

MOLNÁR DÁVID\*

# A JELENT ÉS A JÖVŐT ÖSSZEKÖTŐ LÁNC: A BLOKKLÁNC-TECHNOLÓGIA ÉS AZ ADATVÉDELEM ÖSSZEHANGOLÁSA A GDPR TÜKRÉBEN

## 1. Bevezetés

A blokklánc-technológia – a kriptográfiai hitelesítést, a konszenzusos validációt és az elosztott adattárolást egyesítő infrastruktúra – olyan normatív provokációval szembesíti az adatvédelmi jogot, amely a digitalizáció korábbi hullámaiban nem jelent meg ilyen nyers formában. A technológia strukturális önleírása – a megváltoztathatatlan és az átláthatóság – első ránézésre ellentétben áll a személyes adatokhoz fűződő szubjektív jogosultságokkal, különösen a törlés (az „elfeledtetéshez való jog”) és a helyesbítés igényével.<sup>1</sup> Ugyanakkor e feszültség nem szükségképpen antagonisztikus: a blokklánc ígérete – a manipulációrezisztens, auditálható, időpecsételés nyilvántartás – éppen a személyes adatok védelmének és az elszámoltathatóság elvének szolgálatába állítható, ha a jogi és technikai konstrukciók kölcsönösen reflektálnak egymás korlátaira.<sup>2</sup> A tanulmány ennek a dialektikának a kifejtésére vállalkozik: diagnosztizálja a fő ütközési pontokat, bemutatja a gyakorlati tanulságokkal szolgáló esetelemeket, és olyan megoldásrendszert vázol, amely a GDPR teleológiájához illeszkedő módon teszi kompatibilisé a blokkláncot az európai adatvédelmi renddel.

A módszertani kiindulópont kettős. Egyrészt a jogdogmatikai elemzés szintjén vizsgáljuk a GDPR fogalmi apparátusának (személyes adat, adatkezelő, adatfeldolgozó, közös adatkezelés, adattakarékosság, elszámoltathatóság) alkalmazhatóságát a decentralizált architektúrákban. Másrészt a technológiai realitások felől közelítünk: mit jelent „törölni” egy megváltoztathatatlan főkönyvben, milyen műszaki eszközök alkalmasak az érintetti jogok gyakorlati érvényesítésére, és milyen kormányzási mechanizmusok képesek a felelősséget a tényleges befolyás szerint allokálni.

## 2. A megváltoztathatatlan és az „elfeledtetéshez való jog” doktrinális konfliktusa

A blokklánc megkülönböztető jegye az a belső integritási konstrukció, amely hash-láncolásra és – tipikusan Merkle-fákra épülő – kompozit ellenőrző összegekre támaszkodik.<sup>3</sup> A hálózati csomópontok a konszenzusos protokoll (proof-of-work, proof-of-stake vagy egyéb bizánci hibatűrő mechanizmus) révén egyetértésre jutnak a következő állapotról;<sup>4</sup> a már lerögzített blokkok módosítása csak a teljesített számítási/érvényesítési ráfordítás „visszatekerésével”, a valóságban praktikus lehetetlen költséggel érhető el.<sup>5</sup> E technikai megváltoztathatatlan azonban nem azonos a jog által elvárt adattörléssel: a GDPR a személyes adat és az érintett közötti érdemi kapcsolat megszüntetését, a hozzáférés és a feldolgozhatóság megszűnését követeli meg,<sup>6</sup> nem pedig az adat fizikai megsemmisítést.

Ez az elmozdulás – a fizikai törléstől a hozzáférhetetlenné tétel, azaz a funkcionális törlés irányába – teremti meg a kompromisszum lehetőségét. Ha a törlés normatív célját úgy értjük, mint az érintett irányuló kockázat végleges lezárását, akkor az a technikai megoldás, amely a személyes adathoz való hozzáférést a gyakorlatban helyreállíthatatlanul megszünteti, a törlés érdemi követelményét teljesítheti. E gondolati keretben értelmezhető újra a kriptográfiai törlés: amennyiben az adat láncban titkosított formában található, és a dekódoláshoz szükséges kulcsok véglegesen és ellenőrizhetően

megsemmisülnek, a személyes adat az érintett szempontjából megszűnik.<sup>7</sup> A megfelelés kulcsa itt nem a blokk szintű rescriptio, hanem a kulcskezelés kormányzása: többkulcsos (threshold) megoldások, küszöbalapú aláírások, kulcsrotáció és visszavonási protokollok együttese teremti meg a funkcionális törlés bizonyítható feltételrendszerét.<sup>8</sup>

