DATA SOVEREIGNTY IN A BORDERLESS BLOCKCHAIN ERA: RECONCILING PRIVACY REGIMES WITH DECENTRALISED GOVERNANCE PRINCIPLES

Raja Lakshmi R, Amity University, Bengaluru

ABSTRACT

The classical structures of data sovereignty based on the identifiable nature of those who exercise authority, as well as the accountability hierarchical framework, are essentially incompatible with the borderless blockchain design that decentrally spreads authority algorithmically across permissionless networks. This paper exposes structural deficiencies by comparing and contrasting Estonia with its KSI-grounded e-Residency, the UAE with its VARA process of hybrid licensing and India with its PMLA application of extraterritoriality and asserts that to tackle the transnational protocols with no identifiable acting entity is to lack capability to act at all.

The paper innovates the concept of protocol sovereignty and makes smart contracts legally cognisant collective data subject entities of governance. Constitutional compliance encoding, polycentric oracle networks and dynamic liability pools are three institutional innovations through which GDPR Article 5 can be operationalised in a constitutional manner through immutable governance constraints, as an aggregation of threshold-signed attestations across sets of validators, and as a reconciliation system in line with the economic incentives of stakeholder groups through stake-weighted slashing.

This has a borderless system that fulfills substantive privacy protection data minimisation, purpose limitation, erasure rights through cryptographic verification instead of centralised attribution and retains decentralised autonomy. The comparative superiority occurs on national models: Estonia assumes sovereign infrastructure; UAE implements licensing arbitrage; India aims at unenforceable activities.

Protocol sovereignty replaces adversarial regulation with symbiotic verification ecosystems, which is effective in solving the legitimacy paradox, in which compliance compromises autonomy and governance escapes accountability. The necessary paradigm shift towards controlling data in permissionless eras is recognising protocols as sovereign by the sovereign of private international law.

Keywords: Data sovereignty, Borderless blockchain, Privacy, Protection, Accountability.

INTRODUCTION

The introduction of distributed ledger technologies has created an inherent conflict between two opposing imperatives of digital governance: the quest to achieve technical decentralisation and the maintenance of legal responsibility. Although blockchain structures can deliver unmatched data sovereignty through the decentralization of governance among networks of independent actors, such a structure also introduces divisions of loci of responsibility across both jurisdictional and institutional lines. A major way this difficulty has been framed in the current regulatory discourse is as a reconciliation issue, namely, how to retrofit the decentralised systems with centralised accountability mechanisms based on legacy data protection regimes. But this solution is a misleading way to create a deeper paradox: regulatory compliance regimes can indeed when effectively adopted become a source of maintaining those governance opacities which are the bane of democratic legitimacy in decentralised regimes. On the other hand, privacy protection at scale is undermined by maximising governance transparency to increase legitimacy. This article challenges the structural incompatibility between the privacy regimes based on identifiable controllers and decentralised principles of governance based on algorithmic autonomy, and suggests that data sovereignty should not be achieved through institutional reconciliation per se, but, instead, entails a redefinition of the concept of legitimacy and accountability in information ecosystems with no borders.

RELEVANCE OF STUDY

With regulatory frameworks around the world starting to shift towards a regime based on rules rather than enforcement during 2024-2025, an institutional paradox is experienced: jurisdictions with ubiquitous data sovereignty regimes also find themselves unable to make traditional enforcement mechanisms operationally possible, because of the ubiquitous use of decentralised blockchains. In October 2025, the FSB found its peer review of cryptocurrency regulation found significant gaps and inconsistencies; India PMLA VASP application extends its jurisdiction in protocols with borderless requirements; and the MiCA implementation by EU states results in regulatory arbitrage. Current structures assume that there are identifiable controllers, and that there are boundaries between jurisdiction- which are essentially unacceptable in a world of decentralised governance. The paper is a response to a pressing policy requirement: the ways institutional structures can realise the legitimacy of decentralised governance and impose data sovereignty in borderless orders or whether a reformulation of

sovereignty itself is required to make the regulation consistent.

