Doctoral (PhD) Dissertation Abstract

The Problems of Effective Forgetting in Blockchain Wallet Providers: A European Union Data Protection Perspective

Presented by

PhD Candidate:

MARIAM PILISHVILI

Supervisor:

Prof. Dr. habil. ILDIKÓ BARTHA, Ph.D.

Professor of Law

UNIVERSITY OF DEBRECEN

Marton Géza Doctoral School of Legal Studies

Debrecen, 2026

Research Problem and Objectives

1. The Transformation of Data in Digital Society

Over the last few decades, we have transitioned from a society that uses digital tools to one that inhabits them.[1] Data is no longer generated only in discrete interactions but is continuously produced through everyday activities such as communication, online browsing, financial transactions, geolocation tracking, and participation in digital platforms.[2] Individuals increasingly exist within environments characterised by constant data generation, where technological infrastructures mediate access to employment, financial services, healthcare, education, and social participation.[3]

The traditional view of data as a „by-product" is no longer theoretically tenable.[4] Instead, we must recognize that digitalization has integrated personal data into the very scaffolding of the social order.[5] Behavioural data, metadata, and transactional information collectively form persistent digital profiles capable of influencing decision-making processes in both public and private sectors.[6] Algorithmic processing systems rely on these data flows to produce predictive insights and behavioural classifications, contributing to the emergence of data-driven governance models.[7]

In this environment, the protection of personal data becomes closely linked to the preservation of autonomy, dignity, and informational self-determination. Legal frameworks governing data processing must therefore respond not only to technological change but also to the broader transformation of social relations mediated by digital infrastructures.[8] The expansion of data processing capabilities has intensified debates concerning transparency, accountability, and control over personal information.

---

[1] McLuhan, M. (1994). *Understanding media: the extensions of man.* Cambridge, MA: MIT Press, pp. 7–21. Available at: https://designopendata.wordpress.com/wp-content/uploads/2014/05/understanding-media-mcluhan.pdf, (Accessed: 19 April 2026).

[2] Lupton, D., (2016). *The Quantified Self.* Polity Press, ISBN-13: 978–1–5095–0059–8, pp. 94–112.

[3] Goodchild, M.F. (2007). *Citizens as sensors: the world of volunteered geography*. GeoJournal, 69(4), pp. 211–221, DOI 10.1007/s10708-007-9111-y.

[4] Lyon, D. (2018). *The Culture of Surveillance: Watching as a Way of Life*. Cambridge: Polity Press, ISBN-13: 978-0-7456-7172-7, pp. 2–6; see also, Cohen, J.E. (2019). *Turning Privacy Inside Out*. Theoretical Inquiries in Law, 20(1), pp. 1–32. doi:10.1515/til-2019-0001, pp. 3-6. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3162178, (Accessed: 19 April 2026); see also, Ghosh, A. (2022). *RegTech: From KYC to KYD to ... KYDL*. MEDIUM, Available at: https://medium.com/@avi900in/regtech-from-kyc-to-kyd-to-kydl-47e219e4a424, (Accessed: 19 April 2026).

[5] Mayer-Schönberger, V. and Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think*. pp.40–48, 98–101.

[6] Beer, D. (2016). *Metric Power*. Basingstoke: Palgrave Macmillan, ISBN 978-1-137-55648-6, p. 148–156; see also, Pistor, K. (2019). *The Code of Capital: How the Law Creates Wealth and Inequality*. Princeton: Princeton University Press, pp. 210–213.

[7] Kitchin, R. (2016). *Thinking critically about and researching algorithms.* Information, Communication & Society, 20(1), pp. 1–14. Available at: https://www.researchgate.net/publication/297664844_Thinking_critically_about_and_researching_algorithms, (Accessed: 19 April 2026).

[8] O'Connell, A. and Frick, W. (2014). *You've Got the Information, But What Does it Mean? Welcome to "From Data to Action*." Harvard Business Review, p. 1; see also, Kitchin, R. (2014). *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences*. London: SAGE, pp. 27–30.