A láncon kívüli tárolás ettől eltérő, ám nem kevésbé releváns kompromisszum. Az off-chain modellben a személyes adat a hagyományos – de megerősített – infrastruktúrában marad, a blokklánc csupán a változatlan integritást garantáló lenyomatot (hash) és időpecsétet őrzi.<sup>9</sup> A törlés ebben a modellben a primer tárhelyen megy végbe; a hash önmagában – a forrásadat visszaállíthatósága híján – értelmezhetetlenné válik. E megoldás előnye a törlések (és helyesbítések) operatív kezelhetősége, ára viszont a decentralizációs ethosz részleges feladása és a centralizált réteg klasszikus kitérési mechanizmusainak visszatérése.<sup>10</sup> A mérlegelés tehát nem bináris: a jog által védett érdekek – az érintetti önrendelkezés – és a technológia által védett érdekek – a globális integritás – közötti optimumot a felhasználási kontextus, a kockázati profil és a költség-hatás elemzés együttese határozza meg.

Mindkét modell kiegészíthető az adatvédelmet erősítő kriptográfiával. A zéró-tudás bizonyítások és a szelektív közzétételi protokollok azt teszik lehetővé, hogy a hálózat szereplői bizonyos állítások (például életkörülmények teljesítése, jogosultság fennállása) igazságát ellenőrizhessék a mögöttes személyes adatok megismerése nélkül.<sup>11</sup> A tranzakciók érvényessége ellenőrizhető marad, miközben a személyes adatok on-chain lábnyoma minimálisra zsugorodik; ez a célhoz kötöttség és adattakarékosság elvének technológiai implementációja.

A doktrinális konfliktus gyakorlati metszeteire plasztikus példákat adnak a blokkláncalapú közigazgatási nyilvántartási kísérletek (például ingatlan-nyilvántartás), ahol a történeti adatok megőrzése a közbizalom előfeltétele, és a blokklánc erre kivételesen alkalmas.<sup>12</sup> Ha azonban a nyilvánosságtól és megváltoztathatatlanágtól elválaszthatatlan bejegyzések személyes adatot is tartalmaznak, a törlési kérelmekkel való összeütközés elkerülhetetlen. A megoldás ilyenkor a személyes adatok kivitele a megváltoztathatatlan rétegből, és a blokklánc mint hitelesítés- és időpecsét-infrastruktúra használata; ellenkező esetben a rendszer vagy jogsértő, vagy működésképtelen lesz.

## 3. Adatkezelői minőség, decentralizált kormányzás és a felelősség rétegzett allokációja

A GDPR fogalmi rendszere az adatkezelő és az adatfeldolgozó közötti különbségtételre épül, amely a cél- és eszközmeghatározás szerinti felelősségtelepítést feltételezi. A nyilvános blokkláncokban azonban a „cél” és „eszköz” meghatározása kollektív, folyamatos és többközpontú cselekvés eredménye.<sup>13</sup> A protokollfejlesztők a kódot írják és módosítják; a validátorok/bányászok a hálózat biztonságát és az érvényesítés rendjét biztosítják; a csomópont-üzemeltetők infrastruktúrát szolgáltatnak; a dappszolgáltatók a felhasználói interfészen keresztül végső soron meghatározzák, hogy milyen adatok kerülnek a láncra; a felhasználók pedig tranzakcióikkal alakítják a rendszer adatfolyamát.<sup>14</sup> Ilyen környezetben az „adatkezelői minőség” doktrinális keresése csak akkor nem válik öncélú formalizmussá, ha a felelősség teleológiáját – azaz a vé-

\* Jogász hallgató (PTE ÁJK). A 37. OTDK-n a tanulmány különdíjat kapott az infokommunikációs jogi tagozatban.

delem célját – tekintjük rendező elvnek: azt a szereplőt kell felelősségi pozícióba állítani, aki ténylegesen és érdemben képes a személyes adatok sorsára hatni.