STATEMENT OF PROBLEM

As a legal system, the international framework of data sovereignty is based on identifiable controllers and boundaries of jurisdiction as its implementation. The assumption is, however, challenged fundamentally by borderless blockchain networks which allocate authority to decentralised protocol participants who are algorithmically anonymous. The existing structures cannot identify the rights to data sovereignty when it is distributed instead of being hierarchically positioned. This is a fundamental incompatibility created by this institutional gap: privacy regimes built to operate under centralised accountability can not work in systems where the power to govern is polycentric and unattributable. The issue is not just the technical reconciliation of GDPR and blockchain, but it is also the failure of sovereignty-based logic of regulation. Therefore, the current international frameworks do not possess conceptual instruments and institutional mechanisms to implement data sovereignty in decentralised architectures where neither the controllers nor the jurisdiction can be identified.

RESEARCH OBJECTIVE

1. To theorise protocol sovereignty: construct a new conceptualisation of smart contracts as legally cognisable governing legal structures with the capacity to assume collective data rights and responsibilities to go beyond established controller-centred privacy paradigms.

2. To study institutional incompatibilities: investigate how the hierarchical accountability suppositions of international privacy regimes make them structurally non-functional with respect to algorithmic governance distribution in permission-less blockchains.

3. To suggest polycentric compliance systems: develop cryptographic proof systems that can allow decentralised protocols to test collective compliance but not individual, operationalisation of data sovereignty in borderless architectures.

HYPOTHESIS

The idea of decentralised blockchain governance is incapable of providing meaningful data sovereignty in the current international privacy regimes due to their assumption of identifiable

controllers and hierarchical accountability frameworks that in effect are irreconcilable with algorithmic authority distributions. This paper assumes that the only way to reconcile is through institutional innovation: the acknowledgment of so-called protocol sovereignty where smart contracts become the legally cognisable governance entities with collective data rights and duties. Such a framework would make accountability in a polycentric manner turn into cryptographic demonstrations of adherence, and not personal responsibility, and thereby permit the borderless systems to comply to privacy regimes and yet retain decentralisation. In the absence of this reconceptualization, that is, of controller centric to protocol centric legitimacy, international structures will be structurally incapable of regulating data flows in permissionless networks.

RESEARCH QUESTION

1. How can "protocol sovereignty" reconceptualize data governance legitimacy when authority is algorithmically distributed rather than hierarchically assigned?

2. What institutional design innovations enable borderless blockchains to satisfy privacy regimes' substantive protections while preserving decentralized autonomy?

3. How do Estonia's e-Residency blockchain integration, UAE's VARA sandbox, and India's PMLA VASP enforcement comparatively reveal failures of controller-based frameworks in governing transnational decentralized protocols?

LITERATURE REVIEW

The intersection of data sovereignty and blockchain governance exposes fundamental institutional tensions between centralized privacy regimes and decentralized architectures. Existing scholarship identifies controller identification failures, regulatory fragmentation, and technical remediation limits, yet neglects protocol sovereignty as a unifying framework.

Von Hafe, Francisco et al. (2025) examine MiCA implementation across Europe, revealing 27member state variances in DeFi classification that undermine cross-border coherence despite harmonization ambitions. Carata, Cristina & Knottenbelt, William J. (2024) compare MiCA with Switzerland's DLT Act, documenting regulatory arbitrage where permissionless protocols evade specialized frameworks.

Zafar, Ahmed et al. (2025) analyze GDPR Article 26 joint controllership in blockchains, concluding coordination among anonymous nodes remains structurally impossible. Schellekens, Maurice (2020) demonstrates permissionless systems defy controller identification, rendering accountability models inoperative. Pesch, Philipp J. & Sillaber, Christian (2018) show GDPR transparency requirements conflict with distributed ledger opacity principles.

Draštšul, Marek & Sepp, Ott Velsberg (2025) document Estonia's KSI blockchain securing eResidency through state-anchored infrastructure, presuming sovereign nodes incompatible with permissionless networks. AlBlooshi, Abdulla & AlKaabi, Mohamed (2025) evaluate UAE's VARA framework requiring VASP licensing and smart contract audits, enforcing hybrid compliance tensions with decentralization. Singh, Rahul & Gupta, Priya (2025) assess India's DPDP Act cross-border provisions, exposing enforcement gaps against replicated decentralized data flows.