2. EU Data Protection Law as a Technologically Neutral Framework

The evolution of European data protection law isn't just a reaction to the digital age, it's a deliberate attempt to reconcile the human right to privacy with the economic reality of a data-driven market. By establishing the General Data Protection Regulation (GDPR), the EU sought to create a framework that is both robust enough to protect the individual and flexible enough to let information flow across borders.[9]

Technological neutrality plays a central role in ensuring the long-term relevance of data protection law. Rather than regulating particular technical solutions, the GDPR establishes general principles governing lawful processing, data minimisation, purpose limitation, transparency, and accountability.[10] This approach allows the regulation to remain applicable across evolving technological environments, including cloud computing, artificial intelligence, and distributed ledger technologies.

At the same time, the effectiveness of technologically neutral legislation depends on the interpretative flexibility of legal concepts such as personal data, processing, controllership, and erasure. The application of these concepts to emerging technological infrastructures often requires doctrinal adaptation capable of preserving the underlying objectives of fundamental rights protection.

The Court of Justice of the European Union has consistently emphasised that data protection law must ensure effective and complete protection of individuals' rights. This interpretative orientation supports a functional approach that focuses on the practical impact of processing activities on individuals rather than on purely technical distinctions between forms of data architecture.

3. Blockchain as a Structural Challenge to Data Protection Law

Blockchain technology introduces a distinctive form of data architecture based on decentralised validation, cryptographic verification, and append-only data structures.[11] Transactions recorded on blockchain networks are replicated across multiple nodes and are designed to resist modification once confirmed through consensus mechanisms.[12] This structural persistence contributes to the perceived reliability and security of blockchain infrastructures.

---

[9] European Parliament and Council, (2016). Regu*lation (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). Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj, (Accessed: 19 April 2026).

[10] Nyrén, O., Stenbeck, M. and Grönberg, H., (2014). *The European Parliament proposal for the new EU General Data Protection Regulation may severely restrict European epidemiological research*. European journal of epidemiology, 29(4), pp. 227–230. Available at: https://www.researchgate.net/publication/262111577_The_European_Parliament_proposal_for_the_new_EU_General_Data_Protection_Regulation_may_severely_restrict_European_epidemiological_research, (Accessed: 19 April 2026).

[11] Tapscott, D., Tapscott, A. (2016) *Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World*. New York: Penguin, pp. 22–28.

[12] Mougayar, W. (2016). *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. Hoboken, NJ: John Wiley & Sons, pp. 15–18; see also, King, M. (2016). *The End of Alchemy: Money, Banking, and the Future of the Global Economy*. New York: W. W. Norton, pp. 3–8.

Yet these same characteristics, immutability, replication, pseudonymity, bring blockchain into sharp tension with data protection law. The right to be forgotten under Article 17 GDPR presumes the possibility of erasure or modification,[13] while blockchain ledgers are designed to resist alteration.[14] Similarly, GDPR presupposes identifiable controllers and processors who determine the purposes and means of processing,[15] whereas blockchain distributes decision-making across decentralised networks.[16] As John Mathews observes, "The GDPR was written on the assumption that you have centralized services controlling access rights to the user's data, which is the opposite of what a permissionless blockchain does."[17] The paradox is stark: is data recorded on blockchain still subject to GDPR? If so, how can its requirements be met without undermining the very properties that make blockchain distinctive?[18]

Yes, the GDPR applies, but not to the "blockchain" architecture, but to the object of its processing: personal data.[19] The moment personal data enters the ledger, be it in the form of public keys, transaction metadata, or hashed identifiers, the regulatory obligations are triggered. In other words: the law attaches to the data,[20] while the difficulty lies in the design.[21]

4. The Role of Wallet Providers in Blockchain Ecosystems

The rapid adoption of blockchain technologies and the proliferation of blockchain wallets, both custodial and non-custodial, have fundamentally reshaped how personal data is generated, stored, and shared. Every wallet transaction leaves an immutable, publicly verifiable trail on the distributed ledger.[22] This technical feature, while essential for transparency and trust, creates an ecosystem of "remember-by-default" data, in stark contrast to the human brain's natural "forgetting-by-default" mechanism.[23]

This persistence of data raises several critical challenges.

