Eszteri Dániel

Az új technológiák megjelenésének hatása a személyes adatok védelmére: gépi tanulás, blokklánc, internet-of-things, agyhullám-olvasás

1. Bevezetés

Az „új technológia" kifejezés nem hangzik idegenül az adatvédelemmel foglalkozó szakembereknek, kutatóknak. Maga az Európai Unió 2018-ban alkalmazandóvá vált általános adatvédelmi rendeletében[1] (közkeletű angol rövidítéssel: GDPR) is szerepel a kifejezés több helyen, holott annak pontos fogalmát az nem határozza meg. Ez nem véletlen, hiszen az új technológia kategóriájába tartozó konkrét eszközök, adatkezelési megoldások időről-időre változnak, attól függően, hogy azok mennyire lesznek kiforrottak a tudomány és technika fejlődésével az adott területen, és az alkalmazásuk által jelentett kockázatokat mennyire sikerült a társadalom és a tudományos élet képviselői által is elvárható szintre lecsökkenteni. Amíg például egy ujjlenyomat-alapú azonosítórendszerre 25-30 évvel ezelőtt még kétségkívül új technológiaként tekintettek, ma már nem feltétlenül kezelik azt akként. Gondoljunk csak bele, hogy ma már teljesen bevett dolog, hogy a piacon elérhető okostelefonok jelentős részében alapvető tartozék az ujjlenyomat-olvasó, az ember már meg sem lepődik rajta.[2]

Kevés más olyan jogterület van, amelynek alakulását annyira meghatározná a technológiai fejlődés, mint a személyes adatok védelméhez fűződő jogét. Maga a GDPR is kimondja annak (6) preambulumbekezdésében, hogy a megalkotására többek között azért is volt szükség, mivel a gyors technológiai fejlődés és a globalizáció új kihívások elé állította a személyes adatok védelmét. Ennek oka, hogy a folyamatos fejlesztés alatt álló új technológiai megoldások lehetővé teszik a piaci és állami szereplők részére, hogy egyre nagyobb mértékben használjanak fel személyes adatokat. Ezen felül az érintett természetes személyek is egyre nagyobb mértékben hoznak magukról nyilvánosságra és osztanak meg személyes adatokat. Ha belegondolunk ez valóban így van: a szélessávú internet, valamint mobilinternet lakossági elterjedése, a közösségi hálózatokon zajló kommunikáció sajátosságai, valamint az egyre jobban a személyre szabottság irányába fejlesztett online szolgáltatások adatéhsége mind-mind katalizátorai ezen folyamatoknak.

Az új technológiák adatvédelemre jelentett hatásáról véleményem szerint csak úgy érdemes szólni, ha kiválasztunk néhányat közülük, amelyek az elmúlt időszakban talán a legnagyobb vagy legérdekesebb kérdéseket, kihívásokat jelentették az emberek magánszférájára és egyben személyes adataikra. A fentiek alapján ezért úgy gondoltam, hogy a négy új és kellően konkrét technológiát választok jelen írásomban vizsgálódási témaként, amelyek adatvédelmi értékeléséről egyre több szó esik mind a tudományos, mind a gyakorlati diskurzusban.

Szó lesz először a gépi tanulásról, mint a mesterséges intelligencia-fejlesztés egyik ágáról, amely a legtöbb személyes adat kezelésével, feldolgozásával járó folyamat az ilyen szoftverek fejlesztése és működtetése során. Ennek kapcsán röviden kitérek az Európai Unió nemrég nyilvánosságra hozott mesterséges intelligencia rendelet-tervezetére is.

Másodszor a blokklánc technológiáról szeretnék szólni adatvédelmi szempontból. Ez a technológia olyan elosztott és sajátos működési mechanizmusai révén rendkívül különleges

---

[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).

[2] ESZTERI Dániel: Blokklánc és mesterséges intelligencia: két új technológia az adatvédelmi megfelelés kapujában. In: *Az Infotörvénytől a GDPR-ig* (szerk.: Szabó Endre Győző), Ludovika Egyetemi Kiadó, Budapest 2021., 143.

rendszereket takar, amelyek tanulmányozása rendre kétségbe ejti nem csak az adatvédelemmel foglalkozó szakembereket.

Harmadszorra az úgy nevezett Internet-of-Things, vagy röviden IoT szolgáltatások adatvédelmi értékelésére szeretnék kísérletet tenni, amely szintén egyre fontosabb téma az internetre csatlakozó eszközök számának növekedése és az általuk kezelt adatok, így különösen felhasználói szokások nyomon követése miatt.

Végül egy még kissé futurisztikusnak ható, de minden bizonnyal a közeljövőben egyre nagyobb problémát jelentő technológiát szeretnék bemutatni és azonosítani néhány adatvédelmi kérdést azzal kapcsolatban. Ez pedig nem más, mint a biometrikus adatok egyik rendkívül különleges kategóriájának kezeléséhez kapcsolódó technológia: az emberi agyhullámok olvasásának és kezelésének kérdésköre.

A technológiákat a fenti sorrendben, egymás után mutatom be. Remélem, hogy írásommal fel tudom kelteni az érdeklődést a feldolgozott témák iránt, valamint hozzá tudok járulni a körülöttük folyó tudományos és szakmai párbeszédhez.

2. Gépek tanítása és adatvédelem: néhány kulcskérdés

2.1.Az irányított gépi tanulás társadalomra gyakorolt hatása

A mesterséges intelligencia (MI) fejlesztése és üzemeltetése kapcsán az elmúlt időszakban elkezdődött tudományos diskurzus – ha a társadalomtudományokat és azokon belül is a jogtudományt nézzük – még nem tudott teljes mértékben kilépni azon gondolatiságból, amelyet az ismeretlentől való rettegés fog át. Való igaz, a jelek egyre biztatóbbak a naiv rettegés leküzdése terén, azonban még mindig tetten érhető az a fajta ősfélelem, amelyet az autonóm, döntések meghozatalára képes szoftverek és gépek világától való idegenkedés jelent az ember számára.

Emberi lényként hajlamosak vagyunk arra, hogy a „gondolkodó gépet" egy ponton túl antropomorf, az élő szervezetekre jellemző tulajdonságokkal ruházzuk fel, végső soron pedig mint – felsőbbrendűnek hitt – új létformát az emberiségre veszélyt jelentő jelenségként azonosítsuk. A filozófiában ezt a jelenséget a hátborzongató völgy *(uncanny valley)* fogalmával írták le először az 1970-es években. Ezek szerint, amint egyre inkább emberszerűbbek lesznek a robotok, úgy nő velük szemben a rokonszenvünk – de egy ponton túl, amikor már nagyon emberszerűek, egyszer csak bizarrnak, hátborzongatónak és veszélyesnek látjuk őket.[3]

Az önálló tudatra ébredő és teremtőjét elpusztító mesterséges lény archetipikus képét felvázoló pesszimista irányzatok gyökerei a 20. század előtti szépirodalomban és folklórban is megtalálhatók (például Frankenstein története). Ráadásul az emberek és a mesterséges lények közötti konfliktus nem csak az irodalmi fikció szintjén jelent meg. Az ipari forradalom alatt a gépektől való rettegés szülte például a géprombolók mozgalmát az 1810-es években.[4]

A pesszimista vagy *alarmista* elméletek alapját elsősorban az úgynevezett *technológiai szingularitás* problémája adja, amely Ray Kurzweil szerint *egy jövőbeli korszak, amelyben a technológiai változás üteme olyan gyors lesz, a hatása pedig olyan mély, hogy az emberi élet visszafordíthatatlanul átalakul.* Kurzweil szerint a szingularitás hatására megjelenő emberfeletti intelligencia pedig könnyen kiszoríthatja az embert a létezésből.[5]

Stuart Russel és Peter Norvig az MI-jelenséget elemző, összefoglaló munkájában bemutatott más, optimistább elméletek (például I. J. Good, Moravec) szerint az embereket leigázó MI

---

[3] Masahiro MORI: The uncanny valley. In: *IEEE Robotics and Automation 19. (2012), 2.,* 99.

[4] Ulrike BARTHELMESS – Ulrich FURBACH: Do We Need Asimov's Laws? In: *Lecture Notes in Informatics*. Bonn, Gesellschaft für Informatik, 2014., 5.

[5] Ray KURZWEIL: *A szingularitás küszöbén*. Budapest, Ad Astra, 2014. Idézi: MAROSÁN György: Mi vár ránk a szingularitáson túl? *Népszava,* 2019. 12. 15.

víziója az ismeretlentől, emberfelettitől való rettegésből fakad, csakúgy, mint korábban a szellemektől vagy boszorkányoktól való félelem. Az optimisták szerint, ha az MI-t megfelelően, azaz olyan ágensekként tervezik, amelyek a gazdáik céljait teljesítik, akkor a jelenlegi tervezés lépésenkénti előrehaladásából származó MI-k szolgálni fognak, nem pedig leigázni.[6]

A magam részéről a két felfogást áthidaló *navigacionista* elméletet tartom racionális szempontból a leginkább támogathatónak. Ezen irányzat szerint a kurzweili szingularitás mentén létrejövő intelligenciarobbanás eljövetele, ha nem is kerülhető el, de annak lefolyásában végső soron az emberiségnek lesz óriási szerepe és felelőssége. Ennek alapján a számítási, problémamegoldási képességben az emberit meghaladó gépi intelligencia megfelelő irányba történő bölcs navigálása a jövő leglényegesebb kihívása.[7]

Az emberi felelősséget és tárgyilagosságot képviselő navigacionista álláspont az MI-fejlesztés felnőttkorát, a felelős szülő és tanító képét vetíti előre. A minden egyes technológiai fejlesztés mögött meghúzódó emberi felelősség fontosságát a téma jogi szempontú feldolgozása kapcsán sem lehet elégszer hangsúlyozni. A bölcs navigálás és fejlesztés az intelligens szoftverek adatalapú tanítása kapcsán érhető tetten a leginkább.[8]

Az MI működésének adatvédelmi vizsgálata szempontjából talán az egyik legfontosabb terület ezért az úgynevezett „gépi tanulás" jelensége, amely során a szoftver a belé töltött adatok alapján „tanul" és hoz meg különböző döntéseket. A piacon ez legtöbbször úgy jelenik meg, hogy az alkalmazott technológia gyakorlatilag képessé válik arra, hogy előre megjósolja az azt használó ember igényeit. A továbbiakban ezen technológia adatvédelmi kérdéskörét igyekszem röviden körüljárni.