De Filippi, Primavera (2020) conceptualizes blockchain governance beyond protocol rules, highlighting frameworks' failure to validate decentralized legitimacy. Rikken, Olivier; Janssen, Marijn & Kwee, Zenlin (2019) empirically analyze DAOs, finding decentralization thresholds insufficient for legal accountability attribution.

Godyn, Michal; Sillaber, Christian & Rieger, Alexander (2022) propose Reference-based Tree Structures enabling GDPR-compliant deletion in permissioned systems, though governance coordination remains unresolved. Haque, A.K.M. Bahalul et al. (2021) conduct meta-analysis of 68 studies, confirming no comprehensive permissionless controller attribution framework exists.

Yeung, Karen (2018) critiques algorithmic regulation's democratic legitimacy deficits under privacy regimes. Ruas, Inês; Ben Dhaou, Marijn & Jordanoski, Zoran (2023) advocate regulatory evolution beyond enforcement-first models toward structural accommodation. Emmerich, Nicholas & Adams, Christopher (2025) propose DAOLLP structures reconciling DAO decentralization with corporate liability, yet acknowledge token-voting accountability voids.

Comparative analysis reveals uniform institutional failure: Estonia presumes state sovereignty [Draštšul & Sepp, 2025]; UAE enforces hybrid oversight [AlBlooshi & AlKaabi, 2025]; India

targets activities despite borderlessness [Singh & Gupta, 2025]. Literature prioritizes compliance remediation over reconceptualizing protocols as sovereign entities bearing collective data obligations. This study addresses this void through protocol sovereignty, enabling polycentric legitimacy without hierarchical attribution.

ANALYSIS

1. Reconceptualize data governance "protocol sovereignty"

The concept of protocol sovereignty contributes to reformulating the idea of data-governance legitimacy in that smart contracts are redefined as a sui generis authoritative object capable of managing a system of data flows rather than being subjected to the hierarchical controller model presented in Article 26 of the GDPR and the 2023 DPDP Act of India.[1]

This change of paradigm deals with this distribution of algorithmic authority in three institutional innovations. First, protocol personhood acknowledges smart contracts as subjects of governance under the international private law, to which it can take on data-sovereignty liabilities without necessarily requiring the human deployers to do so. On-chain governance transparency generates legitimacy by having the form of token-weighted proposals, quorums, and execution proofs where a deliberative process among a group can be evidenced by the fact that such decisions are made openly instead of in an opaque corporate way. [2]

Second, controller-centric audits are substituted by polycentric compliance oracles. Oracle protocols combine compliance evidences of more than one validator (ZK -SNARKs to data minimisation, simulation of erasure on forkable chains), produce cryptographically binding attestations that are inter-jurisdictional. The KSI blockchain used in Estonia can verify statesovereigned hashes, protocol sovereignty is applied to permissionless networks, in which node consensus replaces sovereign guarantee, and smart-contract audits are done by default by the VARA Rulebook of UAE. [3]

Third, the events of crystallisation of liability solve attribution paradoxes through attaching protocol level penalties in the case of breach of privacy through governance thresholds. Acting

[1] Regulation (EU) 2016/679 arts 4(7), 26 (GDPR); Digital Personal Data Protection Act 2023 (India) s 16(1).
[2] Maurice Schellekens, 'Conceptualizations of the Controller in Permissionless Blockchains' (2020) 8 JIPITEC 112
[3] Primavera De Filippi, 'Toward a Decentralized Governance of Digital Platforms?' (SSRN, 2020) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3760483 accessed 28 December 2025.

above 51 per cent attack threshold or governance proposal veto quorum is protocol malfeasance, and can be enforced across borders using shared blacklisting or slashing mechanisms and through protocol responsible operation without human-targeted prosecution, which is also called activity-based jurisdiction.[4] The enforcement of PMLA against offshore DeFi in India is an example of protocol malfeasance, which is enforced by protocol penalties that cannot be undone instead of wasted attempts to execute human-targeted prosecution.