First, loss of control over personal data is inherent to the design. A user who interacts with a decentralized application (dApp) or sends funds using a wallet address cannot later retract that transaction history.[24] This is particularly problematic when addresses can be linked, even indirectly, to a real-world identity through on-chain analysis, leaks, or regulatory reporting

---

13 GDPR, Article 17.

14 Ministry of Digital Affairs, DLT and Blockchain Working Group, (2019). *The GDPR and the blockchain technology*. Warsaw: Ministry of Digital Affairs, pp. 1–10.

15 GDPR, Articles 4(7), 4(8), 26, 5(2), Recitals 79, 74, 81.

16 DLT and Blockchain Working Group, *The GDPR and the blockchain technology*, 2019, pp. 1–10.

17 Meyer, D., (2018). *Blockchain technology is on a collision course with EU privacy law*. International Association of Privacy Professionals Article, The Privacy Advisors. Available at: https://iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law, (Accessed: 29 July 2025).

18 Finck, 2019, pp. 8–13.

19 GDPR, Article 2(1).

20 GDPR, Article 4(1).

21 GDPR, Article 17.

22 Casey, M. & Vigna, P. (2018). *The Truth Machine: The Blockchain and the Future of Everything*. New York: St. Martin's Press, pp. 71–78.

23 Mayer-Schönberger, V., (2009). *Delete: The Virtue of Forgetting in the Digital Age*. Princeton University Press, 2009, pp. 1–15.

24 Antonopoulos, A.M. (2015). *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. 1st edn. Sebastopol, CA: O'Reilly Media, Incorporated, pp. 62–65.

requirements. a wallet address that was once used anonymously may eventually be deanonymized via analytics services or centralised exchange records, revealing years of historical activity.[25]

Second, there are significant contextual dangers associated with everlasting traceability.[26] Consider a scenario where a user experiments with a blockchain-based service that subsequently fails due to controversy or scandal. The user's wallet history is still publicly available years later, which could have an impact on job applications, legal disputes, or even personal and interpersonal relationships. Much like the digital traces left on social media platforms, immutable blockchain records can resurface in ways that users neither anticipate nor consent to.[27]

Third, self-censorship and participation chilling effects emerge. As users become more aware that every interaction is recorded permanently, they may avoid exploring innovative decentralized services or supporting causes that carry social or political sensitivity.[28] In this way, immutable design can inadvertently constrain user autonomy and freedom of expression.

Understanding the role of wallet providers is therefore essential for assessing how GDPR obligations may operate in decentralised technological environments. Their position as interface actors suggests that they may have influenced how personal data becomes accessible, linkable, or interpretable within blockchain ecosystems.

5. The Role of Wallet Providers in Blockchain Ecosystems

Article 17 GDPR establishes the right to erasure, commonly known as the right to be forgotten. The provision allows individuals to request the removal of personal data where specific legal grounds are met, including situations in which the data is no longer necessary for the purpose for which it was collected, consent has been withdrawn, or the processing was lawful.[29]

The effectiveness of erasure largely depends on whether personal data can be technically removed or access to it can be meaningfully restricted. In centralised environments, data controllers can usually delete stored information or adjust databases in order to comply with legal requirements.[30] Blockchain-based systems present additional challenges, as data recorded

---

[25] Greenberg, A. (2022). *Tracers in the Dark: The Global Hunt for the Crime Lords of Cryptocurrency*. 1st edn. New York: Knopf Doubleday Publishing Group, Chapter 14, pp. 99–104.

[26] Brin, D. (1998). *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* ISBN : 978-0-465-02790-3, pp. 18–22.

[27] See most high-profile deanonymization cases, the Silk Road Takedown (2013), the Colonial Pipeline Ransomware Payment (2021), and Roman Sterlingov and Bitcoin Fog (2021), that have been used for legitimate and even critical law-enforcement purposes. However, this also raises concerns about privacy and surveillance, meaning, once a wallet is linked to a person, every past transaction becomes traceable.