2.2.A gépi tanulás általános technológiai háttere és a GDPR fogalomhasználata

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.[9]

A gépi tanulás során az MI-rendszer által végzett adatkezelést három lépcsőre lehet bontani, amelyek a következők: [10]

a) 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.

b) 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.

---

[6] Stuart J. RUSSELL – Peter NORVIG: *Mesterséges Intelligencia – Modern megközelítésben*. Budapest, Panem, 2000. 26. fejezet.

[7] ESZTERI Dániel: A gépek adatalapú tanításának megfeleltetése a GDPR egyes előírásainak. In: *A mesterséges intelligencia szabályozási kihívásai – Tanulmányok a mesterséges intelligencia és a jog határterületeiről* (szerk.: TÖRÖK Bernát – ZŐDI Zsolt), Ludovika Egyetemi Kiadó, Budapest, 2021., 189-190.

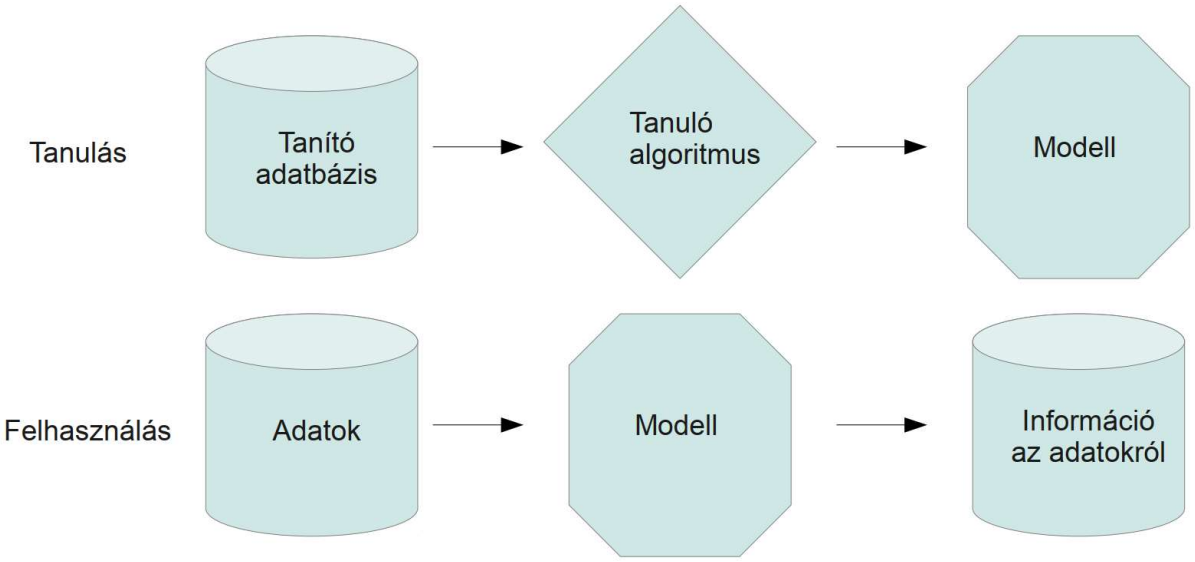
[8] Ibid.

[9] SZEPESVÁRI Csaba: Gépi tanulás – rövid bevezetés. Előadás, MTA SZTAKI, 2005. március 22. http://old.sztaki.hu/~szcsaba/talks/lecture1.pdf (2021. 07. 21.)

[10] Datatilsynet: *Artificial intelligence and privacy*. 2018. www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf (2021. 07. 21.), 7.

c) 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.[11]



Ábra: A gépi tanulás és a tanulás során létrejövő modell felhasználásának lépései[12]

A GDPR nem határozza meg, hogy mit értünk mesterséges intelligencia, vagy gépi tanulás alatt. A rendelet tartalmazza azonban több helyen az *automatizált döntéshozatal* kifejezést, viszont a fogalmát explicite nem határozza meg.

Az Európai Adatvédelmi Testület elődjének tekinthető ún. 29. cikk szerint működő Adatvédelmi Munkacsoport (angol rövidítéssel: WP29) vonatkozó iránymutatása szerint az automatizált döntéshozatal az a képesség, hogy technológiai eszközök segítségével, emberi beavatkozás nélkül hoznak döntéseket.[13] 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.

---

[11] Ibid., 10.

[12] Forrás: KOCSIS Márton: Gépi tanulás a gyakorlatban. Előadás-diasor. http://docplayer.hu/11459797-Gepi-tanulas-a-gyakorlatban-bevezetes.html (2021. 07. 21.)

[13] 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 (2021. 07. 21.), 8.

2.3.A „fekete doboz” és az átláthatóság

Tudományos és műszaki területen a fekete dobozt olyan készülékre, rendszerre vagy tárgyra értik, amely kizárólag csak a bemenete, kimenete és átviteli jellemzői alapján vizsgálható, konkrét belső működése ismeretlen, azaz megvalósítása „átlátszatlan” (fekete).

A gépi tanulással és erre épülő automatizált döntéshozatal kapcsán az egyik legtöbbször hangoztatott aggály, hogy lehetetlen előre megjósolni, a működésének komplexitása és a rengeteg véletlenszerű változó miatt, hogy milyen eredményt fog produkálni a rendszer. A használt modell produkálhat olyan eredményt is, amelyre látszólag semmilyen magyarázat nem létezik.[14] A gépi tanulás és az MI működése során ezt szintén *fekete doboz* jelenségnek nevezzük.

A hálózat mérete és az egyes rétegek közötti kapcsolat olyan bonyolulttá teheti az adatkezelési folyamatokat, amelyeket lehetetlen az ember számára érthetően leírni, felfogni.

Az adatvédelem alapelvei között azonban 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.[15] 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.[16]

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 miként je már több kérdést vet fel. Ez főleg az előző pontokban bemutatott gépi tanulási módszerek esetében jelenthet nagy kihívást az adatkezelő részére, mivel az sokszor rendkívül összetett, nagyon nehezen átlátható adatkezelési folyamatokon alapul. Lásd erre kiváló példaként a fekete doboz jelenséget.

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

---

[14] Datatilsynet, 2018., 12.

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

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

lerontaná a tájékoztatás közérthetőségét, és hátráltatná a befogadását.[17] 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.[18] A technológia komplexitása természetesen nem lehet mentség a tájékoztatás teljes mellőzésére sem.

Az Oxford Internet Institute és a londoni Alan Turing Institute közös kutatása szerint az algoritmusok által hozott döntések és azokhoz kapcsolódó adatkezelések átláthatósága szempontjából jó gyakorlat lehet, ha az adatkezelő lehetőséget biztosít az érintettnek, hogy ún. „alternatív értelmezések" kapcsán ismerhesse meg az adatkezelés működését. Ennek oka, hogy az érintetteket legtöbbször nem is igazán érdekli, hogy maga a logika hogyan működik, hanem inkább az, hogy ők maguk hogyan tudnak javítani az algoritmus által megállapított eredményen.[19] Sokkal érdemibb tájékoztatást hordoz az érintett részére, ha rendelkezésére áll egy nyilvános tesztrendszer, amit akár fiktív adatokkal kitöltve használhat. Így elegendő és érdemi információt kaphat arról, hogy az alkalmazott rendszer a betáplált adatok alapján milyen következtetésekre jut. Ez a megoldás tiszteletben tartja az MI fejlesztőjének üzleti titokhoz és szellemi tulajdonhoz fűződő jogosultságait is.[20] A WP29 vonatkozó iránymutatása is – a brit tanulmányhoz hasonlóan – összehasonlító alkalmazás biztosítását hozza fel példaként.[21] Tehát a tájékoztatás során nem kell a fekete dobozt kinyitnia az adatkezelőnek az érintett előtt, elég, ha megérteti vele, hogy a döntés meghozatala hogyan történt, és ő mit tehet annak érdekében, hogy ügyében más (kedvezőbb) döntés szülessen.[22]

2.4.Az emberi beavatkozás szükségessége

Már a francia adatvédelmi hatóság (Commission nationale de l'informatique et des libertés, röviden: CNIL) 2017 decemberében nyilvánosságra hozott jelentése megjegyezte azt általánosságban, hogy a kritikus (jog)hatást kiváltó döntések meghozatalánál az lenne az ideális, ha az MI-rendszerek biztosítanák az emberi beavatkozás és/vagy felülvizsgálat lehetőségét. A különösebben mélyebb megfontolást nem igénylő „tömegdöntéseknél" azonban meg lehetne hagyni a lehetőséget az algoritmus kezében.[23]

Az emberi beavatkozás szükségessége megjelenik a GDPR előírásai között is. Ezek szerint az adatkezelő köteles lehetővé tenni az érintett számára, hogy emberi beavatkozást kérhessen az őt érintő automatizált egyedi döntéshozatallal kapcsolatban. Lehetővé kell tenni továbbá – adott esetben – az automatikus úton megszületett döntés módosítását is az esetleges téves következtetések, hibák kiküszöbölése érdekében. Ennek keretében az érintett jogosult kifejteni az álláspontját a döntéssel kapcsolatban, és kifogást is benyújthat az őt érintő hibás döntés orvoslása, megváltoztatása céljából az adatkezelőnél.[24]

