ESZTERI DÁNIEL*

A BLOKKLÁNC MINT SZEMÉLYES ADATKEZELÉSI TECHNOLÓGIA GDPR-MEGFELELŐSÉGÉRŐL

A blokkláncról manapság már szinte mindenki hallott, aki az elmúlt nagyjából tíz évben követte a technológia világából érkező híreket. Az elmúlt évek jogi szakirodalmában is sorra jelentek meg olyan publikációk, amelyek a blokklánc-technológiára épülő decentralizált vagyonkezelési rendszerek (az ún. kriptovaluták) által felvetett kérdéseket kísérelték meg elemezni, elsősorban a pénzügyi jog, a vagyonjog, illetve a bűnügyi tudományok szempontjából.

Jelen tanulmányban igyekszem elszakadni a blokklánc-technológián alapuló fizetési rendszerek és így szükségszerűen a kriptovaluták jogi elemzésétől, hiszen ezt a témát a magyar és nemzetközi szakirodalomban is számos publikáció tárgyalta már. A továbbiakban kizárólag a blokkláncban esetlegesen előforduló személyes adatok jogi sorsára szeretnék koncentrálni, kerülve így a téma pénzügyi-, vagyonjogi értékelését. Az elemzésben tehát nem lesz szó a különböző kriptovalutákról, hanem csupán az ilyen értékképző eszközök működésének alapját is jelentő adatkezelési technológiáról, amelyre nemcsak virtuális fizetési rendszereket, hanem számos más adatkezelésen alapuló rendszert is lehet fejleszteni.

A technológia használatával végzett adatkezelés jogi megfelelőségét az Európai Unió 2018-ban alkalmazandóvá vált általános adatvédelmi rendeletében[1] foglalt előírások szempontjából vizsgáltam. Ennek természetesen előfeltételének tekintettem azt, hogy a blokkláncban személyes adatok kezelése (is) történjen.

A tanulmány célja rávilágítani arra, hogy a blokklánc európai uniós adatvédelmi szempontú megfelelésének elemzése az adatkezelési technológiák fejlődési irányainak ismeretében kulcskérdéssé kezd válni. Ennek a technológiának számtalan olyan előnye van, amelynek kamatoztatása mindenképpen előnyökkel járna az európai adatkezelési piacon. Remélem, az elemzéssel elejét tudom venni a technológiával szembeni esetleges pesszimista vélekedéseknek, és sikerül rávilágítanom arra, hogy annak megfelelő irányba való fejlesztésével lehetőség nyílhat az ilyen rendszerek adatvédelmi jogi megfeleltethetőségére.

* PhD, osztályvezető, Nemzeti Adatvédelmi és Információszabadság Hatóság, 1055 Budapest, Falk Miksa u. 9–11. E-mail: *daniel.eszteri@outlook.com*.

[1] *Az Európai Parlament és a Tanács 679/2016. számú rendelete 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* (közkeletű angol rövidítéssel: GDPR).

1. A BLOKKLÁNC HASZNÁLATÁN ALAPULÓ ADATKEZELÉS SAJÁTOSSÁGAI

1.1. A BLOKKLÁNC MINT ADATOK KEZELÉSÉRE SZOLGÁLÓ SZÁMÍTÓGÉPES HÁLÓZAT

A blokklánc-technológia az ún. „distributed ledger technologies" vagy „elosztott főkönyvi technológiák" egyik gyakorlatban is megvalósított képviselője. Az elosztott főkönyvi technológia kifejezés elég precízen ragadja meg a blokkláncon alapuló adatkezelés lényegét. A tanulmányban én mégis inkább a blokklánc kifejezést használom a vizsgálat tárgyát képező konkrét technológia megnevezésére, mivel az elosztott főkönyvi technológia terminus inkább elméleti és így gyűjtőfogalomként viselkedik, továbbá – az alábbiakban is kifejtettek szerint – inkább pénzügyi/vagyonjogi szempontból van értelme a használatának. Ettől függetlenül a jobb érzékeltetés érdekében előfordulhat ennek a másik fogalomnak a használata is.

Az elosztott főkönyvi technológia mint gyűjtőfogalom lényege az Európai Központi Bank iránymutatása szerint, hogy az tulajdonjog nyilvántartására szolgál – legyen szó pénzeszköz vagy más eszköz, vagyonelem tulajdonjogáról. Jelenleg a bankok ügyleteiket – vagyis azon műveleteiket, amelyek keretében pénz- vagy egyéb pénzügyi eszközük tulajdonjoga gazdát cserél – centralizált rendszereken keresztül bonyolítják le, amelyeket gyakran központi bankok üzemeltetnek. Az elosztott főkönyv ezzel szemben olyan tranzakciós adatbázis, amely több számítógépből álló hálózaton oszlik el, nem pedig központi helyen tárolják. Az elosztott főkönyvi technológia leggyakrabban előforduló formája a blokklánc. A név onnan ered, hogy a tranzakciók csoportonként, azaz blokkonként időrendi sorrendben egymáshoz kapcsolva láncot alkotnak.[2]

A blokklánc mint adatok kezelésére szolgáló, elosztott főkönyvi technológián alapuló rendszer működésének lényegre törő és könnyen érthető összefoglalása olvasható a 2019-ben megjelent *Kriptopénz ABC* című könyvben.[3] A technológia alább következő bemutatását nagyrészt az ebben a műben olvasható összefoglalóra alapozom.

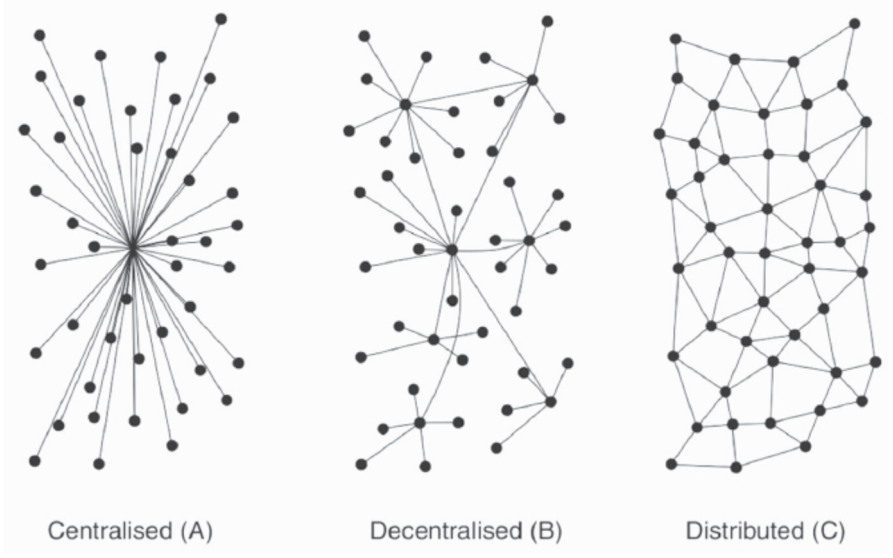
A blokkláncot – szándékosan leegyszerűsítve – adatok tárolására és mozgatására szolgáló rendszerként lehet leírni. Az adatok blokkláncon belüli tárolásának és mozgatásának előfeltétele egy számítógépekből álló hálózat. Mint látjuk, ebben a tekintetben a blokklánc nem különösebben tér el a más típusú számítógépes hálózatoktól. A különböző felépítésű számítógépes hálózatokat az említett szakkönyv három alapvető típusba sorolja: centralizált, decentralizált és elosztott.

A centralizált rendszerre jó példa egy iskola vagy munkahely belső hálózata, ahol minden felhasználó számítógépe (kliensek) ugyanahhoz a központi szerverhez kap-

[2] Európai Központi Bank: „Hogyan formálják át a technológiai újítások a pénzügyi piacokat?", 2017. április 19., *www.ecb.europa.eu/explainers/tell-me-more/html/distributed_ledger_technology.hu.html*.

[3] Györfi András – Léderer András – Paluska Ferenc – Pataki Gábor – Trinh Anh Tuan: *Kriptopénz ABC* (Budapest: HVG Könyvek 2019).

csolódik. Az adatátvitel a hálózatra kapcsolódott kliensek között úgy történik, hogy azok minden esetben először a központi szerverrel kommunikálnak, amely aztán továbbküldi az információt a címzetteknek. A decentralizált hálózati rendszerek ehhez képest már több központi szervert kötnek össze, amelyek az információ elosztásának csomópontjaiként viselkednek. Erre maga az internet a legkézenfekvőbb példa. Az elosztott típusú hálózatokban nincs az előző két típusra jellemző alá-fölé rendeltség az egyes számítógépek között. Az elosztott hálózatra kapcsolódó gépek ún. csomópontokként (angolul: „node"-okként) funkcionálnak, amelyek egymáshoz kapcsolódnak. Végeredményben mindegyik csomópont összeköttetésben áll az összes többivel. Az ilyen típusú hálózat előnye, hogy egy csomópont kiesése semmilyen fennakadást nem okoz a rendszer működésében, feladatait azonnal át tudják venni más csomópontok. Ezzel szemben egy centralizált rendszer azonnal megbénul, ha a központi egység valamiért kiesik (pl. áramkimaradás, hackertámadás vagy természeti katasztrófa következtében).[4]



1. ábra: A számítógépes hálózatok típusai: centralizált (A), decentralizált (B) és elosztott (C)[5]

A blokklánc értelemszerűen az elosztott típusú hálózatok közé tartozik. A technológia létrehozásának elsődleges célja annak megalkotója szerint egy központi kontroll nélküli fizetési rendszer megvalósítása volt.[6] Fontos azonban itt is hangsúlyozni, hogy a blokklánc nem csak fizetésre, elszámolásra alkalmas virtuális egységek

[4] Lásd Györfi–Léderer–Paluska–Pataki–Tuan (3. lj.) 57–59.
[5] Lásd Györfi–Léderer–Paluska–Pataki–Tuan (3. lj.) 58.
[6] Satoshi Nakamoto: „Bitcoin: A Peer-to-Peer Electronic Cash System" 2008, *bitcoin.org/bitcoin.pdf*.

(„kriptopénzek") mozgatására lehet alkalmas. A hálózaton kezelt adatcsomagok bármilyen más információ tárolására, kezelésére alkalmasak lehetnek, így maga a technológia univerzálisan használható más adatkezelési célokra is.