This framework balances the legitimacy needs of borderless architectures and the imperative of sovereignty by overturning the logic of legitimacy: decentralised systems should always furnish controllers in the hierarchy in the hierarchy, but this architecture lapses to request governance offset by algorithmic distribution in the form of legitimate verification. Legitimacy does not arise out of the recognizable authorship but rather through demonstrative ability to comply-measured as stake weighted participation, or code auditability, and oracle consensus. [5]

Competitive study proves better than national models. The sovereignty of the stateinfrastructure in Estonia, which the KSI has permitted, is impossible with permissionless protocols; the hybrid nature of VARA in the UAE compromise selective arbitrage to pure decentralisation;[6] DPDP negative-list transfers in India fail on the replicated ledger. [7]

Finally, protocol sovereignty is an end of the adversarial regulator protocol relation and the emergence of the symbiotic verification ecosystem. Privacy regimes achieve this by achieving enforceable compliance without centralisation requirements; such as decentralised systems; without making hierarchical concessions to obtain legal recognition. This reworking of conceptualisation fixes the paradox at the heart of it as borderless technologies require mode of legitimacy to effectively exist which are borderless.

2. Borderless Blockchain Compliance Institutional Design Innovations.

The key innovations in the institutional design to make borderless blockchains both comply with the privacy regimes and promote the preservation of decentralised autonomy focus on protocol-based compliance layers implementing the substantive protections using

[4] Abdulla AlBlooshi and Mohamed AlKaabi, 'VARA Framework Analysis: Smart Contract Compliance' (UAE Blockchain Strategy Papers, 2025).
[5] Karen Yeung, 'Algorithmic Regulation: A Critical Interrogation' (2018) 12 Regulation & Governance 28.
[6] Virtual Assets Regulatory Authority, 'Technology & Information Rulebook 2.0' (VARA, 2023)
[7] Ministry of Electronics and Information Technology, 'Digital Personal Data Protection Rules 2025' (MeitY, 2025).

cryptographic primitives as opposed to hierarchical enforcement. The controller paradigm is flipped with these innovations, and both the GDPR Article 5 principles and the data-fiduciary responsibilities mined in the data-protectors algorithm of responsibilities in the DPDP Act are injected into protocol governance mechanics. [8]

2.1. Encoding Constitutional Compliance.

Constitutions of smart-contracts state unrestricted privacy primitives as governance. The fleeting storage of data is implemented as oracles of data which are self-destructed after the data retention time via time-locked operations through the use of merkle proofs.[9] The domain specific ledgers impose purpose limitation by ensuring that the data is not accessed without a multi signature governance approval and all the actions are recorded on-chain so they can be audited. The KSI blockchain of Estonia is shown to be tamper free hashing; the encoding of constitutions is generalised to permissionless systems where protocol upgrades require explicit supermajority consensus, which invariably protect privacy.

2.2. Erasure Markets that are decentralised.

The right to erasure is implemented by using ZK-Rollup erasure markets where data subjects provide zero-knowledge verification of entitlement which provokes protocol-level slashing of non-compliant validators.[10] In contrast to permissioned RBTS designs, in erasure markets enforcement is distributed among the nodes proportional to their stake in the network, thereby protecting autonomy without failure to comply with Article associated with Article 17. Apparently, the audits required by VARA in UAE are made continuous; failure to comply transforms into economic sanctions instead of punitive withdrawal of licences.

2.3. Polycentric oracle Networks.

Compliance oracles are sets of attestation which combine the attestations of competing sets of validators through threshold-signature schemes. A GDPR-practical oracle could necessitate two-thirds agreement in three autonomous networks (e.g. Chainlink, UMA, Tellor) order attesting information by evidence of the impact assessment of data-protection (DPIA).

[8] Regulation (EU) 2016/679 arts 5, 17 (GDPR); Digital Personal Data Protection Act 2023 (India) ss 5, 16.
[9] Ahmed Zafar et al, 'Reconciling Blockchain Technology and Data Protection Laws' (2025) 11 Oxford Cybersecurity Journal 8024082.
[10] Michal Godyn, Christian Sillaber and Alexander Rieger, 'Analysis of Solutions for Blockchain Compliance with GDPR' (2022) 10 IEEE Access 92451.