Engedélyezett blokkláncokban a konzorciumi megállapodás e logika szerint artikulálható: a tagok közötti adatkezelői és adatfeldolgozó szerepek, az érintetti kérelmek csatornái, a tárolási idők és törlési mechanizmusok, a kulcskezelési és auditálási rend részleteiben rögzíthetők.<sup>15</sup> Nyilvános hálózatokban a dappszoftalkáló – mint a felhasználói adatforgalom elsődleges kapuőre – tipikusan olyan pozícióban van, amelyben célokat és eszközöket határoz meg; felelőssége ezért nem kerülhető meg azzal, hogy „a lánc decentralizált”.<sup>16</sup> A protokollszintű szereplők számára – különösen, ha intézményesültek (alapítványok, testületek) – átláthatósági, kockázatkezelési és incidenskoordinációs kötelezettségek írhatók elő anélkül, hogy ezzel automatikusan adatkezelővé válnának.<sup>17</sup> A csomópont-üzemeltetők és validátorok esetében a gondossági kötelezettségek (például biztonsági frissítések, jogellenes tartalom terjesztésének tudatos facilitatívja elleni fellépés) differenciáltan írhatók elő a tényleges befolyás mértéke szerint.

A pszeudoanonimitás doktrinálisan vegyes képet mutat. A kriptocím mint önálló adat nem szükségképpen személyes adat; azonban, ha a címhez utólag azonosító adatok (például tőzsdei ügyfél-azonosítás) kapcsolódnak, vagy hálózati viselkedésmintázatokról reidentifikáció lehetséges, a cím és a tranzakciós történet személyes adattá válik.<sup>18</sup> Ez azt jelenti, hogy a megfelelés nem szorítható a „ne tárolj on-chain személyes adatot” trivialisára: a tervezésnél az adatminimalizálás és a célhoz kötöttség elvének technikai implementációjára (például determinisztikus naplózás helyett kriptográfiai igazolások alkalmazása) van szükség.

#### 4. Decentralizáció és szuverenitás: joghatóság, végrehajthatóság, jogpolitikai opciók

A blokklánc transzjurisdikcionális működése a klasszikus szuverenitásdoktrína alapjait feszegeti. A GDPR extraterritoriális hatálya – amelyet a szolgáltatásnyújtás irányultsága és az érintett Unióban való tartózkodása határoz meg – elvben biztosítja a védelem kiterjesztését, ám a nyilvános blokkláncok esetében a címzettek azonosítása és a szankciók végrehajtása gyakran illuzórikus. A decentralizált infrastruktúrában a felelősség címzettje sokszor nem jogalany, hanem kódszintű entitás; így a klasszikus állami végrehajtási eszközök – pénzbírság, eltiltás, kötelezés – jogilag hatástalanok, ha nincs kikényszeríthető címzett.<sup>19</sup> A technológia kriminalizálása ezért nemcsak kontraproduktív, hanem dogmatikailag is tarthatatlan: a válasz nem a tiltás, hanem a kockázatalapú, arányos és célzott szabályozás.

A belső jogi dimenzióban indokolt a blokkláncszolgáltatások minimális adatvédelmi és információbiztonsági követelményeinek kodifikálása. Ezek közé tartozik a kulcskezelési és hozzáférés-szabályozási protokollok, incidenskezelési rendek, törlési és helyesbítési eljárások, valamint az adatvédelmi hatásvizsgálat (DPIA) kötelező tartalmi minimumának rögzítése.<sup>20</sup> Az ilyen előírások nem korlátozóak, hanem felelőssé tehetik a decentralizációt. Intézményi szinten pedig szükséges a felügyeleti hatóságok – adatvédelmi, pénzügyi, versenyjogi – koordinált együttműködése, valamint az innovációt és megfelelést integráló *sandbox*-típusú kísérleti engedélyezés.

