshozatal során alkalmazott logika, valamint annak az egyénre gyakorolt várható hatásainak megértését és az erről való tájékoztatást.

Fontos kihangsúlyozni, hogy a blokklánc-alapú elosztott MI viselkedésének lenyomata a blokkokban kerül eltárolásra és együttesen jelen lesz az összes csomópont által kezelt kópiában is, egy okosmérő-hálózat esetén így valamennyi háztartásba telepített mérőeszközben. Az MI működésének lenyomatáról a fő forrás pedig a blokktörténet lehet.

Természetesen tisztában vagyok azzal, hogy a fenti elmélet egyelőre erősen hipotetikus, azonban úgy gondolom, hogy tudományos és gyakorlati érdemei lehetnek az ilyen rendszerek munkájának megtervezésekor vagy működésük megfigyelésében. Ily módon a különböző nagy adatkezelők automatizált módon kezelhetik a személyes adatokat a blokklánc-megoldások által kínált minták és elvek alapján.

A blokklánc működése során létrejövő adatkezelési mintázatok vizsgálata jó eszközként szolgálhat ahhoz, hogy a beépített adatvédelem elvének való megfelelést is tanulmányozzuk azon keresztül. Amennyiben a kezelt adatokkal történő automatikus döntéshozatalra képes alkalmazások is futnak a blokkláncon, úgy az adatkezelési mintázatokban az MI működésének lenyomatát is meg lehet vizsgálni.

A blokklánc épülése közben így az adatvédelmi jogi megfelelőség az adatkezelési mintázatokban rajzolódhat ki. Ezek a mintázatok a csomópontok által kezelt összes kópiában megtalálhatóak. Később pedig az MI működésének lenyomata is tanulmányozható a blokktörténetben. Ezek a funkciók segíthetnek a későbbi adatvédelmi megfelelőség finomhangolásában is.

9. Összegzés: a blokklánc és az MI összefonódásának adatvédelmi kockázatai

Fentebb láttuk, hogy elméletileg lehetséges olyan összetett, elosztott alapú rendszerek kifejlesztése, amelyek gyorsan és hatékonyan hozhatnak döntéseket a személyes adatokból tanult minták felhasználásával. Azt is láttuk, hogy a blokklánc egy olyan adatkezelési rendszer, amely elosztott hálózati struktúrát használ a magas szintű adatbiztonság biztosítása és az elosztott erőforrások hatékony kezelése érdekében. Ha egy gépi tanulási rendszer egy blokklánc adatbázisban kezelt személyes adatokat használ a döntések meghozatalához, akkor ez a két rendszer ötvözete. Amennyiben pedig az egyes blokkok a hálózatra csatlakoztatott felhasználói eszközöknek felelnek meg, úgy az ilyen rendszer alkalmassá tehető egy IoT-környezet kialakítására is. A tanulmányban erre az intelligens-fogyasztásmérő rendszereket hoztam példaként.

Egyes vélemények szerint első látásra az MI fejlesztése és a blokklánc alapvető működési elvei ellentmondásosnak tűnnek. Ennek az az oka, hogy az MI hatékony fejlesztéséhez nagy mennyiségű naprakész, kiváló minőségű adatra van szükség az algoritmusok megfelelő tanításához és ezáltal pontos döntések meghozatalához.[64] Ezért azok az adatkezelők vannak előnyben, akik a legmagasabb minőségű (naprakész, pontos) adatokkal és a legmodernebb technológiával rendelkeznek. A hatékony fejlesztést ezért ma nagy mennyiségű kiváló minőségű adat összegyűjtésével hatalmas számítási kapacitás mellett végzik, jellemzően egy kézben összpontosítva és központosítva. A blokklánc viszont egy olyan technológia, amely az erőforrások és adatok elosztásán alapul a központi ellenőrzés megszüntetésével, ahol az adatokhoz a hálózat minden szereplője hozzáférhet. Ezeknek az ellentmondásos

[64] Európai Unió Alapjogi Ügynöksége (2019) op. cit., pp. 10-12.

technológiáknak a keverése[65] azonban az MI-ipar demokratizálódásához, valamint az erőforrások és adatok igazságos elosztásához is vezethet a kisebb és nagyobb szereplők között.[66] Azt is meg lehet állapítani, hogy az ilyen rendszerek decentralizált jellege akár arra is képessé teheti a független szervezeteket, hogy az adatokat ugyanazon adatkezelési mintázatok alapján jogszerűen dolgozzák fel, összhangban a GDPR beépített adatvédelemről rendelkező elvével. Vannak egyébként már olyan MI fejlesztési projektek a piacon – ilyen például a SingularityNET is –, amelyek a decentralizált MI létrehozását tűzték ki célul.[67]

Fontos azonban azt is hangsúlyozni, hogy az érintettekre, azaz az emberekre gyakorolt hatás szempontjából az adatvédelmi kockázatok meglehetősen magasak lennének az ilyen rendszerek üzemeltetése során, mivel egyelőre meglehetősen kiforratlan technológiákról beszélünk. Ezért is fontos, hogy már idejekorán elinduljon a tudományos diskurzus arról, hogy az ilyen rendszerek megfeleltethetők-e az adatvédelmi jogszabályoknak, így Európai Uniós szinten a GDPR-nak. Remélem, hogy a jelen tanulmánnyal hozzájárultam ehhez a párbeszédhez.

---

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

[66] Banafa, A. (2019) *Blockchain and AI: A Perfect Match?* Online: https://www.bbvaopenmind.com/en/technology/artificial-intelligence/blockchain-and-ai-a-perfect-match/

[67] A projektcsapat egy munkatársa, Arif Khan szerint: *„Gondoljunk úgy a blokkláncra, mint egy széles horinzontális rétegre, amely átfog különböző kultúrákat, nemzeteket és földrajzi területeket. Mindenkinek hozzáférési lehet ehhez a horizontális réteghez és kapcsolatba léphet a technológiával, amely lehetővé teszi így 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: Rachel WOLFSON: Diversifying Data with Artificial Intelligence and Blockchain Technology, Online: https://www.forbes.com/sites/rachelwolfson/2018/11/20/diversifying-data-with-artificial-intelligence-and-blockchain-technology/#407937894dad