[28] Kenyon, M. (2017). Jon Penney on the Chilling Effects of Online Surveillance. Available at: https://citizenlab.ca/2017/07/jon-penney-on-the-chilling-effects-of-online-surveillance/, (Accessed: 19 April 2026).

[29] GDPR, Article 17; see also, Belen-Saglam, R., Altuncu, E., Lu, Y. and Li, S., (2023). *A systematic literature review of the tension between the GDPR and public blockchain systems*. Blockchain: Research and Applications, 4(2), p.100129. Available at: https://arxiv.org/pdf/2210.04541, (Accessed: 19 April 2026).

[30] Solove, D., J., (2023). *The Limitations of Privacy Rights*. 98(3) Notre Dame Law Review 977, 983–985. Available at: https://ndlawreview.org/wp-content/uploads/2023/03/NDL301_Solove_Cropped.pdf, (Accessed: 19 April 2026).

on distributed ledgers may remain accessible across multiple nodes, even where access through user interfaces has been limited or removed.[31]

The persistence of data recorded on blockchain systems raises concerns regarding the long-term traceability of personal activity. Transaction histories may remain visible for an indefinite period, making it possible to reconstruct behavioural patterns through increasingly sophisticated analytical techniques.[32] Although blockchain identifiers are typically pseudonymous, developments in data analytics may enable the connection of such identifiers to identifiable individuals by combining blockchain data with external datasets.[33]

These characteristics invite reconsideration of how erasure should be understood in technologically complex environments. Rather than focusing exclusively on the physical deletion of data, it becomes relevant to assess whether restricting accessibility and limiting the possibility of linkage may provide comparable levels of protection. Legal interpretation must therefore consider whether the objectives of Article 17 GDPR can be satisfied through functional measures that reduce the practical likelihood of identifying individuals, even where the underlying data remains technically present within the system.

6. Effective Forgetting as a Doctrinal Response

The central premise of this dissertation is that the objectives of Article 17 GDPR may remain attainable in decentralised technological environments when erasure is understood in functional rather than purely literal terms.[34] Instead of requiring the complete physical deletion of data recorded on distributed ledgers, compliance may be assessed with reference to the practical accessibility, identifiability, and usability of personal data within a given technical and organisational context.

The concept of effective forgetting reflects this functional understanding of erasure.[35] Effective forgetting describes a situation in which the likelihood that personal data can be linked to an identifiable individual is significantly reduced through the application of appropriate technical and organisational measures. Such measures may include the deletion of off-chain data that

---

[31] Dewey, J., N., (2018). *Global legal insights: Blockchain & cryptocurrency regulation 2019 (1st ed.)*. Global Legal Group Ltd, pp. 5–8.
Available at: https://www.acc.com/sites/default/files/resources/vl/membersonly/Article/1489775_1.pdf, (Accessed: 19 April 2026).

[32] Koulu, R., (2016). *Blockchains and online dispute resolution: smart contracts as an alternative to enforcement*. SCRIPTed, Vol. 13 No. 1, pp. 41–69. Available at: https://journals.ed.ac.uk/script-ed/article/view/11491, (Accessed: 19 April 2026); see also, Binns, R., (2018). *Fairness in machine learning: Lessons from political philosophy*. Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR 81, pp. 149–159. Available at: https://proceedings.mlr.press/v81/binns18a.html, (Accessed: 19 April 2026).

[33] Mulligan, C., Scott, J.Z., Warren, S. and Rangaswami, J.P., (2018). *Blockchain beyond the hype: A practical framework for business leaders*. In white paper of the World Economic Forum, pp. 3–8. Available at: https://www.weforum.org/publications/blockchain-beyond-the-hype/, (Accessed: 19 April 2026).