A nemzetközi dimenzióban a decentralizált rendszerek ellenőrzése nem valósítható meg pusztán nemzeti jogi eszközökkel. A határon átnyúló információcsere, közös vizsgálati csoportok, harmonizált eljárási protokollok és bizonyítási csatornák képezik azt az együttműködési infrastruktúrát, amely nélkül a joghatósági normák deklarativává válnak.<sup>21</sup> A reális jogpolitikai cél nem a centralizáció kikényszerítése, hanem a felelősségi réseket lezáró, többszintű kormányzási modell kiépítése, amelyben az állami, iparági és technológiai normák koherens policentrikus struktúrában működnek. A szuverenitás ebben a rendszerben nem tűnik el, hanem adaptív, hálózati jellegűt, amely a decentralizáció realitásait integrálja a jogrendbe.

#### 5. GDPR-kompatibilis architektúra: technológiai és kormányzási integráció

A megfelelés nem egyetlen varázsszék, hanem egymásra rétegzett, egymást komplementer módon erősítő megoldások összjátéka. A hibrid tárolási modell kiindulópontja változatlan: a láncon kívüli réteg kezeli a személyes adatokat olyan környezetben, ahol a törlés, helyesbítés, hozzáférés-biztosítás és adathordozhatóság ténylegesen operacionalizálható, míg a láncon belüli komponens az integritáshorgony, az időpecsételés bizonyítást és az auditálhatóság infrastruktúráját adja.<sup>22</sup>

Ezt a szerkezetet kriptográfiai törléssel lehet megerősíteni. A kulcsmegsemmisítés – ha bizonyíthatóan végleges és visszafordíthatatlan – a törlés funkcionális követelményét teljesíti anélkül, hogy a főkönyv megváltoztathatatlanúságát megtörné.<sup>23</sup> A zéró tudás bizonyítások és a szelektív közzétételi protokollok, szükség esetén ellenőrizhető hitelesítési adatokkal és attribútumalapú jogosultságkezeléssel kombinálva, lehetővé teszik a jogosultságigazolás és a hozzáféréskontroll megvalósítását a személyes adatok on-chain kitettsége nélkül.<sup>24</sup> A többpárti számítás és a részben homomorf titkosítás a feldolgozás során is fenntarthatja a titkosságot.

A sidechaine és a rétegzett (L2) architektúrák dedikált „privát zónát” teremtenek a személyesadat-intenzív műveleteknek – például érintetti joggyakorlás, kulcs-governance, jogosultságkezelés –, miközben a fő lánc változatlanul a megmászhatatlan ellenőrző és vita-rendezési referenciareteg. A kormányzás oldalán a szerep- és felelősségallokáció írásban rögzített, pontos rendje a kulcs: konzorciumi környezetben szerződésben kell tipizálni az adatkezelői és adatfeldolgozó minőséget, az érintetti kérelmek határidőit és folyamatait, az adathordozhatóság és a rendszerelhagyás protokollját, a naplózás és audit kötelező elemeit, valamint a kár- és felelősség-megosztás szabályait.<sup>25</sup>

Nyilvános hálózatokban a dappszoftalkáló és az interfészüzemeltetők számára magatartási kódexek és tanúsítási sémák rajzolhatnak ki előre verifikálható megfelelési útvonalat. Az adatáramlási térkép, a kulcs-governance policy, a reidentifikációs kockázateszt, az incidenskezelési „játékkönyv” és a DPIA-minták együttese a *privacy by design* elv tényleges operacionalizálását szolgálja.<sup>26</sup>

A mérhetőség horizontális követelménye az egész ökoszisztémát áthatja. A törlési kérelmek végrehajtását visszaigazoló bizonylatok, a kulcsmegsemmisítés kriptográfiai igazolásai, a zéró tudás állítások formális helyességi tanúsításai, az off-chain táruk auditnaplói és a hozzáféréslógok integrált összekapcsolása adja az elszámoltathatóság bizonyítási anyagát. Enélkül a megfelelés deklarativ marad, a jogérvényesítés pedig a bizonyíthatóság hiányán meghiúsul. A gyakorlatban mindez *privacy engineering* folyamatba ágyazható: kockázatalapú tervezés, kontrollkiválasztás, implementáció, assurance case-ek összeállítása, majd folyamatos megfeleléstelemtéria és atesztáció. A megfelelés így nem statikus állapot, hanem fenntartott, auditálható üzemenet.