1.2. A BLOKKLÁNCOT ALKOTÓ BLOKKOK SZEREPÉRŐL AZ ADATKEZELÉSBEN

A blokklánc-technológiát használó hálózatokon az adatok tárolása az ún. blokkokban történik. Bizonyos felfogások szerint a blokkokat úgy képzelhetjük el, mint egy üres dokumentumot, papírlapot vagy táblát, amire bármilyen információt leírhatunk.[7] Ennek mentén bontva tovább a gondolatot egy blokk megszületésének pillanatában az empirista gondolkodók által használt *tabula rasa* fogalmának feleltethető meg. Ezzel az empirikus iskolát képviselő filozófusok azt kívánták érzékeltetni, hogy – véleményük szerint – az emberi elme – mint egyfajta információhordozó és feldolgozó közeg – a megszületés pillanatában még nem tartalmaz semmiféle veleszületett tudást.[8] Ehhez képest a racionalizmus filozófiai iskolájának képviselői szerint minden ember elméje rendelkezik bizonyos előre meghatározott ideákkal, amelyek elméjének mélyebb rétegeiben a születés pillanatától jelen vannak.[9] Ennek a két irányzatnak a blokklánc-alapú adatkezelések adatvédelmi jogi vizsgálatánál is fontos szerepe lehet, amelyet a tanulmány befejező részében fejtek ki részletesebben. Először azonban térjünk vissza a blokkok adatkezelésének technikai oldalára.

A blokkokban mint adattárolási egységekben bármilyen információt eltárolhatunk, függően az adott blokklánc létrehozásának céljától. A blokkláncot alkotó blokkokat először a Bitcoin-rendszer kapcsán kriptopénzekkel kapcsolatos tranzakciók adatainak tárolására használták, de azok tulajdonképpen bármilyen más adat és azokkal végzett művelet tárolására is alkalmasak lehetnek. Az egyes blokkok alkotják a blokkláncot. Az információkat tartalmazó blokkok láncszerűen, utólag megváltoztathatatlanul kapcsolódnak egymáshoz, ami annyit jelent, hogy az újabb blokkok és a bennük lévő új adatok mindig csak a lánc végére kerülhetnek. A lánc kezdetén lévő első létrejött blokkot nevezzük „genezis-blokknak".[10]

A blokklánc-alapú adatkezelés lényege egy olyan titkosítási (kriptográfiai) eljárás, ahol minden egyes fél rendelkezik legalább egy *nyilvános* és egy *privát* kulcspárral (ún. aszimmetrikus titkosítás), amelyek digitális jel- és karaktersorozatok. A nyilvános kulcsú algoritmus használatával bármely felhasználó végezhet adatkezelési műveletet a hálózaton, amely során a műveletben (pl. adatok megosztása, „mozgatása") érintett információkat, adatokat privát kulcsával rejtjelezi. Az így titkosított

[7] Lásd Györfi–Léderer–Paluska–Pataki–Tuan (3. lj.) 60.

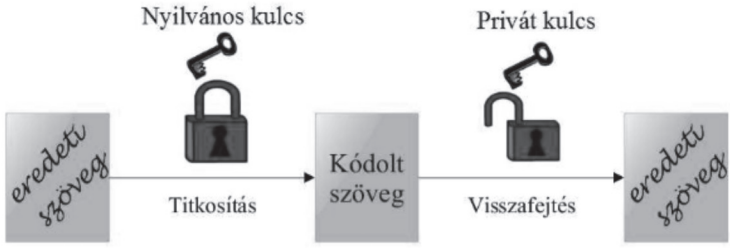
[8] Lásd erről legkorábban Arisztotelész (a „A lélekről" című műben), majd később a felvilágosodás során John Locke („Értekezés az emberi értelemről" című könyvben) írásait. Andrássy György: *Filozófia és jogászi etika* (Pécs: Dialog Campus 2008).

[9] Lásd legkorábban Platón gondolatait az ideák világáról (a „Parmenidész"-ben), majd később pl. Descartes foglal állást a racionalizmus mellett a tabula rasa koncepciójával szemben (az „Értekezés a módszerről" című műben). Lásd Andrássy (8. lj.).

[10] Lásd Györfi–Léderer–Paluska–Pataki–Tuan (3. lj.) 61.

adatokat, továbbá a műveletben érintett felek (pl. feladó és címzett) nyilvános kulcsait bármely másik felhasználó láthatja a hálózaton, azonban csak a felek tudják azt értelmezni, dekódolni a privát kulcsaik használatával.[11]

Az adatkezelési műveletet kezdeményező fél a hálózaton futó titkosító algoritmussal és saját egyedi, titkos kulcsával rejtjelezi az információt, majd a címzett fél nyilvános kulcsát hozzárendeli az általa meghatározott rejtjelezett adatokhoz, ezzel létrehozva az eredeti adat kódolt formáját. A továbbiakban kizárólag az így létrehozott kódolt adat lesz látható minden felhasználó számára a blokklánc rendszerben. A blokkláncban a címzett ehhez a kódolt adathoz hozzárendeli a saját titkos kulcsát, és az algoritmus használatával dekódolja az adatokat. A dekódolással számára az adat már értelmezhető információként jelenik meg. Az érintett adatokat tartalmazó blokkot minden esetben időpecséttel, illetve a blokkhoz kapcsolódó digitális aláírással (ún. hash) zárják le. Abban az esetben, ha a blokklánc valamely felhasználója újabb adatkezelést kíván végezni a hálózaton, a fentiekhez hasonlóan végez el egy újabb műveletsorozatot.[12]



2. ábra: A blokkláncon végzett műveletek aszimmetrikus titkosításának egyszerű ábrája[13]

Fontos kiemelni, hogy az 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.[14]

[11] Eszteri Dániel: „A World of Warcraft-tól a Bitcoin-ig: Az egyén, a gazdaság és a tulajdon helyzetének magán- és büntetőjogi elemzése a virtuális közösségekben." Doktori értekezés, Pécsi Tudományegyetem, 2015, 174–179., *ajk.pte.hu/sites/ajk.pte.hu/files/file/doktori-iskola/eszteri-daniel/eszteri-daniel-vedes-ertekezes.pdf*.

[12] Labancz Andrea: „Blockchain: az adatvédelem jövője?" in Erdős Csaba (szerk.): *Doktori Műhelytanulmányok 2018* (Budapest: Gondolat 2018) 118–120.

[13] Kallós Gábor: „Előadás: Titkosítás, RSA algoritmus" Széchenyi István Egyetem 2015, 11., *docplayer.hu/2770220-4-eloadas-titkositas-rsa-algoritmus.html*.

[14] Nemzeti Adatvédelmi és Információszabadság Hatóság állásfoglalása a blokklánc („blockchain") technológia adatvédelmi összefüggéseivel kapcsolatban, 2017. július 24., 3., *naih.hu/files/Adatved_allasfoglalas_naih-2017-3495-2-V.pdf*.

A láncszerűen felépülő és így egyre növekvő adatbázishoz az újabb adatokat újabb blokkokban adják hozzá. A blokkokban tárolt adatokkal végzett valamennyi művelet naplója is az egyes blokkokban tárolódik. A blokkláncot alkotó blokkokban tárolt adatokkal végzett műveletek naplóját nevezzük összefoglaló néven „blokktörténetnek".

A blokkláncban kezelt adatokkal végzett műveletek során a magát a műveletet elrendelő parancsot a rendszer először belefoglalja az adatot tartalmazó blokkba. Ilyenkor a rendszer rögzíti a művelettel kapcsolatos legfontosabb adatokat, például egy átutalásnál azt, hogy az adott adat feletti rendelkezési jogosultság melyik felhasználót illeti meg ezentúl.

Minden egyes blokk tartalmazza az adott műveletre jellemző információt; egy ún. *hash*-értéket; és hivatkozást a blokkláncban előtte elhelyezkedő blokkra. A *hashing* mint művelet egyirányú adatmódosítás, amelynek során a rendszer végigfuttat egy algoritmust a tranzakción, amely az információt számsorrá konvertálja, így jön létre a hash-érték. A számsor egyedileg azonosíthatóvá teszi az adatot, azonban az adat titkosított, nem fejthető vissza a hash-értékből.[15]

Ezek után az elosztott hálózatra kapcsolódott számítógépek (a csomópontok) feladata az, hogy az adatkezelési művelet hitelességét algoritmikus úton ellenőrizzék.[16] A művelet jóváhagyása során algoritmikus úton azt ellenőrzik, hogy a tranzakciót digitálisan megfelelően aláírta-e a műveletet indítványozó felhasználó, és van-e annak bármilyen hiteles előzménye a blokkláncon (tehát a hash-értékek és az érintett adatok egymásnak megfeleltethetők-e).

Amennyiben a csomópontok (vagy előre meghatározott számú csomópont) jóváhagyják a műveletet[17], úgy azt rögzítik a blokkban, ami ezentúl megmásíthatatlanul hozzákapcsolódik a teljes lánchoz. A hitelesség további garanciáját nyújtja, hogy minden egyes csomópont letölt egy másolatot ezek után a friss blokkláncból, hogy egymást is tudják folyamatosan ellenőrizni, és megosztani egymás között a blokklánc legfrissebb kópiáját.[18]

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

[15] Bagi Veronika – Héjja Domonkos – Incze Johanna – Kovács Petra – Máriás Bertalan – Molnár Antal – Olajos Marcell – Péter Dániel – Simon Orsolya Anna – Számel Artúr – Szűcs Márk – Tepliczky Dóra – Viczán Gergely: „A kriptovaluták lehetséges megjelenése a magyar jogrendszerben" 2018, 8., *josz.elte.hu/wp-content/uploads/2019/03/Kriptoprojekt_eg%C3%A9sz.pdf*.

[16] Hossein Kakavand – Sevres De Kost – Bart Nicolette – Bart Chilton: „The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies" 2017. január 1., 4–7., *dx.doi.org/10.2139/ssrn.2849251*.

[17] A kriptovalutákat kezelő blokklánc-rendszerekben a tranzakciók ellenőrzése általában különleges csomópontok, az ún. bányászgépek feladata. Jelen leírásban az egyszerűség és az adatkezelés általánosabb leírásának kedvéért nem tettem említést ezen különös csomópontokról, mivel a blokklánc-alapú adatkezelés lényege ezek nélkül is leírható.

[18] Lásd Györfi–Léderer–Paluska–Pataki–Tuan (3. lj.) 63., 68.