[34] Lynskey, O., (2015). *Control over Personal Data in a Digital Age: Google Spain v AEPD and Mano Costeja Gonzalez*. The Modern Law Review, Vol. 78, No. 3, pp. 526–527, 529. Available at: https://www.jstor.org/stable/43829127, (Accessed: 19 April 2026).

[35] Mantelero, A., (2014). *The future of consumer data protection in the EU Re-thinking the "notice and consent" paradigm in the new era of predictive analytics.* Computer Law & Security Review, 30(6), pp. 643–660. Available at: https://www.sciencedirect.com/science/article/pii/S026736491400154X, (Accessed: 19 April 2026).

enables attribution,[36] the use of encryption to restrict access,[37] the delinking of identifiers,[38] the limitation of visibility at the interface level, and the minimisation of metadata collection capable of facilitating re-identification.

This approach is consistent with the technologically neutral character of EU data protection law, as well as with the interpretative approach of the Court of Justice of the European Union, which has emphasised the need to ensure the effective protection of fundamental rights in changing technological contexts.[39] The purpose is not to restrict technological development, but to ensure that legal safeguards remain capable of providing meaningful protection as digital infrastructures evolve.

By exploring the relationship between doctrinal interpretation and technical system design, the dissertation argues that data protection law can continue to operate effectively even where certain technological architectures limit the possibility of literal data deletion. In this sense, the analysis highlights the capacity of legal principles to adapt to structural characteristics of decentralised technologies while maintaining the underlying objectives of fundamental rights protection.

Research Questions

This dissertation examines whether the Article 17 can be meaningfully implemented within blockchain-based wallet ecosystems, and whether compliance should be reframed through the concept of "effective forgetting," whereby personal data becomes practically inaccessible even if not technically erased. By doing so, the dissertation develops a framework that reconciles the operational realities of decentralised, immutable technological infrastructures with the legal requirements of EU data protection law.

To achieve this goal, this dissertation addresses the following research question:

> *To what extent can custodial and non-custodial wallet providers comply with the Right to be Forgotten under Article 17 GDPR, and should the compliance standard be reframed as "effective forgetting," meaning practical inaccessibility of personal data rather than absolute erasure?*

The following grouped sub-questions, reflecting the doctrinal, governance, operational, and normative aspects of compliance, are addressed in the dissertation in order to answer this primary research question.

Group A. Doctrinal and Interpretative Questions
(Answered primarily in Chapter 3)

---

[36] Antonopoulos, 2015, pp. 235–236.

[37] Torres et al., 2023, pp. 1–3.

[38] Address delinking refers to the practice of reducing or removing the link between a blockchain address and a specific natural person by using techniques such as address rotation, hierarchical deterministic wallets, or off-chain identifiers. This reduces identifiability and supports pseudonymisation under GDPR (Recital 28).

[39] Floridi, L., (2005). *The ontological interpretation of informational privacy*. Ethics and information technology, 7(4), pp. 185–200. Available at: https://www.researchgate.net/publication/226949294_The_Ontological_Interpretation_of_Informational_Privacy, (Accessed: 19 April 2026).

- What constitutes “effective forgetting” in blockchain ecosystems, and can functional inaccessibility satisfy the substantive aims of Article 17 GDPR?
- To what extent can principles from CJEU jurisprudence, particularly Google Spain and Google v CNIL, be adapted to the unique architecture of blockchain networks?

Group B. Governance and Accountability Questions
(Answered primarily in Chapters 4 and 5)

- How should controllership and accountability be allocated in decentralized wallet ecosystems under the GDPR?

Group C. Operational and Compliance Questions
(Answered primarily in Chapter 5)

- What technical, regulatory, and contractual mechanisms could operationalize functional forgetting without undermining blockchain’s operational integrity?

Group D. Normative and Policy Questions
(Answered primarily in Chapter 5)

- What are the normative and policy implications of embedding effective forgetting in blockchain governance frameworks?