A WP29 iránymutatása kiemeli, hogy az emberi beavatkozást olyan személynek kell végeznie, aki megfelelő jogkörrel és képességgel rendelkezik a döntés megváltoztatására. A

---

[17] PÉTERFALVI Attila – RÉVÉSZ Balázs – BUZÁS Péter (szerk.): *Magyarázat a GDPR-ról*. Wolters Kluwer, Budapest, 2018., 158.
[18] GDPR (63) preambulumbekezdés
[19] Sandra WACHTER – Brent MITTELSTADT – Chris RUSSELL: Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR. *Harvard Journal of Law & Technology,* 31. (2018), 2., 863–871.
[20] Ibid., 844.
[21] A 29. cikk szerint működő Adatvédelmi Munkacsoport, 2017., 28.
[22] Datatilsynet, 2018., 21–22.
[23] CNIL: How can humans keep the upper hand? The ethical matters raised by algorithms and artificial intelligence. 2017. https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_ai_gb_web.pdf, (2021. 07. 21.), 30.
[24] PÉTERFALVI – RÉVÉSZ – BUZÁS, 2018., 201.

felülvizsgálónak alaposan meg kell vizsgálnia az összes releváns adatot, ideértve az érintett által rendelkezésre bocsátott minden további információt. [25]

Korábbi írásomban is már kifejtett véleményem szerint az emberi beavatkozás kérésének gyakorlása során a döntéshozatali mechanizmusok felülvizsgálatát az érintettre gyakorolt hatás szemszögéből kell megközelíteni. Meg kell tehát vizsgálnia az emberi beavatkozásra kijelölt személynek, hogy pontosan milyen adatok voltak érintettek a döntéshozatalban, és hogy milyen döntés született, majd ezt összevetnie az érintett által előterjesztett kifogásokkal. Ez ebben az esetben sem igényli a fekete doboz felnyitását, így a döntés mögött meghúzódó algoritmikus folyamat aprólékos feltárását és megértését. Erre a legtöbb esetben nem is lenne valós lehetősége a felülvizsgálatra jogosult személynek, hiszen – mint már az előzőekben is kifejtettem – az adatokon végzett műveletek egy bizonyos szint után az emberi szemlélő számára felfoghatatlanok lesznek. A felülvizsgálatra jogosult személynek tehát azt kell elsősorban mérlegelni, hogy a döntésnek vajon ugyanez lett volna-e az eredménye, ha azt nem egy algoritmus végzi.[26]

2.5.Az új mesterséges intelligencia rendelet-tervezet

2021. április 21-én az Európai Bizottság nyilvánosságra hozott egy rendelet-tervezetet, amely a GDPR-hoz hasonlóan közvetlenül alkalmazandó, valamennyi tagállamban egységesen végrehajtandó jogszabályként szabályozná a mesterséges intelligencia fejlesztést.

A nyilvánosságra hozott tervezet célja a Bizottság sajtóközleménye szerint, hogy Európa a megbízható MI globális központjává váljon. A tervezet az MI-ként való besorolásra három feltétel együttes teljesülését írja elő. Először is az MI-nek meghatározott technológiákat kell alkalmaznia, másodszor az ember által kijelölt célokat önállóan kell tudnia követni, majd végül olyan kimeneteleket kell tudnia produkálni, amelyekkel „befolyásolja" a környezetet. Ződi Zsolt idevágó írása alapján az utóbbi két kritérium tulajdonképpen az „autonómia" pontos meghatározásának kísérlete. Az új kódex tervezete egyébként a gépi tanuláson alapuló rendszereken kívül még két másik technológia-csoportot is megjelöl, amelyekre kiterjed a hatálya. Ezek a tudásreprezentáción alapuló és a statisztikai rendszerek. Ződi szerint ennek oka az lehet, hogy ily módokon is építhetőek olyan rendszerek, amelyek kimenetei a bonyolultságuk, összetettségük és a feldolgozott adatok mennyisége miatt nem tűnnek determinisztikusnak.[27]

A kódex ezen felül kockázatalapú megközelítést alkalmaz az MI-k besorolása szempontjából, amely összesen négy nagy kategóriába igyekszik felosztani a rendszereket:

a) Az első kockázati kategória, az elfogadhatatlanul magas kockázatúként besorolt rendszereket tartalmazza. Ezek alatt olyan MI-ket ért, amelyek egyértelműen veszélyeztetik az emberek biztonságát, megélhetését és jogait. Ide érti például a szabályozási koncepció az olyan rendszereket vagy alkalmazásokat, amelyek a felhasználók szabad akaratának megkerülése érdekében manipulálják az emberi viselkedést, valamint ide tartoznak az olyan rendszerek is, amelyek lehetővé teszik a kormányok általi „társadalmi pontozást".[28] Ez utóbbit, mint tiltást

---

[25] A 29. cikk szerint működő Adatvédelmi Munkacsoport, 2017., 29. és PÉTERFALVI – RÉVÉSZ – BUZÁS, 2018., 201.

[26] ESZTERI Dániel: A gépek adatalapú…, 2021., 207.

[27] ZŐDI Zsolt: A mesterséges intelligencia jogi fogalma. Blogbejegyzés, 2021., https://www.ludovika.hu/blogok/itkiblog/2021/06/18/a-mesterseges-intelligencia-jogi-fogalma/ (2021. 07. 21.)

[28] Európai Bizottság: A Digitális korra felkészült Európa: A Bizottság új szabályokat és intézkedéseket javasol a kiválóságra és bizalomra épülő mesterséges intelligencia terén. Sajtóközlemény, 2021., https://ec.europa.eu/commission/presscorner/detail/hu/IP_21_1682 (2021. 07. 21.)

igénylő kategóriát, minden bizonnyal a Kínai Népköztársaságban kifejlesztett és tesztelt ún. társadalmi kreditrendszer ihlette.[29]

b) A második, azaz magas kockázati kategóriába sorolja be a kódex-tervezet azon MI-technológiákat, amelyeket összesen kilenc olyan területen és/vagy célból alkalmaznak, amelyek magas kockázatot jelentenek az emberek egyes alapvető jogaira nézve. Ezek a területek:

- kritikus infrastruktúrák (pl. közlekedés),
- oktatás vagy szakképzés (pl. vizsgák pontozása),
- egyes termékek biztonsági berendezései (pl. robotsebészet),
- foglalkoztatás és munkavállalók irányítása (pl. munkaerő-felvételhez önéletrajz válogatás),
- alapvető magán- és közszolgáltatások (pl. hitelbesorolás),
- bűnüldözés (pl. bizonyítékok megbízhatóságának értékelése),
- menekültügy és határellenőrzés (pl. úti okmány valódiságának ellenőrzése),
- igazságszolgáltatás és demokratikus folyamatok (pl. törvények konkrét tényállásra való alkalmazása),
- végül az összes távoli biometrikus azonosító rendszer magas kockázatúnak minősül a kódex szerint. Használatuk bűnüldözési célból nyilvános helyeken, valós időben fő szabály szerint tilos lenne. Ezen tilalom alól néhány kivételes esetben enged csak eltérést a szabályozási koncepció (pl. eltűnt gyermek felkutatása, közvetlen terrorveszély vagy súlyos bűncselekmény megelőzése) és azt is bírói vagy más független hatósági engedélyhez köti.[30]

A fenti kategóriákba besorolható MI-rendszereknek forgalomba hozataluk előtt szigorú kötelezettségeknek kell megfelelniük. A tervezet előírja, hogy valamennyi ilyen rendszernek a fejlesztése során megfelelő kockázatértékelési és csökkentési folyamatokon kell keresztülmennie. Az MI fejlesztése során használt adatkészleteknek kiváló minőségűeknek kell lenniük és az eredmények nyomon követhetősége miatt minden tevékenységet naplózni kell, továbbá részletes dokumentációnak kell rendelkezésre állnia a megfelelőség értékelésével kapcsolatban. A tervezet előírja továbbá a felhasználók egyértelmű és érthető tájékoztatását, az emberi felügyelet szükségességét, valamint egyfajta alapelvi éllel a rendszer megbízhatóságát, pontosságát és biztonságos működésének követelményét.[31]

c) A tervezet korlátozott kockázatú MI-nek sorolja be az olyan rendszereket, amelyek használata során a felhasználóknak tisztában kell lenniük azzal, hogy nem emberrel, hanem egy géppel kommunikálnak (pl. csevegőrobotok). Ezen átláthatósági kötelezettségre valószínűsíthetően azért van szükség, hogy a felhasználókat ne tévessze meg a program és tisztában legyenek azzal, hogy nem egy másik ember van a „monitor túloldalán."

d) A tervezet végül a minimális kockázati kategóriába sorolja be az MI-k legnagyobb részét kitevő olyan rendszereket, amelyek használata a felhasználók jogaira és biztonságára nézve szinte alig hordoz kockázatokat. A kódex szabadon lehetővé teszi ezen rendszerek használatát és nem tartalmaz rájuk nézve beavatkozó intézkedéseket, így azokat gyakorlatilag kivonja a hatálya alól. Ilyen MI-re példa a spamszűrők vagy videojátékok használata.