1.3. A BLOKKLÁNCOK BIZONYOS TÍPUSAI 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. Ilyen hálózatra a legkézenfekvőbb példa a Bitcoin-rendszer. 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.[19]

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 egészségügyi személyzet adhat hozzá adatokat. Az *engedély nélküli* blokklánc-rendszerekhez bárki kapcsolódhat, és adatokat adhat hozzá.[20]

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.[21] A felhasználók által végzett tranzakciók azonosításra szolgáló kódok közvetetten a felhasználót is azonosítják a hálózaton, azonban egyéb személyes adatok (pl. név, felhasználónév, IP-cím) kezelése hiányában azok konkrét természetes személyhez kötése szinte lehetetlen. Ettől függetlenül mégsem 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. Például az online kriptopénz-kereskedő platformokon, tőzsdéken az egyes felhasználóknak a kulcsaik mellett viszonylag sok személyes adatot is meg kell adniuk magukról (pl. e-mail-cím, felhasználónév, bankkártya- és bankszámlaadatok, azonosító okmányadatok stb.).

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

[19] 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., *ssrn.com/abstract=3091218*.

[20] Tom Lyons – Ludovic Courcelas – Ken Timsit: „Blockchain and the GDPR" in *European Union Blockchain Observatory & Forum eublockchainforum.eu*, 2018. október 16., 14–15., *www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf*.

[21] Lásd Bacon–Michels–Millard–Singh (19. lj.) 26–27.

nemcsak pszeudonim, hanem közvetetten az érintettel összekapcsolható információkat is kezelnek.[22] Ilyen rendszerek lehetnek például a bonyolultabb okosszerződéses alkalmazásokat használó platformok, amelyekről a következő részben lesz részletesebben szó.

1.4. AZ OKOSSZERZŐDÉSEK SZEREPE A BLOKKLÁNCON ALAPULÓ ADATKEZELÉSBEN

A blokkláncon alapuló adatkezeléseknek a szerződéses jogviszonyokban való alkalmazását segítik elő az ún. okosszerződések (angolul: smart contract). Az okosszerződés koncepciójáról először Nick Szabó írt 1996-ban megjelent tanulmányában. Szabó szerint az okosszerződés olyan szerződés, mely az előre meghatározott feltételek érvényesülése esetén automatikusan megvalósul, a szerződés 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.[23] A blokklánc az okosszerződések megkötésére és teljesítésére az alábbiakban foglaltak miatt lehet alkalmas.

Az okosszerződések kötésének lehetőségét mint funkciót a Vitalik Buterin által megalkotott koncepció alapján létrehozott Ethereum nevű blokklánc-technológiát alkalmazó platform vezette be először. Lényege, hogy a blokkláncalapú hálózaton olyan programokat futtatnak, amelyek az előre kikötött szerződéses feltételek megvalósulása esetén végrehajtanak bizonyos feladatokat a hálózaton az ott kezelt adatokkal.[24]

Erre jó példa lehet egy lakásbérleti szerződés megkötése, amely során a bérbeadó a szerződés létrejöttéhez és a lakáskulcsok átadásához a bérlőtől az első havi bérleti díj és kéthavi bérleti díjnak megfelelő kaució megfizetését kéri. Tételezzük fel, hogy a kulcsot egy kóddal nyitható szekrénykében helyezi el a bérbeadó a lakásajtó mellett. Maga a szerződés mindkét fél számára rejt kockázatot, hiszen a bérlő késlekedhet a díj megfizetésével, a bérbeadó pedig a kulcs átadásával. Blokkláncalapú okosszerződés kötésével azonban a kockázat minimalizálható: a hálózaton futó, előzőleg a felek mint felhasználók által hitelesített okosszerződés ugyanis automatikusan el fogja küldeni a bérlőnek a kulcs átvételéhez szükséges kódot, ahogy a megszabott összeg megérkezik a bérbeadó számlájára (az Ethereum rendszerében a kriptopénztárcájába).[25]

[22] Lásd Bacon–Michels–Millard–Singh (19. lj.) 27.

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

[24] Vitalik Buterin: „A Next-Generation Smart Contract and Decentralized Application Platform" 2013, *github.com/ethereum/wiki/wiki/White-Paper*.

[25] Lásd Györfi–Léderer–Paluska–Pataki–Tuan (3. lj.) 72–73.

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.

Nick Szabó már hivatkozott tanulmányában megemlítette az ún. okosvagyon fogalmát is, amelybe olyan vagyonelemek tartozhatnak, amelyek vagyonjogi státuszát (pl. a tulajdonos személyét) okosszerződésekben rögzített feltételek biztosítják.[26]

1.5. A BLOKKRÁCS MINT ADATKEZELÉST GYORSÍTÓ TECHNOLÓGIA

A blokkláncon alapuló adatkezelés egyik hátrányaként róják fel gyakran, hogy minél inkább nő a blokkokban tárolt adatok mennyisége, annál lassabb a rendszer működése a validálási folyamat idejének növekedése miatt. Ezen felül az egyes csomópontoknak is folyamatosan nagyobb és nagyobb adatmennyiséget kell letölteniük és kezelniük. További problémát jelenthet az adatokkal végzett műveletek volumene is, mivel az egyidőben végzett tranzakciók nagy száma is a gyorsaság ellen dolgozik.[27]

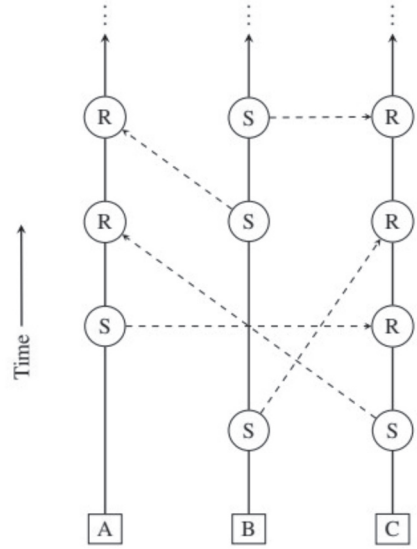
A fenti probléma megoldására született meg a blokkrács koncepciója (angolul: „block lattice"), amelynek lényege, hogy nem egyetlen, hanem párhuzamosan több blokklánc alkotja a hálózatot. A NANO elnevezésű projektben például minden egyes csomópont, tehát az összes felhasználó külön „saját" blokklánccal rendelkezik. A blokkok azonban sokkal kevesebb információt tartalmaznak, mint egy hagyományos blokklánc-rendszerben. A NANO által használt koncepció szerint ha történik egy tranzakció, akkor az utaló fél blokkláncában „utalási blokk" keletkezik, a fogadó fél blokkláncában pedig „fogadó blokk". A felhasználók blokkláncai egymással párhuzamosan, az adatkezelési műveletek pedig keresztül-kasul futnak a hálózaton. Az ellenőrzés szerepét ún. *ellenőrző csomópontok* látják el, amelyek időnként összesítik és hitelesítik a lefutott tranzakciókat.[28]

A blokkrácsban tehát az adatkezelési műveletek gyorsabban és kevesebb adat feldolgozásával futnak le, mint a „hagyományos" blokkláncban, mivel az egyes felhasználók csak a számukra releváns tranzakciókat tárolják és hitelesítik. A rendszer további hitelességének fenntartása és az egyes tranzakciók összevetése az ellenőrző csomópontok feladata. A felesleges adatkezelés kiiktatásával így erőforrások spórolhatók meg a rendszerben.

[26] Lásd Szabó (23. lj.) 9–10.

[27] Györfi András: „A blokkláncon túl vár a blokkrács" 2018. november 24., *kriptoakademia.com/2018-/11/24/a-blokklancon-tul-var-a-blokkracs.*

[28] Lásd Györfi–Léderer–Paluska–Pataki–Tuan (3. lj.) 78–80.



3. ábra: A blokkrács modellje: Az (A), (B), (C) betűk a felhasználókat (csomópontok) jelölik. A nyilak az általuk kezelt egyéni blokkláncokat, amelyek a szaggatott vonalakkal jelölt tranzakciók mentén az utaló (S) és fogadó (R) blokkok létrehozásával jönnek létre az időben előrehaladva.[29]

2. A GDPR MEGFELELŐSÉG ELSŐ LÉPCSŐJE: ALKALMAZHATÓSÁG ÉS JOGALANYISÁG

2.1. A GDPR ALKALMAZHATÓSÁGÁNAK ELŐKÉRDÉSE

Témánk szempontjából fontos előkérdés, hogy a GDPR mint európai uniós jogi norma előírásai vajon alkalmazhatók-e a blokkláncalapú adatkezelésekre. Ennek eldöntésére először tekintsük át röviden a GDPR tárgyi és területi hatályára vonatkozó előírásokat.

A GDPR 2. cikk (1) bekezdése határozza meg a rendelet tárgyát. E szerint a rendelet előírásait kell alkalmazni a személyes adatok[30] részben vagy egészben automatizált módon történő kezelésére, valamint azoknak a személyes adatoknak a nem automatizált módon történő kezelésére, amelyek valamely nyilvántartási rendszer részét képezik, vagy amelyeket egy nyilvántartási rendszer részévé kívánnak tenni. A GDPR ezen előírásai tehát a személyes adatokon végzett automatizált vagy bizonyos helyzetekben nem automatizált (nyilvántartások vezetése) műveleteket vonja annak hatálya alá.

[29] Lásd Györfi (27. lj.).

[30] A GDPR 4. cikk 1. pontja szerint a közvetlenül vagy közvetett módon azonosított vagy azonosítható természetes személyre („érintett") vonatkozó bármely információ minősül személyes adatnak.

A GDPR 4. cikk 2. pontja határozza meg az adatkezelés fogalmát, amely alapján ennek minősül a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége. Adatkezelés lehet a személyes adatok gyűjtése, rögzítése, rendszerezése, tagolása, tárolása, átalakítása vagy megváltoztatása, lekérdezése, az azokba való betekintés, felhasználásuk, közlésük továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétellel, összehangolásuk vagy összekapcsolásuk, továbbá azok korlátozása, törlése, illetve megsemmisítése.

Ezen fogalommeghatározás és a rendelet fentiekben idézett 2. cikk (1) bekezdése alapján a személyes adatokkal végzett szinte bármilyen művelet annak *tárgyi hatálya* alá esik. A blokklánc-technológiát használó automatizált adatkezelések akkor eshetnek a GDPR tárgyi hatálya alá, ha ahhoz közvetlenül vagy akár közvetetten (pl. pszeudonim módon) kapcsolódva személyes adatok kezelése is történik.

Ha feltételezzük, hogy a blokkláncot személyes adatok kezelésére is használják, úgy további kérdésként merül fel, hogy vajon a GDPR *területi hatályra* vonatkozó rendelkezései alapján azt pontosan hol történő adatkezelésekre kell alkalmaznunk.

A GDPR 3. cikke tartalmazza a területi hatályra vonatkozó előírásokat. Ezek alapján különbséget tehetünk az olyan adatkezelők[31] között, akik az Európai Unióban rendelkeznek, illetve nem rendelkeznek *tevékenységi hellyel*.