#### 6. De lege ferenda: a funkcionális törlés kodifikációja és a decentralizált fogalmi készlet bevezetése

A jelenlegi jogi állapot legfőbb kockázata a dogmatikai bizonytalanság. Amíg a törlés kizárólag fizikai megsemmisítésként gondolható el, addig a megváltoztathatatlan főkönyvvel való ütközés szükségképpen. Normatív megoldásként indokolt a törlés alternatív formáinak – mindenekelőtt a visszavonhatatlan pszeudonimizálásnak és a kulcsmegsemmisítésen alapuló kriptográfiai törlésnek – kifejezett elismerése, szigorú garanciarendszerhez kötve.

A garanciák minimális magja: többkulcsos, küszöbalapú kulcskezelés; a kulcsok teljes életciklusának – generálás, rotáció, archiválás, megsemmisítés – kötelező dokumentálása és auditálhatósága; a megsemmisítés kriptográfiai bizonyíthatósága és vissza nem fordíthatósága; akkreditált, harmadik feles ellenőrzés lehetősége; valamint incidensekre és visszaélésekre előre kidolgozott reakciós játékkönyv.<sup>27</sup> E garanciák együttesen teremtik meg azt a bizonyítást

rendet, amelyben a funkcionális törlés nem fikció, hanem ellenőrizhető és számon kérhető gyakorlat.

Fogalmi oldalon célszerű egy decentralizált környezetre szabott kategóriarendszer bevezetése. A „decentralizált adatkezelő” címke azon szereplőkre alkalmazható, akik ténylegesen meghatározzák a személyes adatok sorsát, még ha nem klasszikus szervezeti struktúrában is. A „hálózati résztvevő” státusz azokra a validátorokra és üzemeltetőkre vonatkozhat, akik a rendszer integritásához hozzájárulnak, ezért objektív gondossági és együttműködési kötelezettségekkel tartoznak.<sup>28</sup> A kártérítési felelősségben a kollektív, de differenciált modell – az okozati hozzájárulás és a tényleges befolyás arányában – igazságosabb és végrehajthatóbb, mint a formalista, mindenre kiterjedő egyetemlegesség.<sup>29</sup>

Elodázhatatlan a DPIA-kötelezettség blockchainspecifikus konkretizálása is. Felügyeleti szinten szükségesek a tartalmi minimumlisták és minták, amelyek az adatáramlási térképet, a kulcs-governance követelményeket, a reidentifikációs kockázatértékelést, a híd- és orákulumkomponensek elemzését és az érintetti joggyakorlás csatornáit standardizálják.<sup>30</sup> A magatartási kódexek és tanúsítási mechanizmusok, piaci ösztönzőkkel párosítva, a megfelelést reputációs és üzleti előnnyé konvertálják.

A szuverenitási dimenzióban a belső jogi kapacitások megerősítése mellett megállapodásalapú nemzetközi végrehajtási infrastruktúrára van szükség. Idetartozik az információcsere, a közös vizsgálati mechanizmusok, a harmonizált eljárási protokollok és a bizonyítási csatornák.<sup>31</sup> A decentralizált protokollok érdemi ellenőrzésének realitása csak így teremthető meg; enélkül a szabályozás könnyen megkerülhető, deklaratív normák szintjén ragad. A javasolt kodifikáció lényege tehát kettős: a funkcionális törlés elismeré-

se és bizonyítási rendje, valamint a decentralizált szereplőkre szabott, felelősségtranszparens fogalmi apparátus beemelése. E kettő együtt képes a blokklánc innovációs ígérteit a GDPR teleológiájával fenntartható módon összeegyeztetni.