Novelty and Original Contribution

This dissertation contributes to European data protection scholarship by addressing the challenges that decentralised technological environments pose for the interpretation of the Right to be Forgotten. Rather than simply restating the tension between immutability and erasure, the research develops the concept of effective forgetting as a practical way to interpret Article 17 GDPR in systems where data cannot easily be deleted. By analysing technical and governance measures such as off-chain deletion, delinking identifiers, and encryption-based access restrictions, the dissertation proposes a structured approach that helps clarify how wallet providers may implement proportionate compliance solutions. In this way, the study connects legal doctrine with technological design and offers a practical contribution to ongoing debates on data protection in distributed systems.

Second, the dissertation develops a functional approach to controllership in blockchain environments by examining the different roles played by custodial and non-custodial wallet providers. By analysing how decision-making power is distributed across technical infrastructures, the study shows how existing GDPR concepts of responsibility may still apply in decentralised systems. Drawing on CJEU case law, including Google Spain, Google v CNIL, and Wirtschaftsakademie, the research demonstrates that established legal principles can be adapted to new technological contexts.

Third, the dissertation explores how privacy-enhancing technologies, smart contractual governance tools, and regulatory testing environments may support compliance with data protection law in blockchain ecosystems. By examining how technical design choices may help

balance confidentiality,[40] accountability,[41] and regulatory oversight,[42] the study provides practical insight into how hybrid compliance models may function in decentralised environments, while remaining consistent with the EU's broader commitment to fundamental rights and informational self-determination.

Methodology

This dissertation adopts a combined doctrinal and socio-legal methodology in order to examine how blockchain wallet providers may comply with EU data protection law.

The doctrinal legal approach, sometimes referred to as the black-letter method,[43] focuses on analyzing primary legal sources, including:

- The General Data Protection Regulation (GDPR)
- Relevant CJEU judgments (such as Google Spain and Google v. CNIL)
- Guidance and opinions from the European Data Protection Board (EDPB)
- Supplementary EU legal instruments relating to privacy and data protection

This approach is supported by a thorough review of secondary legal sources, including scholarly articles, legal commentaries, and regulatory reports, to critically examine how Article 17 (Right to Erasure), data minimization, purpose limitation, and controllership principles are interpreted in legal and academic discourse.

The socio-legal dimension places legal analysis within the practical context of blockchain technology. It examines how custodial and non-custodial wallets process personal data and how technical design choices affect the feasibility of GDPR compliance.

Together, these methods provide a framework for analysing controllership and erasure obligations in blockchain ecosystems, illustrating how legal doctrine interacts with technological design.

Structure of the Dissertation

The dissertation begins with an Introduction presenting the research background, objectives, methodology, and scope.

---

[40] Joseph, S., (2024). *Balancing data privacy and compliance in blockchain-based financial systems.* Journal of Engineering Research and Reports, 26(9), pp.170–184.

[41] Neisse, R., Steri, G. and Nai-Fovino, I., (2017). *A blockchain-based approach for data accountability and provenance tracking.* In Proceedings of the 12th international conference on availability, reliability and security, pp. 1–8. Available at: https://arxiv.org/pdf/1706.04507, (Accessed: 19 April 2026).

[42] Coinmetro, (2025). *Regulatory Sandboxes: Fostering Crypto Innovation Within Legal Frameworks*. Available at: https://www.coinmetro.com/learning-lab/regulatory-sandboxes, (Accessed: 19 April 2026).

[43] McConville, M. Chui, W., H., ed., (2017). *Research methods for law.* Edinburgh University Press. Second Edition, pp. 1–18. Available at: https://edinburghuniversitypress.com/pub/media/resources/9781474404259_Research_Methods_for_Law_-_Introduction_and_Overview.pdf, (Accessed: 26 July 2025).

Chapter 2 traces the development of EU data protection law from Convention 108 and Directive 95/46/EC to the GDPR. It examines key CJEU judgments in order to clarify the legal meaning of personal data controllership. Chapter 3 analyses the Right to be Forgotten under Article 17 GDPR. The chapter shows that erasure may operate through limiting accessibility of personal data rather than requiring deletion of lawful content. Chapter 4 explains the technical structure of blockchain systems and the role of custodial and non-custodial wallet providers, identifying how personal data may arise through on-chain and off-chain processing. Chapter 5 develops the concept of effective forgetting as a functional interpretation of Article 17 GDPR in decentralised environments, and Chapter 6 concludes that Article 17 GDPR can remain effective in decentralised technological systems.