Az EU-ban tevékenységi hellyel rendelkező adatkezelőkkel kapcsolatban a következőket állapíthatjuk meg. A GDPR 4. cikk 16. pontja ugyan meghatározza a tevékenységi *központ* fogalmát, azonban a területi hatályra vonatkozó értelemben a tevékenységi *hely* fogalmával adós marad. A törzsszövegen kívül a rendelet (22) preambulumbekezdésében találkozhatunk a tevékenységi helyre vonatkozó előírásokkal, amely alapján „a tevékenységi hely valamely tevékenység tényleges és valós, tartós jelleget biztosító keretek közötti gyakorlását feltételezi. E keretek jogi formája – legyen szó akár fióktelepről vagy jogi személyiséggel rendelkező leányvállalatról – e tekintetben nem meghatározó tényező." A GDPR 3. cikk (1) bekezdése azt is kimondja, hogy az adatkezelést nem feltétlenül kell fizikai értelemben az uniós tevékenységi helyen (annak a területén) végezni, hanem elég, ha az adatkezelést az adatkezelők vagy adatfeldolgozók „tevékenységeivel összefüggésben" végzik. A tevékenységi hely meghatározása szempontjából tehát nincs jelentősége annak a tényezőnek, hogy az adatkezelést milyen jogi formában gyakorolják.[32] Az EU-ban a valamilyen fajta adatkezelési tevékenység végzésére alkalmas hellyel rendelkező adatkezelőknek az ilyen helyszínen végzett adatkezeléseire alkalmazni kell a rendelet előírásait.

Különböző esetekben az EU-ban tevékenységi hellyel nem rendelkező adatkezelőkre is kiterjed a GDPR területi hatálya (ún. extraterritoriális hatály). A GDPR 3. cikk (2) bekezdése alapján a „rendelet előírásait kell alkalmazni az Unióban tartózkodó érintettek személyes adatainak az Unióban tevékenységi hellyel nem rendel-

[31] A GDPR 4. cikk 7. pontja alapján adatkezelőnek minősül az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza [...].

[32] Péterfalvi Attila – Révész Balázs – Buzás Péter (szerk.): *Magyarázat a GDPR-ról* (Budapest: Wolters Kluwer Hungary Kft. 2018) 58–59.

kező adatkezelő vagy adatfeldolgozó által végzett kezelésére, abban az esetben, ha az adatkezelési tevékenységek áruknak vagy szolgáltatásoknak az Unióban tartózkodó érintettek számára történő nyújtásához kapcsolódnak". Röviden összefoglalva tehát, ha az adatkezelési tevékenységek termékeknek vagy szolgáltatásoknak az érintettek részére történő nyújtásához kapcsolódnak, az EU-ban tevékenységi hellyel nem rendelkező adatkezelő vagy adatfeldolgozó az EU-ban tartózkodó érintettek személyes adatait csak a GDPR előírásainak betartásával kezelheti. Ez a követelmény független attól, hogy a szolgáltatáshoz társul-e bármilyen kifizetés, vagy esetleg azt ingyenesen is igénybe lehet venni. Ha tehát a vizsgált adatkezelő tartós jelleggel olyan, (akár csekély mértékű) valós és tényleges tevékenységet folytat az Európai Unió területére irányítva, amelynek keretében az ott tartózkodó érintettek személyes adatainak kezelésére sor kerül, úgy EU-s tevékenységi hely hiányában is alkalmazni kell az általa végzett adatkezelésre a GDPR előírásait.[33]

A fentiek alapján megállapíthatjuk, hogy akár nyilvános, akár privát blokkláncról beszélünk, személyes adatok kezelése esetén arra alkalmazni kell a GDPR előírásait. Ennek azonban előfeltétele, hogy a technológiát alkalmazó adatkezelő tevékenységi hellyel rendelkezzen az Európai Unióban, illetve ennek hiányában az ott tartózkodó érintettek adatait kezelje a tevékenységének keretein belül. A privát, tehát egy adott adatkezelő által fejlesztett, fenntartott és csatlakozás szempontjából „zárt" blokklánc megítélése ebből a szempontból egyszerűbbnek tűnik. A privát blokkláncalapú adatkezeléshez való csatlakozást ugyanis kellően szűkre lehet már előzetesen szabni a csomópontokat üzemeltetők és felhasználók szempontjából. Egy blokkláncalapú egyészségügyi vagy földhivatali nyilvántartásban például az adatokat tároló csomópontok hálózati struktúrája kialakítható „házon belül" is. A nyilvános blokklánc már problematikusabb, mivel ehhez akár olyan csomópontok is kapcsolódhatnak, amelyek harmadik országban működnek. Ennek hatására pedig a blokkláncon tárolt adatok könnyen olyan helyre kerülhetnek, ahol az adatvédelem szintje nem felel meg a harmadik országba történő adattovábbítás GDPR-ban foglalt követelményeinek.[34]

2.2. AZ ADATKEZELŐ ÉS AZ ADATFELDOLGOZÓ AZONOSÍTÁSA A BLOKKLÁNCON

A blokkláncon belül az adatkezelők és az adatfeldolgozók[35] azonosításával a francia adatvédelmi hatóság (Commission Nationale de l'Informatique et des Libertés, röviden: CNIL) jelentése[36] és magyar adatvédelmi hatóság (Nemzeti Adatvédelmi és Információszabadság Hatóság, röviden: NAIH) állásfoglalása[37] is foglalkozott.

[33] Lásd Péterfalvi–Révész–Buzás (32. lj.) 59–60.
[34] Lásd GDPR 44–50. cikkei.
[35] A GDPR 4. cikk 8. pontja alapján adatfeldolgozó az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel.
[36] CNIL: Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data, 2018. 11. 06., *www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf.*
[37] Lásd NAIH (14. lj.).

A CNIL jelentése szerint egy blokkláncalapú adatkezelés során adatkezelőnek minősülhet az a „résztvevő”[38], aki arról döntött, hogy regisztrálja magát a szolgáltatásra, és így adatokat ad hozzá az adatbázishoz, majd azokat valamilyen más adatkezelési művelet során hitelesítésre küldi szét a hálózaton. Ez független attól, hogy a résztvevő természetes személyként, jogi személyként vagy esetleg egyéb szervként vesz részt a folyamatokban. A CNIL kiemeli, hogy a természetes személy csak akkor minősül adatkezelőnek, ha nem kizárólag magáncélból, hanem szakmai vagy üzleti célból kezel adatokat.[39]

A NAIH állásfoglalása az adatkezelő személyét illetően nagyrészt megegyezik a CNIL-ével. Az állásfoglalás alapján minden egyes olyan felhasználó, amely blokkokat és abban tárolt adatokat ad hozzá a rendszerhez egyben adatkezelőnek minősül. Ennek oka, hogy rendszerhez adatokat hozzáadó felhasználó kizárólagos rendelkezési jogosultságot kap a blokkokban tárolt adatai felett, így ő határozhatja meg, hogy az adatokat mely tranzakciók kivitelezéséhez fogja felhasználni. Amennyiben a tranzakciók révén a blokkban tárolt személyes adatok feletti rendelkezési jogosultságot átadták egy másik felhasználónak, onnantól kezdve ez a felhasználó (az adatok címzettje) szerez az adatok felett rendelkezést, így ő minősül adatkezelőnek.[40]

A CNIL jelentése az adatfeldolgozók személyének azonosításával kapcsolatban kifejti, hogy az adatkezelési műveletek kriptográfiai hitelesítése a hálózaton a többi csomópont által adatfeldolgozásnak minősül. Azon csomópontok üzemeltetői, akik a más résztvevő által elrendelt műveletek hitelesítését végzik adatfeldolgozást végeznek. Ennek oka, hogy az adatkezelés célját ebben az esetben nem ők határozták meg, csupán részt vesznek azok hitelesítésében a technikai szabályozó közeg sajátosságai miatt.[41]

A CNIL a fentieken túl adatfeldolgozónak tekinti azokat is, akik a blokklánchoz okosszerződések kötésére és teljesítésére alkalmas alkalmazásokat fejlesztenek, amelyeket használva azonban a szükséges személyes adatokat már egy másik adatkezelő adja meg. Az elhatárolás lényege itt is az lesz, hogy az okosszerződés megkötése során a szükséges személyes adatok körét és az adatkezelés célját jellemzően nem a fejlesztő határozza meg, csupán az eszközt tervezi meg hozzá.[42]

A CNIL által hozott példával élve: egy szoftverfejlesztő cég olyan blokkláncon futó okosszerződés alkalmazást fejleszt és üzemeltet egy biztosítótársaságnak, amely automatikusan visszatéríti a repülőjegy árát az utasoknak, ha a járatot törölték, vagy késett. Ebben az esetben az alkalmazást üzemeltető cég adatfeldolgozónak, az adatkezelés célját meghatározó biztosító pedig adatkezelőnek minősül.[43]

A hatóságok fenti megállapításai pontosan körülírják, hogy a blokkláncon ki minősülhet adatkezelőnek és adatfeldolgozónak. Megjegyzem, hogy privát blokklánc ese-

[38] A CNIL jelentésének angol verziója is a „participant”, tehát magyarul a „résztvevő” kifejezést használjuk.
[39] Lásd CNIL (36. lj.) 1.
[40] Lásd NAIH (14. lj.) 4.
[41] Lásd CNIL (36. lj.) 2.
[42] Lásd CNIL (36. lj.) 3.
[43] Lásd CNIL (36. lj.) 3.

tén könnyebb feladat az adatkezelő személyének azonosítása, mivel ott az azt létrehozó szervezet (pl. a fenti példánál maradva a biztosító) határozza meg, hogy milyen adatkezelési célokra kívánja létrehozni a blokkláncalapú adatbázist. Az érintettek adatait jellemzően az adatkezelő és az érintett között létrejött szerződési feltételeknek megfelelően kezelik az adatkezelő által erre a célra fenntartott rendszerben. A rendszerhez az adatok és az ezeket tároló blokkok hozzáadása, továbbá a konkrét műveletek elvégzése az adatkezelő kötelezettsége.

Nyilvánosan működő blokklánc esetén az adatkezelő azonosítása azonban problémás lehet, ugyanis itt bárki, aki a rendszerhez csatlakozik, saját céljainak megfelelően blokkokat és személyes adatokat adhat hozzá a hálózathoz. A nyilvános blokklánc üzemeltetése ezért adatvédelmi szempontból sokkal kockázatosabb adatkezelést eredményez. Fontos azonban megemlíteni, hogy a gyakorlatban a nyilvános blokkláncokat eddig jellemzően olyan rendszereknél használták, ahol személyes adatok kezelésére nem vagy csupán pszeudonim formában kerül sor (lásd pl. Bitcoin és más kriptovaluták). Egy személyes adatokat nyilvánosan, nem anonim vagy legalább pszeudinom formában kezelő blokklánc megfelelése a GDPR rendelkezéseinek ezért erősen kérdéses. Erre véleményem szerint igen ritkán, teljes mértékben közérdekből nyilvános személyes adatok[44] kezelése esetén lehet elméleti lehetőség.