A kódex kapcsán nemrég az Európai Adatvédelmi Testület (EDPB) is kifejtette véleményét, amely általánosságban szintén üdvözli a tervezetet. Az EDPB néhány területen – így például a távoli biometrikus azonosítás terén – azonban szigorítaná a szabályokat. A vélemény fő szabály szerint megtiltaná például az olyan távoli biometrikus azonosító rendszerek használatát, amelyek alkalmasak arra, hogy az érintetteket tulajdonságaik alapján kategóriákba sorolja

---

[29] KOLLÁR Csaba: Kína és a társadalmi kreditrendszere. In: *Hadtudomány* 2020/2. https://www.mhtt.eu/hadtudomany/2020/2020_2szam/079-097_Kollar.pdf (2021. 07. 21.)
[30] Európai Bizottság, 2021.
[31] Ibid.

származás, nem, szexuális orientáció alapján, mivel ez könnyen vezethet hátrányos megkülönböztetéshez.[32]

A kódex-tervezet az elkövetkezendő időszakban minden bizonnyal igen sűrűn fogja alapját képezni további szakmai és tudományos diskurzusoknak, amíg az teljesen elfogadásra nem kerül az Európai Unió által. Általánosságban elmondható, hogy a kockázatalapú megközelítés, és a tiltott, valamint magas kockázatú besorolásra tartozó rendszerek viszonylag szűk köre előremutató és kellően rugalmas szabályozást sejtet.

3. A blokklánc: egy új adatkezelési technológia

A blokklánc egy olyan új, elosztott hálózati koncepción alapuló adatkezelési technológia, amelynek első, gyakorlatban is megvalósított képviselője a piacon a Bitcoin elnevezésű virtuális (tehát fizikai formában nem, csupán adatként létező) vagyonképzési és fizetőeszköz volt. Ezt 2009 elején hozták létre egy Satoshi Nakamoto álnevű kriptográfiával foglalkozó szakember (vagy inkább szakemberek csoportjának) ötlete alapján.

A Bitcoin-rendszer és az alapját képező elosztott hálózat lehetővé tette, hogy a felhasználói anonim módon, központi ellenőrzés nélkül, mégis gyorsan és nagyon biztonságosan küldhessenek egymásnak a virtuális vagyontárgyból. Ezen felül minden tranzakció és művelet naplója utólag kitörölhetetlenül és megváltoztathatatlanul rögzül a hálózaton, ez alapján pedig azt bárki bármikor vissza tudja ellenőrizni. Később a technológiát már nemcsak fizetési és vagyonképzési, hanem más célú adatkezelő rendszerek fejlesztésére is elkezdték alkalmazni.

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 elosztott főkönyv olyan tranzakciós adatbázis, amely több számítógépből álló hálózaton oszlik el, nem pedig központi helyen tárolják.[33] 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.[34] A blokkláncban kezelt adatcsomagok bármilyen információ tárolására, kezelésre alkalmasak lehetnek, így maga a technológia univerzálisan használható szinte bármilyen adatkezelési célra.

3.1. A blokk, mint adattárolási egység

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

---

[32] Európai Adatvédelmi Testület – Európai Adatvédelmi Biztos: Joint opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence(Artificial Intelligence Act), 2021., https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf (2021. 07. 21.)

[33] Európai Központi Bank: Hogyan formálják át a technológiai újítások a pénzügyi piacokat? 2017., www.ecb.europa.eu/explainers/tell-me-more/html/distributed_ledger_technology.hu.html. (2021. 07. 21.)

[34] GYŐRFI András et alii: *Kriptopénz ABC.* Budapest, HVG Könyvek, 2019., 57–59.

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".[35]

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, hozzáférés joga kit illet meg.[36]

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. 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.[37] 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.[38]

A blokkláncot legegyszerűbben egy olyan adatkezelési technológiának írhatjuk le a fentiek alapján, amely az adatok kezelését egy közös, elosztott hálózaton teszi lehetővé, amely központi ellenőrző szerv felügyelete nélkül is működőképes. Az adatokkal végzett műveletek hitelesítése a hálózaton algoritmikus alapú önellenőrző mechanizmusokkal biztosított.[39]

3.2.A blokklánc típusok adatkezelési szempontból

A blokkláncban tárolt adatok megismerhetősége szempontjából különbséget tehetünk a *nyilvános („public")* és a *privát („private")* rendszerek között. A nyilvános hálózatok sajátossága, hogy nem tartalmaz az abban kezelt adatokkal kapcsolatban szinte semmilyen hozzáféréskontrollt. A blokkláncban kezelt, szinkronizált adatbázist bárki csomópontként tárolhatja, az abban tárolt adatokat pedig korlátozás nélkül megismerheti. A privát hálózat ezzel szemben már tartalmaz jogosultságkezelési mechanizmusokat. Az adatokat csak az előre meghatározott vagy engedéllyel rendelkező személyi kör ismerheti meg megfelelő regisztráció és hozzáférés-tanúsítás mellett.[40]

A blokkláncok másik fő csoportosítási elvét a blokkláncba történő adatok bejegyzésének joga, azaz a bejegyzések csomópontként történő hitelesítése alapján tehetünk különbséget: az *engedélyhez kötött* blokklánchoz csak az arra engedéllyel rendelkező személy adhat hozzá adatokat, így például egy egészségügyi irattárhoz nyilvánvaló módon csak az arra jogosult

---

[35] GYŐRFI et alii., 2019., 61.

[36] A Nemzeti Adatvédelmi és Információszabadság Hatóság állásfoglalása a blokklánc („blockchain") technológia adatvédelmi összefüggéseivel kapcsolatban, https://naih.hu/files/Adatved_allasfoglalas_naih-2017-3495-2-V.pdf (2021. 07. 21.), 3.

[37] 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). 4–7. http://dx.doi.org/10.2139/ssrn.2849251. (2021. 07. 21.)

[38] GYŐRFI et alii 2019., 63., 68.

[39] ESZTERI Dániel: Blokklánc…, 2021., 146-147.

[40] Jean BACON – Johan David MICHELS – Christopher MILLARD – Jatinder SINGH: Blockchain Demystified. *Queen Mary School of Law Legal Studies Research Paper* No. 268/2017, 25–26.

egészségügyi személyzet adhat hozzá adatokat. Az *engedély nélküli* blokklánc-rendszerekhez bárki kapcsolódhat, és adatokat adhat hozzá.[41]

Különbséget tehetünk végül az egyes blokkláncok között a felhasználók identitásának kezelése szempontjából is. A *pszeudonim* módon működő platformok az adatkezelési műveleteket végző felhasználókat és a csomópontokat működtető felhasználókat különböző kódokkal azonosítják. A Bitcoin rendszerében ilyen kódsor az átutalások kivitelezésére szolgáló, a felhasználók kérésére a rendszer által generált ún. publikus és privát kulcspár.[42] Nem lehet azt mondani, hogy az ilyen rendszerek teljesen anonimak, mivel ha a kulcsot más rendszerekben vagy szolgáltatások igénybevétele során felhasználják, akkor az ott a felhasználóról kezelt személyes adatokkal már összeköthetővé válik.

A pszeudonim platformok mellett a blokkláncok másik típusai identitáskezelési szempontból a *valós identitáson alapuló* rendszerek. Ezek adatkezelési szempontból ugyanúgy blokklánc alapon működnek, viszont az egyes felhasználókról nemcsak pszeudonim, hanem közvetlenül az érintettel összekapcsolható információkat is kezelnek (pl. név, e-mail cím, banki adatok stb.).[43]

3.3. A blokklánc megfeleltetése a „célhoz kötöttség", az „adattakarékosság" és a „korlátozott tárolhatóság" alapelveinek

A GDPR 5. cikke sorolja fel azon alapelveket, amelyeknek az adatkezelés során mindvégig meg kell felelnie az adatkezelőnek. Az alapelveknek egyszerre és egymásra tekintettel kell érvényesülniük a teljes adatkezelés során. Az adatkezelő további kötelezettsége a megfelelésen túl, hogy képesnek kell lennie igazolni is azt, hogy megfelel ezen alapelveknek.[44]

A blokkláncon alapuló adatkezelések alapelvi megfelelési vizsgálata során a *célhoz kötöttség*, az *adattakarékosság* és a *korlátozott tárolhatóság* egymással is szorosan összefüggő alapelvei állhatnak első ránézésre szöges ellentétben egy ilyen típusú technológiával, ezért a következőkben ezekre kívánok koncentrálni.

A *célhoz kötöttség* alapelvét a GDPR úgy fogalmazza meg, hogy a személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet, és azokat nem lehet kezelni ezekkel a célokkal össze nem egyeztethető módon.[45] A 29-es Adatvédelmi Munkacsoport kapcsolódó véleménye szerint a célhoz kötöttség lényege, hogy megakadályozza az adatok olyan célú felhasználását, amelyre az érintettek nem számíthatnak előre, tiltakoznának ellene, vagy az adatok egyébként sem alkalmasak az ilyen célok elérésére.[46] Az alapelv két további részelvből tevődik össze, nevezetesen először a cél meghatározásának kötelezettségéből és másodszor pedig az ezzel összefüggő felhasználás kötelezettségéből.[47] Az adatkezelési célnak explicit módon előre meghatározottnak és legitimnek kell lennie, az adatok felhasználásának pedig ennek megfelelően kell történniük.

A blokkláncon alapuló adatkezeléssel kapcsolatban felmerülhet kérdésként, hogy vajon mennyiben feleltethető meg a célhoz kötött adatkezelés elvének az az alapvető működési elv, hogy az adatok a velük végzett tranzakciós műveletek kivitelezése után is tárolódnak a

---

[41] Tom LYONS – Ludovic COURCELAS – Ken TIMSIT: Blockchain and the GDPR. *European Union Blockchain Observatory & Forum eublockchainforum.eu*, 2018. október 16., www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf. (2021. 07. 21.), 14–15.

[42] BACON – MICHELS – MILLARD – SINGH, 2017., 26–27.

[43] BACON – MICHELS – MILLARD – SINGH, 2017., 27.

[44] PÉTERFALVI – RÉVÉSZ – BUZÁS, 2018., 108.

[45] GDPR 5. cikk (1) bek. b) pont.