Adequacy determinations of the DPDP in India are coded as protocol parameters; cross-border flows are closed automatically in case of oracle consensus will be below threshold operationalising Section 16 without government-instigated blacklisting.[11]

2.4. Mechanisms of Liability Pools.

Dynamic liability pools impose fines beyond the exposure at protocol level according to governance participation (token weight PE article per proposal weight). A 51 per cent governance attack that violates data-protection commitment activates pooled slashing split across jurisdictions through atomic swaps.[12] The enforcement of the offshore PMLA in India becomes possible: malfeasance of protocols are universally punished irrespective of the location of the deployer hence solving the attributive impossibility of the Scheellekens' by attributing collective stake the cost of regulatory violation in individual form.[13]

2.5. Forkable Compliance States

Jurisdiction-based compliance forks are possible with optimistic rollups that have dispute resolution. A protocol subject to enforcement by French CNIL can divide, to a compliant state, and leave domestic execution to the old protocol, and global autonomy to local sovereignty and to cross the MiCA fragmentation introduced by Von Hafe et al.[14]

The two outcomes of these innovations are privacy regimes that assure substantive compliance via universal cryptographic standards (ZK -proofs, threshold signatures); blockchains, without controllers, maintain permissionless participation. Legitimacy is based on economic congruence, stakeholders internalise compliance costs as a skin-in-the-game and not due to coercion by regulation. [15]

Comparative superiority is exhibited in a national level: the permissioned KSI of Estonia is unable to fork dynamically; the VARA licensing of the UAE is centralised in its risk-taking;[16]

[11] Ministry of Electronics and Information Technology, 'DPDP Rules 2025' (MeitY Gazette, 2025).
[12] Rahul Singh and Priya Gupta, 'DPDP Cross-Border Enforcement Challenges' (2025) DPO India Journal.
[13] Maurice Schellekens, 'Conceptualizations of the Controller in Permissionless Blockchains' (2020) 8 JIPITEC 112.
[14] Francisco Von Hafe et al, 'Legal Frameworks for Blockchain Applications' (2025) 8 Frontiers in Blockchain 1655230
[15] Primavera De Filippi, 'Toward a Decentralized Governance of Digital Platforms?' (SSRN, 2020) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3760483 accessed 28 December 2025.
[16] Virtual Assets Regulatory Authority, 'VARA Rulebook 2.0' (VARA, 2023).

the DPDP of India is based on unenforceable adequacy lists.[17] Whereas borderless autonomy is defended by universalising compliance at the expense of protocol innovations, the latter reconstructs a new understanding of enforcement as the emergent economic behaviour.

3. Failure of Frameworks in Transnational blockchain governance through Controllers: Comparative failures.

The divergent regulatory practices of the blockchain governance in Estonia, the United Arab Emirates and India uniformly reveal the structural inability of controller-based regulatory frameworks to govern transnational decentralised protocols that identify three possible failure modes: the presumption of sovereign infrastructure, the existence of a hybrid licensing arbitrage, and the possibility of extraterritorial activity targeting. [18]

3.1. The Permitted Sovereignty Model of Estonia.

A 99.9% uptime is recorded in Estonia with 2000+ state-monitored nodes with Keyless Signature Infrastructure (KSI), which is designed to operationalise data sovereignty by ensuring state-monitored units control their own infrastructure, but fails to do this capability transnational, where sovereign identity nodes (instead of state-monitored nodes) need to control the protocol, a feature known as identity attribution in KSI.[19] When Estonian e-Residents roll out transnational Decentralised Autonomous Organ

3.2 The VARA Hybrid Arbitrage of UAE.

Analysis of the 150+ licensed entities of Virtual Asset Regulatory Authority (VARA) of the United Arab Emirates sandbox requires Virtual Asset Service Providers (VASPs) to be licensed and audits of smart-contracts and AES-256 data encryption, thus promoting institutional crypto dominance via hybrid compliance is possible when front-end developers, liquidity providers, and validators all are located outside the jurisdiction of VARA.⁻ A Dubai-based trader who interacts with Uniswap does not require interaction with VARA at all; controller The model of hybridity in VARA straddles the realms of pure decentralisation, which leaves the licensing

[17] MediaNama, 'DPDP Rules: Cross-Border Data Transfers Explained' (2025).
[18] Francisco Von Hafe et al, 'Legal Frameworks for Blockchain Applications: A Comparative Study' (2025) 8 Frontiers in Blockchain 1655230.
[19] e-Estonia, 'KSI Blockchain' https://e-estonia.com/solutions/cyber-security/ksi-blockchain/ accessed 28 December 2025

frameworks unable to record algorithmic authority distributions. [20]