3. A GDPR MEGFELELŐSÉG MÁSODIK LÉPCSŐJE: AZ ADATKEZELÉS BIZTONSÁGA

3.1. AZ ADATKEZELÉS BIZTONSÁGA ÉS A BLOKKLÁNC ÁLTALÁNOSSÁGBAN

A GDPR a személyes adatok kezelésének biztonságával kapcsolatban is tartalmaz különböző előírásokat a 32. cikkében, 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.

[44] Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 3. § 6. pontja alapján *közérdekből nyilvános adat:* a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét a törvény közérdekből elrendeli.

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 CNIL által kiadott módszertani útmutató is, amely az adatkezeléssel járó kockázatok csökkentésére szolgáló biztonsági/védelmi intézkedéseket mutatja be többet között.[45] A CNIL módszertana 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).[46]

A GDPR 32. cikke némi fogódzóul hoz pár példát a megfelelő biztonsági intézkedésekre, amelyek a következők:

- a személyes adatok álnevesítése és titkosítása,
- az adatkezelésre használt rendszerek és szolgáltatások bizalmas jellegének, integritásának és rendelkezésre állásának biztosítása,
- fizikai vagy műszaki incidens esetén az adatok helyreállíthatóságának képessége,
- az adatkezelés biztonságára hozott intézkedések hatékonyságának rendszeres tesztelése, illetve az erre szolgáló eljárás.

A blokklánccal kapcsolatban a biztonságos adatkezelés GDPR-beli, fentiekben ismertetett követelményének való megfelelés meglehetősen ambivalens kérdéskör.

Láthatjuk egyrészt, hogy az elosztott hálózati struktúra rendkívül szilárd rendszert alkot, ahol adatvesztés, adatmegsemmisülés csak akkor fordulhat elő, ha esetleg a teljes hálózat, benne az összes csomóponttal ki van téve valamilyen fizikai vagy műszaki incidensnek. Ez nemcsak az adatok esetleges megsemmisülésére, hanem azok jogosulatlan vagy véletlen törlésére, megváltoztatására is igaz. Mivel a csomópontok folyamatosan ellenőrzik a teljes adatbázis integritását és struktúrájának egységességét, ezért a biztonság sérüléséből adódó, az adatok rendelkezésre állását vagy integritását érintő adatvédelmi incidensek[47] megvalósulásának esélye szinte minimális. Az adatok bizalmasságát érintő biztonsági incidens (az adatok jogosulatlan közlése vagy az azokhoz való hozzáférés) a személyes adatokkal azonban blokkláncalapú adatkezelések esetén is ugyanúgy bekövetkezhet, ezért maga a technológia ezekre nem nyújt önmagában megfelelő megoldást.

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

[46] Lásd CNIL (45. lj.) 7.

[47] A GDPR 4. cikk 12. pontja alapján: „adatvédelmi incidens": a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

Egy blokkláncalapú adatkezelés továbbá rendkívül jó megoldás az adatok szinte azonnali helyreállíthatósága miatt, hiszen gyakorlatilag valamennyi csomópont egyfajta biztonsági mentési feladatot is ellát a hálózaton. Végül az adatok alapértelmezett titkosítása is olyan tulajdonság, amely a legtöbb blokkláncon alapuló rendszerbe alapvetően be van építve (lásd a tanulmány 1. fejezetében foglaltakat).

A fenti, biztonsági szempontból előnyösnek tűnő tulajdonságok azonban egyszersmind negatívumként is funkcionálhatnak. Például egy jogosulatlan hozzáférésből vagy adatközlésből fakadó (bizalmassági) adatvédelmi incidensnek mindörökre nyoma marad a blokkláncon, az incidenst okozó művelet „tranzakciós" naplói révén. Igaz, ez egyben az incidens adatkezelő általi feltárását, dokumentációját és annak – a GDPR 33. cikk (5) bekezdése szerinti – nyilvántartásba vételét is megkönnyíti egyben.

A blokklánc használatának másik negatívuma, hogy nem minden jellegű adatkezelésnél tekinthető arányosnak a körülményekre, célokra és az érintettek jogaira jelentett kockázat szempontjából. Egy, az érintett hozzájárulásán (GDPR 6. cikk (1) bekezdés a) pontján[48]) alapuló adatkezelésnél (pl. hírlevélküldő szolgáltatás) aránytalan biztonsági intézkedésnek tűnhet blokkláncalapú adatbázis üzemeltetése, mivel az érintett hozzájárulásának visszavonása esetén adatainak végleges és visszaállíthatatlan törlése a rendszerből nehézségekbe ütközne a technológia sajátosságai miatt. Az intézkedés így az adatkezelés jellegére tekintettel nemcsak túlzó, de egyben az ilyen esetekben az érintettnek a GDPR 17. cikk (1) bekezdés b) pontja[49] alapján fennálló törléshez való jogát is korlátozza (erről bővebben később).

3.2. TITKOSÍTÁSI TECHNOLÓGIÁK ALKALMAZÁSA

A blokklánc további előnye, hogy a benne kezelt adatokat alapértelmezetten titkosított formában tárolják és kezelik, azokhoz pedig csak a dekódoláshoz szükséges privát kulccsal rendelkező felhasználók férhetnek hozzá. A hatékony és naprakész titkosítás használatát a GDPR is olyan intézkedésnek tekinti, amely megfelelő garanciát nyújthat az adatbiztonság garantálására.

A titkosításra használt technológiák azonban az idő múlásával és a visszafejtési technológiák párhuzamos fejlődésével könnyen elavulhatnak. A NAIH is megállapította egyik adatvédelmi hatósági eljárásban hozott határozatában, hogy egy évek óta elavult titkosítási technológia használata (a konkrét ügyben ez az MD5 nevű algoritmus volt) a személyes adatok védelme szempontjából nem tekinthető elégséges

[48] A GDPR 6. cikk (1) bekezdés a) pontja szerint „a személyes adatok kezelése kizárólag akkor és annyiban jogszerű, amennyiben [...] az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez; [...]."

[49] A GDPR 17. cikk (1) bekezdés b) pontja szerint „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 [...] értelmében az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja; [...]."

biztonsági intézkedésnek, és az adatkezelés kockázatait növelő tényező.[50] Fontos ezért, hogy az adatkezelő mindig olyan titkosítási technológiára alapítsa a blokklánc-alapú adatkezelést, amely megfelel a tudomány és technológia mindenkori állásának.

A vonatkozó szakirodalom több olyan intézkedést is említ, amely a titkosítás hatékonyságát növelheti. Ilyen például a CNIL által is ajánlott „borsozott hash" („peppered hash") módszer, amelynek lényege, hogy az adatokhoz titkosításuk előtt hozzáadnak egy titkos jelszót is, így a visszafejtéshez nem elég a kulcs, hanem a jelszót is tudni kell.[51]

Egy másik lehetőség az ún. „nullaismeretű bizonyítás" („zero-knowledge proof") használata. Ennek lényege, hogy a rendszer egy adat kezelésének visszaigazolása kapcsán bináris (igaz/hamis) választ ad a kérdésre, az adathoz való konkrét hozzáférés nélkül. Az ilyen technológiát használó blokkláncoknál csak azt láthatják a résztvevők, hogy az adattal végzett tranzakció visszaigazolhatóan megtörtént-e, de azt nem, hogy mely publikus kulcsok között ment az végbe.[52]

Végül érdemes megemlíteni a „zajhozzáadás" módszerét, amelyet a 29-es Adatvédelmi Munkacsoport is elismert mint potenciális anonimizálási technikát.[53] Eszerint a blokkláncon végzett egyes tranzakciókat csoportokba vonnak össze, így a külső szemlélő számára lehetetlen azonosítani a konkrét feladókat és címzetteket.[54]

4. A GDPR MEGFELELŐSÉG HARMADIK LÉPCSŐJE: AZ ÉRINTETTEK ÉS JOGAIK

Az adatbázis-építés és -kezelés fő elveit (parancsait) hagyományos értelemben a „CRUD" mozaikszóval írhatjuk le. Ez a „Create-Read-Update-Delete" szavak rövidítéséből következik, amelyet magyarul a „létrehoz-olvas-frissít-töröl" szókapcsolattal jelölhetünk. Ehhez képest a blokklánc-technológián alapuló adatbáziskezelés a „CRAB" mozaikszóval érzékeltethető, amely a „Create-Retrieve-Append-Burn" szavakból ered, ami magyarul a „létrehoz-lekérdez-hozzáfűz-éget" parancsokat jelenti. A két folyamat között az utolsó két lépésben van különbség, mivel a blokklánc nem teszi lehetővé a benne kezelt adatok frissítését és törlését, csupán a régebbi adatokhoz újabbak hozzáfűzését, illetve az adatok eléréséhez szükséges titkosító kulcsok megsemmisítését (elégetését). Mindkét lépésnél az érintett adatokat tovább kezeli a hálózat: a hozzáfűz parancs használata esetén az időben újonnan hozzáadott adatok jelentik a régiek továbbkezelése mellett a „frissített" adatbázis alapját. Az éget parancs pedig csak az adatokhoz való hozzáférési lehetőséget szünteti meg.[55]

[50] NAIH/2019/2668/2. sz. határozat, *naih.hu/files/NAIH-2019-2668-hatarozat.pdf*, 3.
[51] Lásd CNIL (36. lj.) 6.
[52] Michéle Finck: „Blockchain and the General Data Protection Regulation" *European Parliamentary Research Service,* PE 634.445, July 2019, 33.
[53] 29. cikk Szerinti Adatvédelmi Munkacsoport: 05/2014. számú vélemény az anonimizálási technikákról (WP216), 13.
[54] Lásd Finck (52. lj.) 34.
[55] Gautam Dhameja: „GDPR and CRAB – What's the deal?" *The BigchainDB Blog,* 2018. június 20. *blog.bigchaindb.com/gdpr-and-crab-whats-the-deal-5c2f6b55d90*.