[46] A 29. cikk szerint működő Adatvédelmi Munkacsoport 3/2013-as véleménye a célhoz kötöttségről (WP203), 2013., https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (2021. 07. 21.), 11.

[47] A 29. cikk szerint működő Adatvédelmi Munkacsoport, 2013., 3.

blokkláncon, sőt ezekre fűzik fel a további műveleteket 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 visszakövethetők az egyes adatkezelési műveletek.

Nagyon fontos előkérdés a blokkláncon alapuló adatkezelés jogszerűségének megítélése szempontjából, hogy a fenti, látszólag készletező adatkezelések vajon mennyire egyeztethetők össze az eredeti adatkezelési céllal.[48] Egy blokkláncos adatkezelés csak akkor felelhet meg a célhoz kötött adatkezelés elvének, ha a 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 törlés kivitelezése első ránézésre lehetetlen. De olyan jogszabályi felhatalmazáson alapuló adatkezeléseknél, mint pl. az ingatlannyilvántartás vezetése[49] vagy a levéltári adatkezelések, már könnyebb a helyzet, hiszen ezeknél a cél valamennyi adat megőrzése és azokkal végzett műveletek pontos és részletes vezetése. Szükségszerű tehát, hogy egy adott blokkláncalapú adatkezelés GDPR-megfelelősége a célhoz kötöttség szempontjából csak esetről esetre ítélhető meg teljes bizonyossággal, és különös figyelmet kell fordítani a megfelelő adatkezelési jogalap kiválasztására is.

A célhoz kötött adatkezelés elvével szorosan összefügg az *adattakarékosság* elve, amely szerint a személyes adatoknak az adatkezelés céljai szempontjából megfelelőnek és relevánsnak kell lenniük, és a szükségesre kell korlátozódniuk.[50] Az elv gyakorlatilag azt fogalmazza meg, hogy – a céllal összefüggésben – lehetőleg minél kevesebb személyes adatot kezeljünk, és feleslegesen ne kerüljön sor adatkezelésre.

A blokklánc kapcsán az adattakarékosság elvét elsőre talán nehéz lehet összeegyeztetni azon tulajdonsággal, minthogy az adatbázis folyamatosan növekszik, tartalmazva a valaha elvégzett valamennyi adatkezelési műveletet. A blokklánc replikatív természete szintén problémás, mivel valamennyi csomópont eltárolja az adatbázis teljes másolatát önellenőrzési célokból.[51] Ezek a felvetések visszavezetnek minket a célhoz kötött adatkezelés elvének való megfeleléshez. Amennyiben a blokklánc-technológia adattárolással kapcsolatos sajátosságai összeegyeztethetőek az előre meghatározott legitim céllal, úgy az adattakarékosság elvének való megfelelés sem lesz többé problémás. Ez persze feltételezi azt, hogy az adatkezelő, ha szükséges, megfelelő „törlési" és anonimizálási eljárásokat implementáljon a blokkláncba. Az adattakarékosságot szintén elősegítheti az adatok láncon kívüli (off-chain[52]) tárolásának lehetősége.

Végül a *korlátozott tárolhatóság* elvéről érdemes szólni, amely szerint a személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé.[53] Az alapelv az elavult, már semmilyen célból nem használható személyes adatok tárolásának tilalmát fogalmazza meg. Annak érdekében, hogy az adatokat ne tárolják tovább, minthogy az feltétlenül szükséges, az

---

[48] Michéle FINCK: Blockchain and the General Data Protection Regulation. *European Parliamentary Research Service,* PE 634.445, July 2019., 65.

[49] Juliet MCMURREN – Andrew YOUNG – Stefaan VERHULST: „Adressing Transaction Costs Through Blockchain and Identity in Swedish Land Transfers" 2018. *blockchan.ge/blockchange-land-registry.pdf* .

[50] GDPR 5. cikk (1) bek. c) pont.

[51] FINCK, 2019., 68.

[52] Az off-chain adatkezelés olyan blokkláncalapú technológiai megoldásokat takar, amelyek során a személyes adatokat nem magában a blokkláncban, hanem egy elkülönült adatbázisban tárolják, de kezelésük hash-kulcsok használatával összeköttetésben áll a háttértechnológiát adó alapadatbázissal, amely már blokklánc alapon működik. Lásd: Rosanna MANNAN – Rahul SETHURAM – Lauryn YOUNGE: GDPR and blockchain: A compliance approach. *European Data Protection Law Review,* 5. (2019), 3., 421–426. 423–424.

[53] GDPR 5. cikk (1) bek. e) pont.

adatkezelőnek törlési vagy rendszeres felülvizsgálati határidőket kell megállapítania.[54] A blokkláncalapú adatkezelések esetén az adatok eltávolításának lehetősége a protokoll működési sajátosságai miatt alapvetően nem lehetséges. Az alapelv azonban a tárolási idő behatárolását az érintettek azonosítására alkalmas módon való adattárolás szempontjából korlátozza. Az anonimizált adatok tárolására így továbbra is lehetősége van az adatkezelőnek, azonban annak olyan formában kell történnie, hogy biztosan ne lehessen belőlük az érintettekre következtetést levonni, őket a továbbiakban azonosítani. Az ilyen, ténylegesen anonim adatokra az adatvédelmi jogi előírásait többé nem kell alkalmazni.[55] A megfelelő, naprakész anonimizálási technikák alkalmazásával tehát megfeleltethető a blokkláncalapú adatkezelés is ennek az alapelvnek. Az anonimizálásra az adatokhoz való hozzáférést biztosító privát kulcs visszaállíthatatlan törlése megfelelő módszernek tűnik. Már az Egyesült Királyság Adatvédelmi Biztosa is felhívta a figyelmet a személyes adatok „használaton kívül helyezésére",[56] mint a törléssel majdhogynem egyenértékű intézkedésre. Ezen felül a személyes adatok láncon kívüli tárolása esetén, az off-chain adatbázisból való végleges törlés is megoldást nyújthat a megfelelésre.

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

4.1. A dolgok internete, mint technológiai megoldás és annak társadalmi hatása

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.[57]

A 29. cikk szerinti Adatvédelmi Munkacsoport 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.[58]

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.[59] 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.[60]

---

[54] GDPR (39) preambulumbekezdés

[55] A 29. cikk szerint működő Adatvédelmi Munkacsoport 5/2014. számú véleménye az anonimizálási technológiákról (WP216), 2014. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf (2021. 07. 21.), 3.

[56] Information Commissioner's Office: Deleting Personal Data. 2014. február 26., www.ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf. (2021. 07. 21.), 4.

[57] 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 (2021. 07. 21.)

[58] 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 (2021.07.21.), 4.

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

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

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.[61]

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.[62]

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.[63]

4.2. Az IoT-val kapcsolatban leggyakrabban felmerülő adatvédelmi kérdések az érintettek szemszögéből nézve

A dolgok internetéhez 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.[64]

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.[65] Ezért a GDPR 4. cikk 2. pontja szerinti fogalom[66] 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.

---

[61] 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 , 3.

[62] 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., 56.

[63] Európai Gazdasági és Szociális Bizottság, 2018.

[64] BOCSOK et. alii., 11.

[65] SZABÓ – BOJNÁR – BUZÁS, 2016., 56.

[66] 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.

Az IoT eszközök, kiváltképp a hordozható típusok (okostelefonok, -órák, -szemüvegek) természetükből adódóan folyamatosan bekapcsolt állapotban vannak, állandóan érzékelnek, adatot gyűjtenek és küldenek, kommunikálnak. Az így keletkezett óriási mennyiségű információ esetében azonban, a korábban már tárgyalt adatvédelmi és biztonsági problémákon túl felmerülnek az elégtelen felhasználói tájékoztatásból eredő aggályok is.[67]

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.[68]

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.[69] Igaz, a fenti munkacsoporti vélemény még a GDPR alkalmazhatósága előtt jelent meg, annak aktualitása az elmúlt időszakban sem változott.

4.3. Az adatkezelés biztonságának és az adatvédelmi hatásvizsgálat elkészítésének jelentősége IoT környezetben

A GDPR 32. cikke fogalmazza meg általánosságban a személyes adatok kezelésének biztonságával kapcsolatos követelményeket, továbbá alapelvi szinten rögzíti az integritás és bizalmas jelleg alapelvét – GDPR 5. cikk (1) bekezdés f) pontja –, amely előírásokat a biztonságos adatkezelés érdekében be kell tartaniuk az adatkezelőknek és adatfeldolgozóknak.