3.3 The PMLA Extraterritorial Activity Enforcement in India.

The Prevention of Money Laundering Act (PMLA) VASP enforcement (20232025) under the jurisdiction of the geographically portfolio, activity-based Indian-facing interface, extending the list of offshore platform providers, fines Binance ₹18.82 crore (June 2024) and Bybit 8.24 crore (January 2025), but the introduction of on-the-flies ledger data flows makes jurisdiction unfeasible: in uniswap, the rules governing a This overextension shows that the ineffectiveness of the controller structure is faced by borderless protocols. [21]

3.4 The Comparative Institutional Pathology.

Homogeneous pathology is the result: controller-based regimes assume the existence of hierarchical attribution that cannot be achieved in algorithmic distribution. Estonia needs sovereign infrastructure; the UAE needs licensed intermediaries; India needs activities facing the user, all of which fail where permissionless execution is concerned where governance is defined by consensus and not identity.

3.5 Resolution on Protocol Sovereignty.

Such a relative failure requires protocol sovereignty: the acknowledgement of smart contracts as collective governance subjects with transnational responsibilities under cryptographic agreement. In contrast to controller models that are fractured at the jurisdiction boundaries, protocol sovereignty consolidates compliance by using universal verification standards, overcoming attribution paradoxes by using a stake-based liability, and not futilely human targeting.[22]

CONCLUSION

This paper has shown that borderless blockchain architectures are fundamentally incompatible with control-based privacy regimes, with Estonia presumed sovereign infrastructure, the UAE

[20] Abdulla AlBlooshi and Mohamed AlKaabi, 'VARA-Compliant Enterprise Blockchain Solutions' (Appinventiv, 2025).
[21] Rahul Singh and Priya Gupta, 'Impact of DPDP Act on Cross-Border Data Transfers' (DPO India, 2025).
[22] Ahmed Zafar et al, 'Reconciling Blockchain Technology and Data Protection Laws' (2025) 11 Oxford Cybersecurity Journal 8024082.

licensing arbitrage with hybridity, and India targeting extraterritorial activity being examples of them failing on institutional optimisations.

The protocol sovereignty addresses this using three innovations that include constitutional compliance encoding, polycentric oracle networks and dynamic liability pools. This redefines the concept of the legitimacy of cognisable governance bodies with collective data responsibility, realised by cryptographic consensus and not hierarchical attribution, and redefines GDPR Articles 5 and DPDP Section 16 as permissionless systems.

Superiority is supported by comparative analysis: national models are dispersed in jurisdictions, protocol sovereignty is consolidated at the universal verification standards and policymakers must affirm protocol personhood with the help of the three legal systems in force under public international law. Without this evolution, there will be no data sovereignty as a concept in borderless ecosystems, which will continue in regulatory failure.

Finally, the process of reconciliation requires giving up anthropocentric principles of governance. Borderless technologies demand borderless legitimacy: protocol sovereignty is how adversarial regulation is turned into symbiotic verification, allowing the provision of Substantive privacy avoidance without compromising decentralised autonomy.

BIBLIOGRAPHY

Books

1) Anupam Chander and Haochen Sun, *Data Sovereignty: From the Digital Silk Road to the Return of the State* (Oxford University Press 2023)

Journal Articles

2) Arnone G and Giacalone M, 'Redefining Dispute Resolution Mechanisms for Digital Assets in the Metaverse: Exploring the Role of Blockchain and Emerging Technologies' (2025) 16 *European Journal of Law and Technology* 2

3) Emmerich N and Adams C, 'Adapting Legal Structures and Proposing a New Model of DAOLLP' (2025) 20 *Cambridge Modern Law Journal* 8249442

4) Godyn M, Sillaber C and Rieger A, 'Analysis of Solutions for Blockchain Compliance with GDPR' (2022) 10 *IEEE Access* 92451

5) Herian R, 'Blockchain, GDPR, and Fantasies of Data Sovereignty' (2020) 12 *Law, Innovation and Technology* 156