A fentiekből következik, hogy a GDPR-ban foglalt egyes, az érintett személyeket megillető jogok közül néhány egy blokkláncalapú adatkezelés viszonylatában (első ránézésre) értelmezhetetlen lesz. Az adatkezelő nem fogja tudni mindig teljeskörűen teljesíteni az érintetti joggyakorlási kérelmeket egy blokkláncalapú adatkezelés kapcsán. Az alábbiakban az érintetteket megillető jogok közül a blokklánccal kapcsolatban leginkább érdekeseket emeltem ki, így a hozzáférési jogot, a helyesbítéshez való jogot és végül a leginkább problémást: a törléshez való jogot.

4.1. AZ ÉRINTETT HOZZÁFÉRÉSI JOGA

A GDPR 15. cikke rendelkezik arról, hogy érintett jogosult arra, hogy az adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha igen, jogosult arra, hogy a személyes adatokhoz és azokkal kapcsolatban ezen cikk (1) bekezdés a)–h) pontjai által meghatározott információkhoz (pl. az adatkezelés céljai, az adatok kategóriái, a tárolás időtartama) hozzáférést kapjon.

A hozzáféréshez való jog az érintetti jogok közül az egyik legalapvetőbb, az érintett általi gyakorlása pedig kaput nyithat további érintetti jogok gyakorlása felé. Ha például az érintett hozzáférési jogát gyakorolja az adatkezelőnél, majd a számára szolgáltatott információk alapján tudomására jut, hogy személyes adatai pontatlanok, úgy később erre hivatkozva gyakorolhatja az őt a GDPR 16. cikke alapján megillető helyesbítéshez való jogát.

A hozzáférési jog gyakorlása esetén az adatkezelő kötelezettsége, hogy valamennyi általa kezelt adatot átkutasson az érintett személyes adatai után, majd azokat az érintett rendelkezésére bocsássa. Amennyiben az adatkezelő blokkláncalapú adatkezelést végez, úgy szintén terheli ez a kötelezettség.

Michéle Finck az Európai Parlament felkérésére 2019-ben írt tanulmányában kifejtett álláspontja szerint csupán a technológia működése alapján ennek egyébként nem is lehet különösebb akadálya. A jog hatékony gyakorlásának természetesen előfeltétele, hogy az adatkezelő olyan megfelelő mechanizmusokat dolgozzon ki, amelyek ezt megkönnyítik. Probléma lehet a jog megfelelő gyakorlása szempontjából, ha a blokkláncon a csomópontok üzemeltetői közös adatkezelőnek minősülnek. Erre sor kerülhet az adatkezelést létrehozó, az adatkezelők által kötött szerződéses rendelkezések alapján. Az adatkezelésben részt vevő csomópontok az adatbázis egészét nézve elvileg nagyrészt titkosított adatokkal rendelkeznek, és nem biztos, hogy mindegyik hozzáfér a feloldáshoz szükséges kulcspárhoz. Az érintett hozzáférési jogának gyakorlása [lásd: GDPR 26. cikk (3) bekezdés[56]] szempontjából ezért a közös adatkezelőknek megfelelően kell egymás között rendezni az erre vonatkozó eljárást (pl. érintett kérelem esetén ki kit értesít, ki kommunikál az érintettel stb.).[57]

[56] A GDPR 26. cikk (3) bekezdése alapján az érintett a közös adatkezelők által létrehozott megállapodás feltételeitől függetlenül mindegyik adatkezelő vonatkozásában és mindegyik adatkezelővel szemben gyakorolhatja a rendelet szerinti jogait.

[57] Lásd Finck (52. lj.) 72.

4.2. A HELYESBÍTÉSHEZ VALÓ JOG

A GDPR 16. cikke alapján az érintettet megilleti a jog, hogy kérésére az adatkezelő helyesbítse a rá vonatkozó pontatlan személyes adatokat. Ezen felül az adatkezelés célját figyelembe véve az is jogában áll, hogy kérje a hiányos személyes adatok kiegészítését.

A blokkláncon alapuló adatkezelés alapvető ismérvei miatt – amely a kezelt adatok biztonságát és megváltoztathatatlanságát helyezi előtérbe – a helyesbítéshez való érintetti jognak a gyakorlása már komoly nehézségekbe ütközhet. A blokkláncon az adatokkal végzett műveletek lenyomata ugyanis visszafordíthatatlanul „beleég" az adatbázisba, így ha azokat később módosítják, helyesbítik is, a korábbi adatok is szerepelni fognak előzményként a rendszerben.

Egyes vélemények szerint egy privát blokklánc üzemeltetése esetén az adat helyesbítése megoldható lehet, az azt tartalmazó blokk újrahashelése (tehát az adatkezelési műveleteket hitelesítő algoritmikus lenyomatok újrakalibrálása) révén. Ez azért tűnik könnyebben kivitelezhetőnek, mivel itt a rendszert jellemzően egy adatkezelő üzemelteti, aki dönthet erről. Bonyolultabb a helyzet a publikus blokkláncok esetében, ahol a rendszer központi adatkezelői kontroll nélkül működik, és így valamennyi csomópont-üzemeltető önálló, a teljes adatbázis másolatával rendelkező adatkezelőnek tekinthető. Minél többen csatlakoznak a hálózathoz, az adott csomópontnak annál nehezebb lesz „meggyőznie" az adatok helyesbítéséről a többi csomópontot.[58]

Ezen érintetti jog kapcsán ki kell emelni, hogy a 16. cikk második mondata a személyes adatok kiegészítésére ad lehetőséget a helyesbítés helyett (esetleg mellett) az adatkezelés célját figyelembe véve. Az adatok kiegészítése révén már jobban megfeleltethető lehet a blokkláncalapú adatkezelés a GDPR ezen előírásának a következők miatt. A már korábban bemutatott tulajdonságai miatt a blokklánc alkalmassá tehető arra, hogy a benne kezelt adatokhoz további információk hozzáadása révén érjük el azok helyesbítését.

Fontos azonban, hogy a korábbi (helytelen) adatokat ilyenkor továbbra is kezelni kell, csupán az azokhoz későbbiekben hozzáfűzött kiegészítő információk fogják megmutatni a már helyesbített formát. Pontosan erre való tekintettel az adatok helyesbítéséhez való jog gyakorlása az adatok kiegészítésének formájában nem minden típusú adatkezelés esetén tűnhet megfelelő megoldásnak. Ezért is fogalmaz itt úgy a rendelet, hogy a kiegészítés lehetősége csak az adatkezelés célját figyelembe véve gyakorolható. Ez összhangban van azzal az érveléssel, amelyet az Európai Bíróság (EUB) előtti Peter Nowak kontra Data Protection Commissioner (Írország) ügyben képviselt Juliane Kokott főtanácsnoki indítványában, amely alapján: „a személyes adatok helyességét és teljességét a [...] gyűjtésük vagy további kezelésük céljára tekintettel kell értékelni."[59] A fentiekre tekintettel egy blokkláncalapú adatkezelés jogszerűsége az érintetti jogok érvényesítése szempontjából szükség-

[58] Lásd Bacon–Michels–Millard–Singh (19. lj.) 76–77.

[59] Juliane Kokott főtanácsnok indítványa C434/16 sz. ügy Peter Nowak v. Data Protection Commissioner [2017] EU:C:2017:582, para 35.

szerűen sérül, ha az adatkezelés céljával csak a helytelen adatok tényleges kijavítása egyeztethető össze.

4.3. A TÖRLÉSHEZ („ELFELEDTETÉSHEZ") VALÓ JOG

Az érintett joga ahhoz, hogy a személyes adatai törlését kérje a GDPR 17. cikkében szerepel. Ezek alapján az érintett jogosult személyes adatai törlését kérni az adatkezelőtől. Az adatkezelő számára ezen kérés teljesítése különböző feltételek teljesülése esetén kötelező [GDPR (1) bekezdés a)-f) pontjai].

A törléshez való jog tehát bizonyos esetekre limitált a rendelet előírásai alapján, ezen felül a feltételek teljesülése esetén a már nyilvánosságra hozott személyes adatokra vonatkozó különös szabállyal összhangban kell annak eleget tennie az adatkezelőnek.[60] Ezen felül a törléshez való jogot nem lehet ellentétesen gyakorolni ezen jog szellemiségével, eredeti céljával.[61]

A blokklánc-technológiával összefüggésben a törléshez való jog gyakorlása veti fel a GDPR-megfelelőség tekintetében a legtöbb problémát, ahogy arra már korábban többen is felhívták a figyelmet.[62] Rendkívül nehézkessé teszi az adatok törlését a blokkláncból az a körülmény, hogy minden egyes a hálózathoz csatlakozott csomópontnak végre kellene hajtania a műveletet a saját másolatában, majd a törlés kivitelezése után újraépítenie a blokkláncot a törölt adatok nélkül, figyelemmel a közben folyamatosan eszközölt újabb tranzakciókra is. Értelemszerűen minél régebben keletkezett az adat blokkláncban, ez a művelet annál nehezebben és időigényesebben lenne kivitelezhető.[63]

Amennyiben a törléshez való jog értelmezése kapcsán az EUB eddigi esetjogából indulunk ki, mindenképpen érdemes megemlíteni a Google Spain ügyben 2014-ben hozott ítélet megállapításait. Az ítélet alapján a személyes adatok törlésével „egyenrangú" intézkedésként ítélte meg a bíróság az érintett személyes adatainak eltávolítását a Google keresési felületéről. Ez a művelet ugyan nem járt az eredeti – egy online hírportálon az érintettről közölt – személyes adatok törlésével, viszont a személy nevére (vagy más adataira) való keresés eredményeképpen a Google indexáló szolgáltatása már nem eredményezett találatot. A keresőszolgáltató és az adatokat eredetileg közlő sajtóorgánum közötti kapcsolat megszakítása a releváns adatokra mutató hivatkozások törlése révén így elégséges védelmi intézkedésnek volt tekinthető az ítélet alapján.[64]

[60] GDPR 17. cikk (2) bekezdés: „Ha az adatkezelő nyilvánosságra hozta a személyes adatot, és az (1) bekezdés értelmében azt törölni köteles, az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az észszerűen elvárható lépéseket – ideértve technikai intézkedéseket – annak érdekében, hogy tájékoztassa az adatokat kezelő adatkezelőket, hogy az érintett kérelmezte tőlük a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését."

[61] C434/16 sz. ügy Peter Nowak v. Data Protection Commissioner [2017] EU:C:2017:582, para 52.

[62] Lásd Finck (52. lj.) 75.

[63] Lásd Finck (52. lj.) 75.

[64] C-131/12. sz. ügy. Google Spain SL és Google Inc. kontra Agencia Española de Protección de Datos (AEPD) és Mario Costeja González, [2014], ECLI:EU:C:2014:317.