Az adatkezeléssel összefüggésben ezek szerint olyan megfelelő technikai és szervezési intézkedéseket kell végrehajtaniuk az adatkezelőknek és adatfeldolgozóknak, amelyekkel garantálni tudják a kezelt személyes adatok biztonságát. A rendelet a megfelelő szinttel kapcsolatban nagyrészt általános fogódzókat ad, így előírja, hogy ennek eléréséhez az adatkezelőnek figyelembe kell vennie a tudomány és technológia mindenkori állását, a megvalósítás költségeit, a konkrét adatkezelés jellegét, hatókörét, körülményeit és céljait, valamint az adatkezeléssel az érintettek jogaira kiterjedő kockázatokat.[70]

A GDPR nem sorolja fel kimerítően az alkalmazható technikai és szervezési biztonsági intézkedéseket (csupán néhány példát hoz), azonban az informatikai biztonsági szakirodalomban ezeket jellemzően három nagy csoportra tagolják: logikai, fizikai és adminisztratív biztonsági intézkedések. Ezt a tagolást követi a Francia Adatvédelmi Hatóság által kiadott módszertani útmutató is, amely az adatkezeléssel járó kockázatok csökkentésére

---

[67] Ars Boni: Az IoT eszközök térnyerése az adatvédelem tükrében. 2018. https://arsboni.hu/az-iot-eszkozok-ternyerese-az-adatvedelem-tukreben/ (2021.07.21.)
[68] Ibid.
[69] Ibid.
[70] ESZTERI Dániel: A blokklánc mint személyes adatkezelési technológia GDPR megfelelőségéről. *Állam- és Jogtudomány, 2020/4.*, 37-38.

szolgáló biztonsági/védelmi intézkedéseket mutatja be többet között.[71] A francia módszertan alapján a logikai biztonsági intézkedések azokat a biztonsági kontroll módszereket jelentik, amelyeket magukon a kezelt adatokon hajtanak végre (pl. titkosítás, anonimizálás, particionálás, hozzáférésvédelem, naplózás). A fizikai biztonsági intézkedések magukat az adatkezelésre szolgáló rendszereket védő intézkedéseket takarják (pl. hardverbiztonság, biztonsági mentés, hálózatbiztonsági eszközök, vírusvédelem, tűzfal). Az adminisztratív biztonsági intézkedések pedig leginkább az adatok kezelésére vonatkozó szabályzatokban öltenek testet (pl. adatkezelési szabályzat, informatikai biztonsági szabályzat, szerződések, hatásvizsgálat).[72]

Egy IoT szolgáltatással kapcsolatban a GDPR fenti előírásainak való megfelelés fokozott felkészültséget kíván meg adatkezelői részről. Egyrészt az adatok szenzorokon keresztüli központosított összegyűjtése és elemzése biztonságosabbá teszi az adatkezelést, abból a szempontból, hogy jellemzően nem az egyes felhasználók eszközein történik az adatok tárolása.

Az adatok összegyűjtése az egyes eszközökről jellemzően ún. felhőalapú informatikai megoldásokon keresztül történik. Az infokommunikációs technológiák jogi alapjait feldolgozó, Tóth András által szerkesztett kiadvány meghatározása szerint a felhőalapú szolgáltatás az adatok távoli szervereken történő tárolását, feldolgozását és felhasználását jelenti, amelyek egy hálózaton, általában (de nem kizárólagosan) az internet elektronikus hírközlési infrastruktúráján keresztül válnak hozzáférhetővé. A szolgáltatás így nem egy dedikált és a felhasználó számára fizikailag (térben) is azonosítható hardvereszközön érhető el, hanem azokat a szolgáltató közelebbről nem azonosított eszközein elosztva üzemelteti oly módon, hogy a szolgáltatás üzemeltetési részletei a felhasználó előtt rejtve maradnak.[73]

Az eszköz elveszítése, sérülése így kevésbé okozhat kockázatokat az érintett magánszférájára nézve, az összegyűjtött személyes adatok a központi tárhelyről bármikor helyreállíthatóak az eszköz cseréje esetén is. Mások oldalról nézve viszont így a központi adatbázist üzemeltető adatkezelőnek kell rendkívül magas szintű intézkedéseket tennie annak érdekében, hogy a centralizált adatkezelés biztonsága ne sérülhessen.

Az alkalmazandó biztonsági intézkedések felmérése során az adatkezelőnek még az adatkezelés megkezdése előtt mérlegelnie kell, hogy az adatkezelés az érintettekre nézve milyen kockázattal jár, és ha valószínűsíthetően magas besorolású a kockázat, akkor adatvédelmi hatásvizsgálatot kell végeznie. Az erre vonatkozó előírásokat a GDPR 35. cikke tartalmazza.

Az adatvédelmi hatásvizsgálat egy olyan eljárás, amelyet az adatkezelő folytat le egy új, még meg nem kezdett – tulajdonképpen még tervezési szakaszban lévő – adatkezelés megkezdése előtt. A hatásvizsgálat célja, hogy az adatkezelő még az új adatkezelés megkezdése előtt felmérje azt, hogy az meg fog-e felelni az adatvédelmi jog előírásainak. Az adatvédelmi hatásvizsgálat az érintettek jogait érintő kockázatok kezelésére szolgál, így az ő szemszögükből készül. Az adatvédelmi hatásvizsgálat lényege tehát az adatkezelés előzetes kontrollja. Ennek keretében az adatkezelő feltárja az érintett személyek szemszögéből az adatkezeléssel járó kockázatokat és értékeli a kockázatok mérséklésére teendő intézkedéseket. Az adatvédelmi hatásvizsgálat egyik legfontosabb szakasza, amikor az adatkezelő az előzetes felmért kockázatforrások tekintetében megtervezi, hogy milyen az adatok védelmét szolgáló biztonsági intézkedések alkalmazása indokolt. Az egyes biztonsági intézkedéseknek itt is – a legtöbb hatásvizsgálati metodológia szerint – a logikai, fizikai és adminisztratív kategóriába kell esniük,

---

[71] CNIL: Privacy Impact Assessment (PIA) Methodology. 2018., *www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf* (2021.07.21.)

[72] CNIL, 2018., 7.

[73] TÓTH András (szerk.): *Az infokommunikációs és technológia jogi alapjai*. Nemzeti Közszolgálati Egyetem, Budapest, 2018., 15.

mint ahogy arra a fentiekben is utaltam.[74]

A 35. cikk (4) bekezdés alapján a NAIH összeállította az adatkezelési műveletek típusainak azon jegyzékét[75], amelyekre el kell végezni a hatásvizsgálatot. Az IoT technológia többek között a lista 21. pontjának[76] feleltethető meg, így az ilyen technológiát alkalmazó rendszerek piacra dobásakor mindenképpen adatvédelmi hatásvizsgálatot kell készítenie az adatkezelőnek.

5. Az agyhullám-olvasás technológiájának adatvédelmi értékelése

5.1. Az agyhullám-olvasás, mint az emberi fejlődést segítő technológia

Az emberi agyhullámok olvasása és elemzése manapság már nem csupán a sci-fi irodalom része, azzal egyre gyakrabban kísérleteznek, sőt már a piacon is találhatóak olyan eszközök, amelyek alkalmasak erre a célra. Ilyenre példa az a kísérlet, amely során a különleges szenzorokkal letapogatott agyhullámokat arra használták, hogy azokat beszéddé alakítsák át, tehát tulajdonképpen az emberi gondolatokat hanggá transzformálják. Ez a technikai megoldás segíthet olyan embereknek a beszédben, akik korábban elveszítették beszédképességüket.[77] Japán tudósok pedig azon dolgoznak, hogy az agyhullámok letapogatásán keresztül „lefordítsák" azt, amit az agy a látóközpontjában dolgoz fel, azért hogy később azt képekké lehessen alakítani.[78] A gondolatok lefordítására és olvasására alkalmas technológia tehát már itt kopogtat az ajtónkon és csak idő kérdése, hogy a mindennapok részévé váljon.

Talán nem véletlen, hogy Ray Kurzweil szerint az emberi agy működésének megértése a legfontosabb feladat az univerzum működésének megértéséhez vezető úton és így az emberiség legnagyobb „projektjei" közé tartozik.[79]

Az emberi agy működését számos technológia alkalmazásával lehet ma már elemezni. Az agy működését és felépítését olyan képalkotási technológiákkal elemzik az orvostudományban többek között, mint az elektroenkefalográfia (EEG), a mágnesrezonancia-képalkotás (MRI), a funkcionális mágneses rezonanciavizsgálat (fMRI), komputertomográfia (CT) vagy a pozitronemissziós tomográgia (PET). Ezen technológiák használatának fő célja jelenleg az agy idegi működésének feltérképezése a sérült területek gyógyítása érdekében.[80]

Az olyan technológiákat, amelyek nem csak feltérképezik az agyműködést, de azt fel is használják valamilyen külsőleg is tapasztalható cél elérésére angol kifejezéssel élve brain-computer interface-nek, vagy röviden BCI-nek nevezik. Ezt magyarul „agy-számítógép interfésznek" fordíthatjuk. Feladatuk, hogy a számítógépet egy érintkezési felületen keresztül összekapcsolják az emberi aggyal. Az agy így hatást tud kifejteni, vagy befolyásolni tudja a gép működését és vica versa. A BCI-ket többek között az agyműködés közvetlen észlelésére, arról információ közvetítésére, annak elemzésére, osztályozására, valamint arra használják, hogy az

---

[74] PÉTERFALVI – RÉVÉSZ – BUZÁS, 2018., 226.

[75] https://www.naih.hu/hatasvizsgalati-lista#_ftn1 (2021. 07. 21.)

[76] Új technológiai megoldások használata az adatkezelés során. Ideértve az érzékelővel ellátott eszközök által előállított adatok interneten vagy más csatornán keresztül történő nagyszámú kezelése (pl.: okos televízió, okos háztartási eszközök, okos játékok stb.), és amelyek adatokat szolgáltatnak a természetes személy fizetőképességére, egészségére, személyes érdeklődési körére, megbízhatóságára vagy viselkedésére, tartózkodási helyére és amelyek alapján profilalkotás történik.

[77] Chelsea WHITE: Mind-reading device uses AI to turn brainwaves into audible speech. 2019. https://www.newscientist.com/article/2200683-mind-reading-device-uses-ai-to-turn-brainwaves-into-audible-speech/ (2021. 07. 21.)

[78] Guohua SHEN – Tomoyasu HORIKAWA – Kei MAJIMA – Yukiyasu KAMITANI: Deep image reconstruction from human brain activity. *PLOS Computational Biology 15(1)*. 2019. https://doi.org/10.1371/journal.pcbi.1006633 (2021. 07. 21.)

[79] Ray KURZWEIL: *How to create a mind, the secret of human thought revealed.* Penguin Books, New York, 2012.