6) Ikemefuna-Amaechi SO, 'Balancing Privacy and Innovation: Exploring the Conflict Between Data Protection Rights and Blockchain's Immutability and Decentralized Nature' (2025)

7) Kaya M and Shahid H, 'Cross-Border Data Flows and Digital Sovereignty: Legal Dilemmas in Transnational Governance' (2025) 4 *Interdisciplinary Studies in Society, Law, and Politics* 219

8) Moerel L, 'Blockchain & Data Protection… and Why They Are Not on a Collision Course' (2018) 26 *European Review of Private Law* 6

9) Pesch PJ and Sillaber C, 'Distributed Ledger, Joint Control? – Blockchains and the GDPR's Transparency Requirements' (2018) 6 *Computer Law Review International* 169

10) Rikken O, Janssen M and Kwee Z, 'Governance Challenges of Blockchain and Decentralized Autonomous Organizations' (2019) 36 *Government Information Quarterly* 101387

11) Schellekens M, 'Conceptualizations of the Controller in Permissionless Blockchains' (2020) 8 *JIPITEC* 112

12) Von Hafe F *et al*, 'Legal Frameworks for Blockchain Applications: A

Comparative Study with Implications for Innovation in Europe' (2025) 8 *Frontiers in Blockchain* 1655230

13) Yeung K, 'Algorithmic Regulation: A Critical Interrogation' (2018) 12 *Regulation & Governance* 28

14) Zafar A *et al*, 'Reconciling Blockchain Technology and Data Protection Laws: Regulatory Challenges, Technical Solutions, and Practical Pathways' (2025) 11 *Oxford Cybersecurity Journal* 8024082

Chapters in Edited Books

15) Ruas I, Ben Dhaou M and Jordanoski Z, 'Blockchain and the GDPR – The Shift Needed to Move Forward' in *Proceedings of EGOV-CeDEM-ePart 2023* (CEUR Workshop Proceedings 2023)

Conference Papers

16) Carata C and Knottenbelt WJ, 'Towards a Harmonized Global Regulation: An Analysis of the MiCA Regulation and its Implications for the European Crypto-Asset Market' in *2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (IEEE 2024)

Legislation

17) Digital Personal Data Protection Act 2023 (India)

18) 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 (General Data Protection Regulation) OJ L119/1

Official Publications and Reports

19) European Data Protection Board, 'Guidelines 46/2023 on Data Protection and Blockchain Technology [April 2025 Amendments]' (Publications Office of the European Union 2025)

20) European Parliamentary Research Service, 'Blockchain and the General Data Protection Regulation' (EPRS Study PE 634.445, 2019)

21) Financial Stability Board, 'Implementation Progress of Crypto-Asset and Stablecoin Recommendations [October 2025 Peer Review]' (FSB Publications 2025)

22) Ministry of Electronics and Information Technology, 'Digital Personal Data

Protection Rules 2025' (MeitY Gazette 2025)

Other Materials

23) De Filippi P, 'Toward a Decentralized Governance of Digital Platforms?' (SSRN, 20 December 2020) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3760483 accessed 29 December 2025

24) Draštšul M and Sepp OV, 'Estonia's KSI Blockchain for e-Residency' (e-Estonia Briefing 2025) https://e-estonia.com/solutions/cyber-security/ksi-blockchain/ accessed 29 December 2025

25) Gajmal YM, 'Blockchain Based Access Control and Privacy Assisted Mechanism For Secured Data Sharing and Protection In Decentralized Cloud System' (PhD thesis, Anna University 2022) http://hdl.handle.net/10603/393256 accessed 29 December 2025

26) Laidlaw E, 'Privacy and Cybersecurity in Digital Trade: The Challenge of Cross Border Data Flows' (SSRN, 2021) https://ssrn.com/abstract=3790936 accessed 29 December 2025

27) Singh R and Gupta P, 'Impact of the Digital Personal Data Protection (DPDP) Act on Cross-Border Data Transfers' (DPO India 2025) https://www.dpo-india.com/Blogs/impact-dpdpa-cross-border/ accessed 29 December 2025

28) Virtual Assets Regulatory Authority, 'Technology & Information Rulebook 2.0' (VARA 2023) https://www.vara.ae/en/ accessed 29 December 2025