Igaz, a Google Spain ítélet még a GDPR bevezetése előtt született, azonban annak hatására jött létre a törlési jog egyenrangú alternatívájaként az ún. elfeledtetéshez való jog koncepciója. Ez a rendelet szövegében is visszaköszön, hisz maga a 17. cikk is egymás mellett, már-már szinonimaként utal a két kifejezésre. Nézzük meg, hogy vajon a blokkláncalapú adatkezelések tekintetében a kezelt adat és az ahhoz való hozzáférés megszakítása értelmezhető-e az elfeledtetéshez való jog gyakorlása szempontjából, és megoldást kínálhat-e a törléssel kapcsolatos problémára.

Mivel maguknak az adatoknak a szó szoros értelemben vett törlése (tehát hogy maga az adat tulajdonképpen nem létezik többé) nehezen egyeztethető össze a blokklánc-technológia alapvető ismérveivel, ezért az adathoz való hozzáférés ellehetetlenítése lehet inkább a gyakorlatban is alkalmazható megoldás. A CNIL már korábban hivatkozott blokklánc-iránymutatásában például az adathoz való hozzáférést biztosító privát kulcs törlését (elégetését) hozza mint lehetséges megoldást.[65] A privát kulcs törlésével az adat megmarad a blokkláncban, azonban az ahhoz való hozzáférési/olvashatósági lehetőség a dekódoláshoz való kulcs hiányában végérvényesen elveszik. A kapcsolat megteremtéséhez való lehetőség végleges törlése tehát az elfeledtetéshez való jog érvényesítését szolgálhatja a blokkláncon.

Ezzel egybevágó vélemények szerint a megfelelő technológiával titkosított olyan személyes adatok, amelyekhez senkinek sincs hozzáférése nem tartoznak többet a GDPR hatálya alá, kvázi elveszítik a rendelet által jelentett jogi garanciákra való érdemességüket.[66] A titkosítási technológia elavulása és a potenciális újbóli hozzáférés veszélye azonban véleményem szerint újraéleszti a jogi védelmet.

Egy másik lehetőség a szakirodalom által is már említett „felejtő" vagy „rövidített" blokkláncok koncepciójának kidolgozása. Egy ilyen alapon működő adatbázisban a hozzáférési kulcsokat tartalmazó blokkokat folyamatosan különböző hashek használatával újrakalibrálják egy bizonyos, előre meghatározott idő után, így a hozzáférési lehetőség is elveszik.[67] Ez tipikusan olyan célú adatkezeléseknél lehet jó megoldás, ahol az adatokat bizonyos idő után automatikusan törölni kellene.

Végül meg kell említeni a személyes adatok „láncon kívüli" („off-chain") tárolási lehetőségét, ahol 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. A láncon kívüli adatokból való törléssel az alap blokklánc nem változik, csak az azzal összekötött, személyes adatokat is tartalmazó ráépülő adatbázis. Ezzel a megoldással kiküszöbölhető a blokklánc megváltoztatásának nehézsége.[68]

[65] Lásd CNIL (36. lj.) 8–9.

[66] Kuan Hon W. et. al: „Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2", *Queen Mary School of Law Legal Studies Research Paper* No. 77. 2011, 18.

[67] Giuseppe Ateniese – Bernardo Magri – Daniele Venturi – Ewerton Andrade: „Redactable Blockchain or Rewrtinig History in Bitcoin and Friends" in *Proceeding of the 2nd IEEE European Symposium on Security and Privacy – EuroS&P* 2017, *eprint.iacr.org/2016/757.pdf.*

[68] Rosanna Mannan – Rahul Sethuram – Lauryn Younge: „GDPR and Blockchain: A Compliance Approach" *European Data Protection Law Review* 3/2019. 423–424.

5. A GDPR MEGFELELŐSÉG NEGYEDIK LÉPCSŐJE: ALAPELVEK ÉS TERVEZÉS

5.1. 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.[69]

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. Az integritás és bizalmas jelleg alapelvének való megfelelést már korábban bemutattuk (lásd a tanulmány 3. pontját).

A *célhoz kötöttség* alapelvét a GDPR úgy fogalmazza meg, hogy a személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon.[70] 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.[71] Az alapelv két további részelvből tevődik össze, nevezetesen először a cél meghatározásának kötelezettségéből és másodszor pedig az ezzel összefüggő felhasználás kötelezettségéből.[72] 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 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 menynyire egyeztethetők össze az eredeti adatkezelési céllal.[73] Egy blokkláncos adat-

[69] Lásd Péterfalvi–Révész–Buzás (32. lj.) 108.
[70] GDPR 5. cikk (1) bek. b) pont.
[71] 29-es Munkacsoport 3/2013-as véleménye a célhoz kötöttségről (WP203) 11.
[72] Lásd 29-es Munkacsoport (71. lj.) 3.
[73] Lásd Finck (52. lj.) 65.

kezelés 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 lásd pl. a tanulmány 4.3. pontját!). De olyan jogszabályi felhatalmazáson alapuló adatkezeléseknél, mint például az ingatlannyilvántartás vezetése[74] 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.[75] Az elv gyakorlatilag azt fogalmazza, 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.[76] 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) 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.[77] 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 adatkezelőnek törlési vagy rendszeres felülvizsgálati határidőket kell megállapítania.[78] A blokkláncalapú adatkezelések esetén az adatok eltávolításának lehetősége a protokoll működési sajátos-

[74] Juliet McMurren – Andrew Young – Stefaan Verhulst: „Adressing Transaction Costs Through Blockchain and Identity in Swedish Land Transfers" 2018. *blockchan.ge/blockchange-land-registry.pdf* .
[75] GDPR 5. cikk (1) bek. c) pont.
[76] Lásd Finck (52. lj.) 68.
[77] GDPR 5. cikk (1) bek. e) pont.
[78] GDPR (39) preambulumbekezdés.

ságai 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.[79] 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",[80] mint a törléssel majdhogynem egyenértékű intézkedésre, ezt pedig az elfeledtetéshez való jog kapcsán már ismertetett uniós bírósági gyakorlat, továbbá a jog létének elismerése a GDPR-ban csak megerősítette. Ezen felül a személyes adatok láncon kívüli tárolása esetén, az off-chain adatbázisból való végleges törlés is megoldást nyújthat a megfelelésre.

5.2. A BLOKKLÁNC MEGFELELTETÉSE A BEÉPÍTETT ÉS ALAPÉRTELMEZETT ADATVÉDELEM ELVÉNEK

A GDPR az adatkezelő és az adatfeldolgozó általános kötelezettségei között említi, hogy az adatvédelmi alapelveknek és a rendelet előírásainak való megfelelés, valamint az érintettek jogainak érvényesülése érdekében különböző garanciákat kell beépíteniük az adatkezelés folyamatába. Ezek a garanciák olyan megfelelő technikai és szervezési intézkedéseket kell hogy takarjanak, amelyek figyelembe veszik a tudomány és technológia mindenkori állását és a megvalósítás költségeit, továbbá az adatkezelés jellegét, hatókörét, körülményeit és céljait, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázatokat.[81] Az adatkezelőnek megfelelő technikai és szervezési intézkedéseket kell végrehajtania annak biztosítására, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek. Ez a kötelezettség vonatkozik a gyűjtött személyes adatok mennyiségére, kezelésük mértékére, tárolásuk időtartamára és hozzáférhetőségükre. Ezeknek az intézkedéseknek különösen azt kell biztosítaniuk, hogy a személyes adatok alapértelmezés szerint a természetes személy beavatkozása nélkül ne válhassanak hozzáférhetővé meghatározatlan számú személy számára.[82] A GDPR ezen előírásait nevezik a beépített és alapértelmezett adatvédelem elvének, melynek funkciója, hogy az adatkezelésre szolgáló rendszerek kialakítása során már alap-

[79] Lásd 29-es Munkacsoport (53. lj.) 3.
[80] Information Commissioner's Office: „Deleting Personal Data" 2014. február 26., 4., *ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf*.
[81] GDPR 25. cikk (1) bekezdés.
[82] GDPR 25. cikk (2) bekezdés.

értelmezetten figyelembe vegyék a rendeletnek való megfelelést mind a technikai, mind a szervezési intézkedések szintjén.

Az elvnek való megfelelés a blokkláncalapú személyes adatkezelés tekintetében is természetesen szükséges, így a fejlesztés során mindig alaposan át kell tekinteni, hogy milyen naprakész, a blokkláncra alkalmazható technika és szervezési megoldások érhetők el a piacon. Az adatkezelő kötelezettsége, hogy folyamatosan monitorozza például, hogy a rendszerben korszerű titkosítással biztosítják-e az adatkezelési műveleteket. Ha a céllal összeegyeztethető, úgy megfelelő anonimizálási technikákat használjon, vagy biztosíthassa az érintett tájékoztatásához vagy akár a felejtéshez való jogának hatékony gyakorlását. Ez természetesen nem egyszerű feladat, főleg egy ilyen rohamosan fejlődő területen. Ezért is szükséges lehet már jó előre felmérni, vajon mennyire indokolt és kivitelezhető a blokklánc használata, és arányos-e az általa jelentett kockázatokkal. Erre egy előzetesen elvégzett, a GDPR 35. cikke szerinti adatvédelmi hatásvizsgálat lefolytatása is jó eszközként szolgálhat.

6. ÖSSZEGZÉS: A MEGFELELŐSÉG VIZSGÁLATÁRA SZOLGÁLÓ ELMÉLETI RENDSZER ÉS ELV

Mint láttuk, a blokklánc-technológián alapuló adatkezelés megfeleltethetősége a GDPR előírásainak sok kérdést vet fel, a technológia újdonságából adódóan pedig kevés konkrét megoldás található adatkezelői oldalon. Az elmúlt időszakban jellemzőbb a technológia „tisztes távolságból való szemlélése", vagy az azzal való kísérletezgetés. Jobban áttekintve az eddigi idevágó irodalmat és cikkeket, számos olyan konkrét fejlesztés képe bontakozik ki előttünk, amelyek jó kiindulási pontot jelenthetnek az olyan adatkezelőknek, akik komolyan gondolják, hogy blokkláncalapú személyes adatkezelést kívánnak kifejleszteni és „élesben" is üzemeltetni. A tanulmány összegzéseként a következőkben ezeket foglalom össze, és kísérlem meg elméleti rendszerbe szervezni.