[80] Giordano J. (szerk.): *Neurotechnology. Premises, Potential, and Problems.* Taylor and Francis Books, 2012., 2-3.

visszajelzést közvetítsen használójának valamilyen cél eléréséről.[81] EEG alapú BCI eszközöket már évek óta használnak arra, hogy a valós idejű agyi parancsok, tehát tulajdonképpen gondolatok által irányítson a felhasználó valamilyen számítógép által vezérelt külső eszközt. A BCI ezekben az esetekben az agy idegi elektromos aktivitása során keletkező agyhullámokat, jelen esetben tulajdonképpen a gondolatokat számítógépes parancsokká alakítja át.[82]

Böröcz István a témában nemrég megjelent tanulmánya az emberi-fejlesztési technológiákat (angol kifejezéssel: Human Enhancement Technology, avagy HET) különböző kategóriákba sorolta attól függően, hogy azok pontosan mely típusú képességeket („hatás-területet")[83] érintenek, milyen hosszan fejtik ki hatásukat, mi a fejlesztés célja, milyen mértékig integrálódik az eszköz az emberi testbe és a fejlesztés visszafordítható-e. Azokat a technológiákat, amelyek célja az emberi agy működésének feltérképezése és abból különböző információk kinyerése, kiolvasása mások számára is érthető módon, szintén a HET technológiák közé került besorolásra. Ezek olyan eszközök, amelyek képesek az emberi elme, tehát a gondolataink „olvasására" és ez által új lehetőségeket igyekszenek teremteni a felhasználónak, hozzájárulva az életszínvonal növeléséhez.[84]

5.2.Az agyhullám, mint biometrikus adat

A különböző biometrikus adatok alapján működő rendszerek egyre inkább elterjednek a világban. Ez annak köszönhető, hogy fejlődésük következtében a biometrikus rendszerek egyre gyorsabbá, megbízhatóbbá, pontosabbá, ugyanakkor olcsóbbá is váltak. Ma már szinte mindenki rendelkezik legalább egy olyan eszközzel, amely biometrikus azonosítást használ: a legtöbb laptop és mobiltelefon, illetőleg a magasabb biztonsági kategóriába tartozó pendrive mind-mind ezt a technológiát hasznosítja.[85]

A 29-es Munkacsoport vonatkozó véleménye a biometrikus adatok forrásának két típusát különbözteti meg. Egyrészt léteznek olyan rendszerek, amelyek az érintett fizikai, illetve fiziológiai jellemzőit vizsgálják. Ide tartozik az ujjnyomat-ellenőrzés, az íriszfelismerés, az arcfelismerés, a retinaelemzés, a hangfelismerés, illetve a DNS-mintázat azonosítása. A másik csoportot a viselkedésen alapuló technikák alkotják, amelyek segítségével a személy behaviorális tulajdonságait mérik. Ez utóbbi csoportba sorolják az íráskép vagy a járásmód elemzését, illetőleg az érzelmi állapot hangmintázat alapján történő felmérését.[86]

A GDPR vonatkozó fogalom meghatározása biometrikus adatnak tekinti egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adatot, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását.[87]

---

[81] BÖRÖCZ István: The exposed psyche and the constitutional ambiguities of mind reading (April 9, 2021). *Privacy in Germany (PinG) 04/2021*. https://ssrn.com/abstract=3823181, (2021. 07. 21.), 3.

[82] S. N. ABDULKADER – A. ATIA – M. S. M. MOSTAFA: Brain Computer Interfacing: Applications and challenges. *Egyptian Informatics Journal Volume 16*. 2015. www.sciencedirect.com/science/article/pii/S1110866515000237 (2021.07.21.) 214-215.

[83] A tanulmány az alábbi hat fajtáját különbözteti meg a HET-eknek, attól függően, hogy az ember milyen típusú képességeit fejlesztik, javítják: kognitív-, affektív-, morális-, fizikai-, kinézetbeli- és élethosszhoz kapcsolódó képességek.

[84] BÖRÖCZ, 2021., 5.

[85] SZABÓ – BOJNÁR – BUZÁS, 2016., 62.

[86] A 29-es Adatvédelmi Munkacsoport 3/2012. számú véleménye a biometrikus technológiák terén történt fejleményekről (WP 193). 2012. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_hu.pdf, (2021.07.21.) 4.

[87] GDPR 4. cikk 14. pont: „biometrikus adat": egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat

Az emberi agyban található idegsejtek elektromos aktivitása során keletkező agyhullámok frekvenciáinak mérésére több eszközt is kifejlesztettek már. Ezek alapvető információkat tartalmaznak az adott egyén agyának működéséről, és a közvetített információkból megannyi következtetés vonható le az emberre nézve. Az agyhullámok mérésének, olvasásának eredményeit leggyakrabban az orvostudományban használják diagnosztikai, gyógyászati célból. A szakirodalom megkülönbözteti egymás között az ún. „nyers agyi adatokat" és „agyi adatokat". A nyers agyi adatok az emberi agy elektromos aktivitására és az agyi vér áramlására, oxigén szintjére vonatkozó, különböző műszerek által technikai úton kinyert adatok. Az agyi adatok pedig a nyers adatokból szakértők által levonható következtetések az agy- és elmeműködésre nézve.[88]

Az agyhullámok olvasására során keletkező adatok a GDPR fenti fogalomhasználata alapján az adott érintett személy biometrikus adatának tekinthetőek, mivel azok egyediségük alapján lehetővé teszik az érintett azonosítását.

Adott esetben az agyhullámokból akár egészségügyi következtetések is levonhatóak, ha például azokat egy pszichiátriai kezelés keretei között vizsgálják. Ezekben az esetekben a biometrikus adat egyben egészségügyi adatként is minősül a GDPR vonatkozó fogalomhasználata szerint, mivel az agyhullámból kinyerhető információkat az érintett pszichikai egészségi állapotára vonatkozóan kezelik.[89]

5.3. Az agyhullám-olvasás technológiájának hatása az érintett személyes adatai védelméhez fűződő jogára

Az emberi-fejlesztési technológiák közül az agyhullám-olvasás érintettre jelentkező hatásával kapcsolatban Al-Rodhan idevágó, a transzhumanizmus filozófiai világát idéző gondolatai szerint ezek a technológiák megfelelő szabályozás hiányában egyrészt „szuperemberek" teremtésének eszközei lehetnek, másrészt azonban pont emiatt társadalmi egyenlőtlenségeket idézhetnek elő a HET-et igénybe vevő és azzal nem rendelkező emberek között.[90]

Böröcz elemzése szerint az agyhullám-olvasásra alkalmas HET-ek komoly kockázatokat hordoznak az érintett magánélethez való jogára. A hivatkozott szerző az angolszász jogirodalomból ismert „right to privacy", az az a magánszférához való jogra[91] hivatkozik, amely bővebb kategória, mint a kontinentális felfogás szerinti személyes adatok védelméhez való jog. A szerző az Emberi Jogok Európai Egyezményének 8. cikke szerinti magán- és családi élet tiszteletben tartásához való jog szempontjából is elemzi a kérdést.[92] Én a magam részéről a továbbiakban a személyes adatok védelmére fókuszálnék és az ezen jogot Európai Uniós szinten szabályozó GDPR vonatkozó rendelkezéseire.

A személyes adatok védelméhez való jog azért rendkívül hangsúlyos a technológia kapcsán, mivel az agyhullámokból kiolvasható információkból az érintett személy fizikai, mentális állapotára, és gondolataira vonatkozó adatokat lehet kiolvasni. Ez az előző pontban is már

---

[88] Sara LATINI: To the edge of data protection: How brain information can push the boundaries of sensitivity, Master thesis, Tilburg University, Tilburg Law School, 2018. 17-21.

[89] GDPR 4. cikk 15. pont: „egészségügyi adat": egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról.

[90] Nayef AL-RODHAN: Inevitable Transhumanism? How Emerging Strategic Technologies will affect the Future of Humanity, 2013. https://isnblog.ethz.ch/security/inevitable-transhumanism-how-emerging-strategic-technologies-will-affect-the-future-of-humanity (2021.07.21.)

[91] KOOPS et. alii.: A Typology of Privacy. *38 University of Pennsylvania Journal of International Law, 483*. 2017. Idézi: BÖRÖCZ, 2021., 11.

[92] BÖRÖCZ, 2021., 10-11.

kifejtettek alapján személyes adatnak, azon belül is az adatok különleges kategóriájára tartozó biometrikus adatnak, illetve adott esetben egészségügyi adatnak tekinthető.

Több szerző is kiemeli, hogy az agyhullámok és az azokból kiolvasható, végső soron az emberi elme működésére vonatkozó információk az emberek legszemélyesebb, legintimebb szférájának részei.[93] Mások szerint a külső (jogosulatlan) beavatkozás az emberi elme működésébe súlyosan sértheti a személyes adatok és a magánélet védelmén túl végső soron az emberi méltóságot is, ezért az elmeműködés integritása különösen erős és abszolút védelemre érdemes a jog által.[94]

A technológiai fejlődés következtében egyre gyakrabban használunk olyan eszközöket, amelyek alkalmasak az érintett magánéletébe való beavatkozásra és ezzel összefüggésben személyes adatokat kezelnek. Maradva a HET-eknél, és ezeken belül is agyhullámokat kezelő eszközökre fókuszálva ma már viszonylag sok ilyen eszköz is elérhető a piacon. Ott van például a Muse nevű fejpánt, amely az EEG-technológiát használva elemzi a felhasználó mentális aktivitását és ezáltal meditációt segítő technológiaként jelenik meg a piacon.[95] Szintén nagy hírértéke volt pár éve annak, hogy Kínában több oktatási intézményben a gyermekeknek kötelezően, de egyelőre kísérleti jelleggel egy agyhullámok olvasására és elemzésére alkalmas fejpántot kellett viselniük a tanórákon. A fejpántok wifi-n keresztül adatokat továbbítottak valamennyi gyerek figyelemszintjéről az órát tartó pedagógus számítógépére, aki élőben követhette a gyermekekről küldött adatokat. Később az adatok személyre szabott elemzésére is lehetőség van, amely segíthet az egyes tanulók képességeinek javításában.[96]

Valamennyi agyhullám-olvasó technológiával ellátott rendszernek közös tulajdonsága, hogy a megfelelő működés érdekében a leolvasott EEG-adatokat továbbítsák egy a szoftverfejlesztő által működtetett adatbázisba elemzési célból. Az eszköz által továbbított nyers agyi adatokat automatizált módon működő rendszerek elemzik, majd az elemzés során kinyert információkat megjelenítik a rendszert használó személy részére. Ezen felül a kereskedelmi forgalomban előforduló EEG-olvasó szoftvereknél a személyre szabottság érdekében a szolgáltatás megkövetelheti a felhasználói regisztrációt, IP-cím tárolást, néhol helyadatokat is.