## 7. Záró következtetések

A blokklánc és a GDPR közötti viszony nem zéró összegű játszma. A technológia – ha nem dogmatikus elfogultsággal szemléljük – az adatvédelem számos célkitűzését erősítheti: a változtathatatlan időpecsétek és az auditálhatóság az elszámoltathatóságot, a zérótudás-bizonyítások és a szelektív közzététel az adattakarékosságot, a kulcsmegsemmisítés a funkcionális törlést szolgálja.<sup>32</sup> A jog – ha a teleológiájához hű – nem kényszerít lehetetlenséget, hanem a kockázatot csökkentő és igazolható megoldásokat jutalmazza. E tanulmány mellett érvelt, hogy a két világ közötti híd kiépíthető: a funkcionális törlés doktrínájának elismerése, a decentralizált szereplőkre szabott fogalmi készlet és a kockázatalapú, mérhető megfelelés együttesen képesek a blokklánc innovációs ígérteit és az adatvédelmi jog alkotmányos ígérteit összeegyeztetni.

A „jelen és jövőt összekötő lánc” metaforája nem retorikai fogás, hanem jogpolitikai program: a technológia és a jog kölcsönös adaptációja révén a személyes adatok védelme nem kerül a digitális modernizációval szembe, hanem annak feltételévé válik. A siker feltétele a dogmatikai tisztánlátás, a technikai részletek megértése és az intézményi együttműködés. Ha ez a triász együtt érvényesül, a blokklánc nem az adatvédelem ellenfele, hanem annak – helyesen megkonstruált – infrastrukturális szövetségese lesz.

## Jegyzetek

- PILKINGTON, M.: *Blockchain Technology: Principles and Applications*. In: *Research Handbook on Digital Transformations*. Edward Elgar, London, 2016. 253.
- CASINO, Fran – DASAKLIS, Thomas K. – PATSAKIS, Constantinos: *A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues*. *Telematics and Informatics* 2019/3. 55.
- Смирнов, А. В.: *Прозрачность и децентрализация в блокчейне: технические и социальные аспекты*. *Журнал цифровых технологий и систем* 2022/3. 57.
- MUNARRREM, Tuncay Gencoglu: *Mathematical Analysis of the Hash Functions as Cryptographic Tools for Blockchain*. *Firat University Turkish Journal of Science & Technology*, 17 (2022)/2. 192.
- SHARMA, Dhramandra – SAXENA, Monika: *Different Cryptographic Hash Functions for Security in the Blockchain*. *Proceedings of the International Conference on Data Science and Network Security (ICDSNS)*, 2023. July. 4.
- European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L119, 1-88. (Továbbiakban GDPR) Section 3, Article 17 1.) a)-d).
- LIU, Chen – AGHAEI KHOUZANI, Hoda – YANG, Chengmo: *ErasuCrypto: A Light-weight Secure Data Deletion Scheme for Solid State Drives*. 2017. vol. 1. 132.
- TYAGI, Shobha: *A Review on Zero Knowledge Proof Vulnerabilities in Zcash*. *Proceedings of the International Conference on Advances in Computation, Communication and Information Technology (ICAICIT)*, November 2023. 877.
- GODYN, Mateusz – KEDZIORA, Michal – REN, Yingying – LIU, Yongxin – SONG, Houbing Herbert: *Analysis of Solutions for a Blockchain Compliance with GDPR*. *Scientific Reports* 2022/9. vol. 12. no. 1. 15021.
- SHEN, Charlie: *Blockchain Immutability: A Double-Edged Sword in Compliance with GDPR's Right to Erasure*. *Journal of Technology Law & Policy*, 2019. vol. 22. no. 1. 45.