Kiindulópontként szeretném rögzíteni, hogy a blokkláncot olyan adatkezelési technológiaként azonosítottam, amely működési elveit figyelembe véve önmagában nem lehet alkalmas bármilyen típusú és célú adatkezelés végzésére. A blokklánc használatával kapcsolatban tehát elsősorban olyan adatkezelési célokat szükséges adatkezelői részéről azonosítani, amelyekkel összeegyeztethetőek a technológia sajátosságai. Az alábbi táblázatban a GDPR elemzett alapelveihez és előírásaihoz kísérlek meg hozzárendelni egy-egy azonosított módszert mint a megfelelés kapuját.

A megfelelést előíró jogszabályhely	A felvetett probléma	Lehetséges megoldásokat kínáló elvek és technológiák
Célhoz kötött adatkezelés alapelve[83] GDPR 5. cikk (1) bekezdés b) pontja	A blokklánc a kezelt adatokat és a velük végzett műveletek naplóit időkorlát nélkül tárolja.	Olyan cél meghatározása, amely megfeleltethető a technológia e sajátosságának (pl. egyes állami nyilvántartások)[84] „Felejtő" blokklánc[85] Hozzáféréshez szükséges privát kulcsok elégetése[86] Off-chain adattárolás[87]
Adattakarékosság alapelve[88] GDPR 5. cikk (1) bekezdés c) pontja	A blokklánc a kezelt adatokat és a velük végzett műveletek naplóit időkorlát nélkül tárolja. Valamennyi csomópont eltárolja a teljes adatbázis másolatát önellenőrzési célból.	„Felejtő" blokklánc Hozzáféréshez szükséges privát kulcsok elégetése Off-chain adattárolás Blokkrácsalapú adatkezelés[89]
Korlátozott tárolhatóság alapelve[90] GDPR 5. cikk (1) bekezdés e) pontja	Valamennyi csomópont eltárolja a teljes adatbázis másolatát önellenőrzési célból. A korábban még aktuális adatok tárolása akkor is megvalósul, ha már elavultak, vagy azokra nincs szükség.	„Felejtő" blokklánc Hozzáféréshez szükséges privát kulcsok elégetése Off-chain adattárolás
Integritás és bizalmas jelleg alapelve, az adatkezelés biztonsága[91] GDPR 5. cikk (1) bekezdés f) pontja és 32. cikke	Az adatokkal végzett műveletek nyilvánosan hozzáférhetőek valamennyi résztvevő számára. Az alkalmazott titkosítás elavulhat és az adatok hozzáférhetővé válhatnak a privát kulcs elégetése után is.	Publikus helyett privát blokklánc üzemeltetés[92] Off-chain adattárolás Blokkrácsalapú adatkezelés Naprakész titkosítás használata és annak felülvizsgálata[93]
Az érintett hozzáférési joga[94] GDPR 15. cikke	A csomópontok közös adatkezelőnek minősülhetnek (pl. az adatkezelést szabályozó szerződés alapján), az adatokhoz azonban nem férhetnek hozzá valamennyien. Az érintett jogosult viszont bármelyiknél előterjeszteni a hozzáférési kérelmét.	Hatékony belső eljárásrend kialakítása az adatkezelők között az érintetti kérelmek kezelése szempontjából[95]

[83] Lásd erről bővebben a tanulmány 5.1. pontjában foglaltakat.
[84] Lásd erről bővebben a tanulmány 5.1. pontjában foglaltakat.
[85] Lásd erről bővebben a tanulmány 4.3. pontjában foglaltakat.
[86] Lásd erről bővebben a tanulmány 4.3. pontjában foglaltakat.
[87] Lásd erről bővebben a tanulmány 4.3. és 5.1. pontjaiban foglaltakat.
[88] Lásd erről bővebben a tanulmány 5.1. pontjában foglaltakat.
[89] Lásd erről bővebben a tanulmány 1.5. pontjában foglaltakat.
[90] Lásd erről bővebben a tanulmány 5.1. pontjában foglaltakat.
[91] Lásd erről bővebben a tanulmány 3.1.–3.2. pontjaiban foglaltakat.
[92] Lásd erről bővebben a tanulmány 1.3. és 4.2. pontjaiban foglaltakat.
[93] Lásd erről bővebben a tanulmány 3.2. pontjában foglaltakat.
[94] Lásd erről bővebben a tanulmány 4.1. pontjában foglaltakat.
[95] Lásd erről bővebben a tanulmány 4.1. pontjában foglaltakat.

A megfelelést előíró jogszabályhely	A felvetett probléma	Lehetséges megoldásokat kínáló elvek és technológiák
A helyesbítéshez való jog[96] GDPR 16. cikke	A blokkláncban nem lehet adatokat módosítani, csak újabbakat hozzáfűzni. Az elavult adatokat időkorlát nélkül kezelik az újabb, frissített adatállomány mellett.	Olyan adatkezelési cél meghatározása, amellyel összeegyeztethető az adatok kiegészítése, azok tényleges helyesbítése helyett (pl. egyes állami nyilvántartások)[97] Privát blokklánc esetén az adatot tartalmazó blokk újrahashelése[98] Off-chain adattárolás
A törléshez („elfeledtetéshez") való jog[99] GDPR 17. cikke	A blokkláncból nem lehet adatokat törölni, csak a hozzáférést korlátozni.	Hozzáféréshez szükséges privát kulcsok elégetése Naprakész titkosítás használata az „elfelejtett adatokhoz" való hozzáférés kizárása érdekében[100] Off-chain adattárolás „Felejtő" blokklánc
A beépített és alapértelmezett adatvédelem elve[101] GDPR 25. cikk	Egy publikus blokkláncban az adatok (akár pszeudonim formában) bárki számára hozzáférhetők. A blokklánc-technológia gyorsan fejlődik, új innovatív megoldások merülhetnek fel a piacon az adatvédelem garantálására.	Publikus helyett privát blokklánc üzemeltetés Periodikusan át kell tekinteni, hogy milyen naprakész, a blokkláncra alkalmazható technika és szervezési megoldások érhetők el a piacon.[102]

A fentiekben összefoglaltam az egyes, a tanulmányban kiemelt problémák megoldására jelenleg is alkalmazható elveket és technológiákat. Természetesen a technológia fejlődése révén újabb adatvédelmet elősegítő megoldások láthatnak napvilágot, illetve korábbiak avulhatnak el. Ezért is fontos az adatkezelő részéről a fejlesztések nyomon követése és az alkalmazott módszerek frissítése.

A konkrét megoldásokat áttekintve, visszatérve a tanulmány elején felvetett gondolatmenetre, egy általánosabb elvet is szeretnék felállítani a blokkláncon alapuló személyes adatkezelések kapcsán. Mint látjuk, a blokk mint adattárolási egység bármilyen (digitalizálható) személyes adatot, információt tartalmazhat a lánchoz való hozzáadásának pillanatában. A kezelt adat, információ jellegének csak a meghatározott cél szabhat határt.

[96] Lásd erről bővebben a tanulmány 4.2. pontjában foglaltakat.
[97] Lásd erről bővebben a tanulmány 4.2. pontjában foglaltakat.
[98] Lásd erről bővebben a tanulmány 4.2. pontjában foglaltakat.
[99] Lásd erről bővebben a tanulmány 4.3. pontjában foglaltakat.
[100] Lásd erről bővebben a tanulmány 3.2. pontjában foglaltakat.
[101] Lásd erről bővebben a tanulmány 5.2. pontjában foglaltakat.
[102] Lásd erről bővebben a tanulmány 5.2. pontjában foglaltakat.

A blokkláncban végzett adatkezelés működési elveinek kialakítása azonban már jóval az adatok hozzáadása előtt elkezdődik. Az adatkezelő és az adatfeldolgozó feladata, hogy már a működés kialakítása során figyelemmel kísérje az adatvédelmi megfelelést.

Az adatvédelmi megfelelés pedig visszaköszön a már éles rendszer működésében, hiszen a blokklánc az adatok és a velük végzett műveletek tárolása során egyfajta lenyomatként szolgál. Az adatokkal végzett műveletek kitörölhetetlen lenyomata jelenti azokat a mintázatokat, amelyek vizsgálata kapcsán megállapítható az adatvédelmi jognak történő megfelelés. Hangsúlyozom, hogy ezek a mintázatok a blokklánc valamennyi, a csomópontok által kezelt kópiákban rendelkezésre állnak, ezért azokat „kollektív adatkezelési mintázatoknak" tekinthetjük. A mintázatok lenyomata pedig akkor is rendelkezésre áll, ha egyébként maguknak a személyes adatoknak a kezelése egy elkülönült adatbázisban, off-chain megoldásokat alkalmazva történik.

A blokkláncalapú adatkezelést az emberi elméhez hasonlítva azt mondhatjuk, hogy az egyes, konkrét személyes adatokat tároló csomópontok jelenthetik az egyén tudata által tárolt információkat. Az adatkezelés közös, kollektív mintázatainak megléte valamennyi csomópont részéről pedig az ember biológiai és társadalmi fejlődése során kialakult közös viselkedésmintákat. Egy elsőre távolinak tűnő hasonlattal élve: a pszichoanalitikus iskola képviselői közül Carl Gustav Jung mutatott rá az emberi szellemtörténetben bizonyos archetipikus képek, metaforák azonosságára és ismétlődésére az egyes kultúrákban, amelyeket az emberiség „kollektív tudattalanjának" részeiként jellemez, és amelyek az egyéni gondolkodás- és viselkedésmintákban is visszaköszönhetnek.[103]

A blokk így önmagában valóban „tabula rasa" annak megszületése pillanatában, azonban abban csak az adatkezelő által megtervezett kollektív adatkezelési mintázatok alapján történhet a tényleges adatkezelés. Ez a tervezési folyamat pedig – a beépített és alapértelmezett adatvédelem elve alapján is – csak a vonatkozó jogszabályok tiszteletben tartásával történhet. Ezen követelményt neveztem el a kollektív adatkezelési mintázatok elvének. Az absztrakt, jogi megfelelőséget garantáló mintázatoknak az első blokk létrejöttekor kell leképeződniük, hogy utána a lánc épülésével továbbterjedjenek az adatbázis épülésével valamennyi blokkban és a blokklánc valamennyi kópiájában. Talán nem véletlenül nevezik a blokkláncalapú rendszerekben az első blokkot „genezis-blokknak", hiszen ez teremti meg a rendszer működésének alapjait.

A tanulmány zárásaként szeretném hangsúlyozni, hogy ezen követelményrendszer felállítására a jelenlegi technikai fejlettséget mutató, általam ismert szinten került sor. A jövőbeni fejlődés irányait tekintve – további kutatások alapjául szolgálva – sor kerülhet akár az itt lefektetett kijelentések felülvizsgálatára, kiegészítésére is.

[103] C. G. Jung: *Az archetípusok és a kollektív tudattalan* (Budapest: Scolar Kiadó 2017).