5.4. Anonimizálható-e az agyhullám-olvasás során kinyert személyes adat?

A személyes adatok védelme szempontjából anonimizálásnak tekintjük azokat az eljárásokat, amelyek során a személyes adatokat végérvényesen megfosztják személyes jellegüktől és emiatt az a továbbiakban már se közvetlenül, se közvetetten nem lesz alkalmas arra, hogy azon keresztül az érintettet be lehessen azonosítani.[97]

A GDPR rendelkezéseit az anonimizált adatokra nem kell alkalmazni. Maga a rendelet is kimondja, hogy az adatvédelem elveit nem kell alkalmazni az anonim információkra, amelyek nem azonosított vagy azonosítható természetes személyre vonatkoznak, valamint az olyan személyes adatokra, amelyeket olyan módon anonimizáltak, amelynek következtében az érintett nem vagy többé nem azonosítható.[98]

Az agyhullám-olvasással és az így kinyert adatok kezelésével foglalkozó egyes kutatások amellett érvelnek, hogy az EEG-adatokat ugyan meg lehet fosztani a közvetlen azonosításukhoz

---

[93] HALLINAN et. alii.: Neurodata and Neuroprivacy: Data Protection Outdated? *Surveillance & Society 12(1)*, 2014., 68. Idézi: BÖRÖCZ, 2021., 12.

[94] TAYLOR P. M.: *UN and European Human Rights Law and Practice.* Cambridge University Press, Cambridge, 2005. Idézi: BÖRÖCZ, 2021., 12.

[95] Bővebb információ: https://choosemuse.com/

[96] Meng JING – Zen SOO: This startup is reading the brain of Chinese schoolkids. 2019. https://www.inkstonenews.com/tech/brainco-startup-tests-brain-reading-headbands-chinese-schoolkids/article/3005502 (2021. 07. 21.)

[97] A 29. Cikk Szerinti Adatvédelmi Munkacsoport, 2014., 5-6.

[98] GDPR (26) preambulumbekezdés

szükséges, a kinyert adatokkal párosított azonosítóktól (pl. regisztrációs szám vagy felhasználónév, illetve páciens/felhasználó neve és elérhetőségei), azonban azokat teljesen megfosztani személyes jellegüktől jelenleg szinte teljesen lehetetlen. Ennek oka, hogy a kinyert adatok teljesen egyedi jellegűek, ez pedig többször tesztelve lett már előre meghatározott körülmények között.[99] Az EEG-adatok folyamatos gyűjtése és azok összekapcsolása a korábban gyűjtött adatokkal pedig csak növeli azok személyes és azonosítható jellegét, a használt esetleges anonimizáló technológiák ellenére. Létezik olyan álláspont is, amely az EEG adat anonimitását ahhoz köti, hogy azt anonimizálása után teljesen izolált környezetben kezeljék tovább, megfosztva azt minden metaadattól. Ettől független az EEG adat anonimitása annak más – akár szintén anonim – adatokkal való összekapcsolása és a technikai elemzése során csökkenhet és az érintett újra azonosíthatóvá válhat.[100]

Az EEG-adatokat tehát anonimizálni nem, csupán pszeudonimizáli lehet. A 29-es Munkacsoport vonatkozó iránymutatása szerint a pszeudonimizált adatokat nem lehet az anonimizált információval egyenértékűnek tekinteni, mert azok továbbra is lehetővé teszik az egyéni érintettek kiválasztását és különböző adatállományokon keresztül történő összekapcsolását. A pszeudonimitás valószínűleg lehetővé teszi az azonosíthatóságot és ezért az adatvédelmi jogi szabályozás hatályán belül marad.[101] A pszeodonim adatok pedig így az anonim adatokkal ellentetében a GDPR fogalomhasználata szerinti személyes adatoknak minősülnek, így azok kezelésére alkalmazni kell a rendelet előírásait.

A fentiek alapján láthatjuk, hogy az agyhullám-olvasás technológiája olyan komoly adatvédelmi kockázatokkal jár az adatok egyedisége és az anonimizálhatóság hiánya miatt, amely a jövőben komoly kihívások elé állíthatja az emberiséget. Ez már csak azért is rendkívül fontos terület, mivel az ilyen típusú adatkezelések során az egyén mentális integritása, szellemi teljessége végső soron a tét. Habár jelen fejezetben csak a jelenség rövid bemutatására volt lehetőségem, meggyőződésem, hogy ez a technológia fogja képezni az elkövetkezendő években a legkomolyabb adatvédelmi dilemmákat az adatkezelési piacokon. Fontos ezért a kérdéskör átfogó elemzése és arról további párbeszéd kialakítása a releváns szereplőkkel.

6. Összegzés

Írásomban szerettem volna bemutatni, hogy a személyes adatok védelméhez való jog érvényesülésére milyen technológiai megoldások jelentik manapság a legkomolyabb kihívásokat. Mivel számtalan újabbnál újabb technológia jelenik meg napról napra az adatkezelési piacon, ezért négy viszonylag új, és az embereik magánéletébe való beavatkozás szempontjából nézve igen magas kockázatokat rejtő technológiát választottam ki és ezek bemutatásán keresztül igyekeztem érzékeltetni az ilyenkor felmerülő főbb dilemmákat.

A mesterséges intelligencia-fejlesztés és ezen belül is a gépek adatalapú tanítása révén láthattuk, hogy a szoftver által hozott döntések és viselkedés a tanításhoz felhasznált adatkészletek minőségén múlik. A szoftverfejlesztő és a rendszer üzemeltetőjének felelőssége ezért az ilyen rendszerek kapcsán óriási. A terület pedig minden bizonnyal az EU új MI rendelet-tervezete miatt pedig csak még hangsúlyosabb lesz a jövőben.

---

[99] J. LYNCH – D. PASKEWITZ és M. ORNE: Intersession Stability of Human Alpha Rhythm Densities. *Electroencephalographic Clinic Neurophysiological Volume 36, Issue 5.* 1974., https://www.sciencedirect.com/science/article/pii/0013469474902119 (2021.07.21.), 538–540. továbbá:
M. POULOS – M. RANGOUSSI – N. ALEXANDRIS: Neural Network Based Person Identification Using EEG Features. *Acoustics, Speech, and Signal Processing, IEEE International Conference on IEEE, Volume 2.* 1999., https://ieeexplore.ieee.org/document/759940/ (2021.07.21.), 1117–1120.

[100] BÖRÖCZ István – Paul QUINN: Electroencephalography(EEG)-based brain data: Under lenses of the General Data Protection Regulation. *Shimla Law Review, Volume-III, 2020.*, 22-23.

[101] A 29. Cikk Szerinti Adatvédelmi Munkacsoport: 2014., 11.

A blokklánc technológia kapcsán láttuk, hogy a beépített és alapértelmezett adatvédelem elvének való megfelelés miatt mind a fejlesztés, mind az üzemeltetés során mindig alaposan át kell tekinteni, hogy milyen naprakész, a blokkláncra alkalmazható technika és szervezési megoldások érhetők el a piacon és ennek megfelelően kialakítani és frissíteni az adatkezelést.

Az IoT technológia komoly problémája, hogy könnyen követhetetlenné válik a szenzor által begyűjtött adatok útja, hiszen az adatok személyek-eszközök, eszközök-eszközök, eszközök és a szolgáltatásban részt vevő más rendszerek között vándorolnak. Így az adatvédelmi megfelelés szintén kulcskérdés az érintettek védelme szempontjából.

Végül az emberi elme működésének vizsgálata az agyhullámok kezelésével kapcsolatos technológiák révén is komoly adatvédelmi jogi kérdéseket vet fel, amelyekből kiemelve néhányat általánosságban ismertettem. Az agyhullám-olvasó technológiák által kezelt adatok olyan egyedi és egyéniesített adathalmazt eredményeznek, amelyek kapcsán az anonimizálási technológiák használata jelenleg nem teszi lehetővé a teljes személytelenítést, így ilyen adatkezelések esetén igen magas, az érintett magánszférájára ható kockázatokkal kell szembesülnünk.

Mivel a fenti technológiák még csak most vannak kialakulóban azokat csak igen nagy óvatosság és fokozott óvintézkedések bevezetése mellett üzemeltethetik jogszerűen az adatkezelők. Magánéletünkre való hatás szempontjából a technológiák még jórészt feltérképezetlenek, gyorsan változnak és kiforratlanok, ezért is fontos, hogy az adatvédelmi megfelelésre fokozottan ügyeljenek az ilyen rendszereket tervező és üzemeltető adatkezelők.

Véleményem szerint a GDPR-nak való megfelelés elkerülhetetlen hosszú távon az adatkezelők részéről, így a compliance-alapú megközelítés kifejezetten fontos az ilyen projekteknél. A sűrűn változó és még kiforratlan technológiák fejlesztése során ennek jó eszköze lehet például egy adatvédelmi hatásvizsgálat elvégzése a GDPR 35. cikke alapján, amely az új technológia megoldások használata miatt egyébként explicite kötelező is a legtöbb esetben az adatkezelők részéről.