- KÜHLING, Jürgen – MARTINI, Mario: *Blockchain und die Datenschutz-Grundverordnung: Die Konfrontation zwischen Technik und Datenschutzrecht*. *Juristenzeitung (JZ)* 2022. vol. 74. no. 5. 239.
- Lantmäteriet (The Swedish Mapping, Cadastre and Land Registration Authority) – Telia Company – ChromaWay – Kairos Future: *The Land Registry in the Blockchain*. July 2016. [https://ica-it.org/pdf/Blockchain\\_Landregistry\\_Report.pdf](https://ica-it.org/pdf/Blockchain_Landregistry_Report.pdf) [2025.10.10].
- Шишкин, А. А.: *Блокчейн и GDPR: проблемы защиты данных и перспективные регулирования*. *Право и экономика* 2020/6. 86.
- CASINO, Fran – DASAKLIS, Thomas K. – PATSAKIS, Constantinos: *A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues*. *Telematics and Informatics*, 2019/3. vol. 36. 55.
- SRINIVASAN, S.: *Privacy Protection and Data Breaches*. *Proceedings of Informing Science & IT Education Conference (InSITE)* 2015. 444.
- YANG, Xiao – ZHANG, Ning – LOU, Wenjing – HOU, Y. Thomas: *A Survey of Distributed Consensus Protocols for Blockchain Networks*. *IEEE Communications Surveys and Tutorials*, 2020. vol. 22. no. 2. 1465.
- YI, Sun – SHAO, Ying: *Research on Data Security Communication Scheme of Heterogeneous Swarm Robotics System in Emergency Scenarios*. *Sensors* 2022/8. vol. 22. no. 16. 6082.
- АВНИ, А. I. – SHIN, S. Y.: *BUS: A Blockchain-Enabled Data Acquisition Scheme with the Assistance of UAV Swarm in Internet of Things*. *IEEE Access*. 2019. vol. 7. 103231.
- YI, Sun – SHAO, Ying: *Research on Data Security Communication Scheme of Heterogeneous Swarm Robotics System in Emergency Scenarios*. *Sensors*, 2022/8. vol. 22. no. 16. 6082.
- PINNA, Andrea – IBA, Simone: *Sidechains for GDPR-Compliant Data Protection in Blockchain Ecosystems*. *Journal of Cybersecurity and Privacy*, 2021. vol. 2. no. 3. 225.
- Сидоров, Е. А. – Руднев, И. П.: *Шифрование и защита данных в условиях российского законода-*

- тельства о персональных данных. *Труды Института системного анализа РАН*, 2022/2. 112.
- BOLESCH, Lara – MITSCHKE, Andreas: *Revolution oder Evolution? Funktionsweise, Herausforderungen und Potenziale der Blockchain-Technologie*. *Kreditwesen*, 2016. 1129.
- PILKINGTON, Marc: *Blockchain Technology: Principles and Applications*. In: *Research Handbook on Digital Transformations*. Edward Elgar Publishing, London, 2016. 253.
- PINNA, Andrea – IBA, Simone: *Sidechains for GDPR-Compliant Data Protection in Blockchain Ecosystems*. *Journal of Cybersecurity and Privacy*, 2021. vol. 2. no. 3. 240.
- LIU, Chen – AGHAEI KHOUZANI, Hoda – YANG, Chengmo: *ErasuCrypto: A Light-weight Secure Data Deletion Scheme for Solid State Drives*. 2017. vol. 1. 132.
- Сидоров, Е. А. – Руднев, И. П.: *Шифрование и защита данных в условиях российского законодательства о персональных данных*. *Труды Института системного анализа РАН*, 2022/2. 112.
- RIVA, R. – FANTI, A.: *Risk-Based Approach to Data Protection Impact Assessments for Blockchain Applications*. *Computer Law & Security Review*, 2020. vol. 38. 123.
- SHEN, Charlie: *Blockchain Immutability: A Double-Edged Sword in Compliance with GDPR's Right to Erasure*. *Journal of Technology Law & Policy*, 2019. vol. 22. no. 1. 45.
- Rademacher, Thomas: *Die DSGVO und Blockchain-Technologien: Herausforderungen und Lösungsansätze im europäischen Datenschutzrecht*. *Zeitschrift für europäisches Privatrecht*, 2021. vol. 30. no. 1. 58.
- KASPER, Gabriel: *People Analytics in Privatrechtlichen Arbeitsverhältnissen: Vorschläge zur wirksameren Durchsetzung des Datenschutzrechts*. Dike Verlag & Nomos Verlag, Reihe: Recht der neuen Technologien (RnT), 2021. vol. 2. 450.
- ZÓDI, Zsolt: *A legal theory of platform law*. *Pro Publico Bono – Public Administration*, 2024/1. 101.
- BERBERICH, Manuel – STEINER, Malgorzata: *Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers?* *European Data Protection Law Review*, 2016. vol. 2. no. 3. 422.