Findings

The regulation of data protection within decentralised technological environments presents a structural tension. The GDPR presupposes reversibility and alteration; blockchain systems prioritise permanent record-keeping, decentralised control, and transparent state transitions.

Against this background, this dissertation has examined *whether custodial and non-custodial wallet providers comply with Article 17 GDPR's right to erasure, and if so, does compliance require reconceptualising erasure as effective forgetting?*

At general level, this dissertation has found that while the GDPR and blockchain are not naturally compatible legal-technological models, they are not mutually exclusive. State and private actors remain bound to ensure the continued effectiveness of rights-protection even when operating or regulating within decentralised infrastructures. Accordingly, the GDPR can still operate within blockchain environments provided that its doctrinal concepts are adapted in a manner that reflects the technological and institutional context of processing.

The analysis confirms that while blockchain architectures challenge traditional assumptions underlying data erasure, the GDPR remains capable of operating within decentralised environments where its doctrinal concepts are interpreted in light of technological constraints affecting the persistence and accessibility of personal data.

At a more specific level, the analysis demonstrates that compliance with Article 17 GDPR is possible, but only if erasure is understood functionally rather than literally. Blockchain's technical immutability makes absolute deletion impossible once data reaches the ledger. However, this does not foreclose compliance. CJEU jurisprudence, particularly in search engine cases, treats erasure as achieved when data becomes functionally inaccessible: when linkability breaks down, when context no longer supports identification, when interfaces no longer surface the information. Wallet providers control substantial off-chain processing: user interfaces, metadata flows, key management systems, transaction indexing. Their influence over these layers gives them the means to operationalise effective forgetting even where on-chain deletion remains technically infeasible.

This dissertation concludes that the right to erasure under Article 17 GDPR is not rendered inapplicable by blockchain technology, but requires a functional interpretation adapted to decentralised environments. This approach demonstrates that EU data protection law can remain operational and effective even where technological architectures constrain traditional models of deletion.

THREE OVERARCHING CONCLUSIONS

First, the GDPR is not inherently incompatible with blockchain technology. Although immutability prevents literal erasure, the GDPR's emphasis on user autonomy, proportionality, and contextual interpretation allows for a functional approach to the right to erasure. Regulatory incompatibility is not structurally predetermined; it depends on how the GDPR is interpreted and applied. CJEU jurisprudence supports this functional reading, though whether regulators will accept it for blockchain contexts remains to be tested through enforcement and litigation.

Second, blockchain wallet providers are central to operationalising Article 17. They are the points at which personal data becomes organised, structured, and mediated. They determine how much off-chain data is collected, how information is displayed to users, and how transactions are transmitted. Their proximity to users, their institutional identifiability, and their influence over data flows make them the most viable governance actors within otherwise decentralised ecosystems. This positioning gives them both the capacity and the responsibility to implement effective forgetting mechanisms.

Third, effective forgetting should be recognised as the appropriate compliance standard for Article 17 in decentralised environments. This dissertation has formulated effective forgetting as a standard sensitive to system architecture and operationalised it through a concrete framework for wallet providers. This constitutes an original contribution to data-protection scholarship and blockchain governance debates. It offers a principled means of reconciling legal expectations with technical constraints. It restores user autonomy not by altering the ledger itself, but by reshaping the informational conditions through which the ledger is experienced and interpreted. It is consistent with CJEU jurisprudence on functional erasure, respects the technological logic of distributed systems, and provides a practical model that regulators and industry actors can adopt.

This dissertation does not conclude that the concept of effective forgetting resolves all tensions between privacy and decentralisation. Rather, this research finds that the right to erasure can remain workable and normatively meaningful when interpreted through a model that prioritises functional outcomes, namely, the practical inaccessibility of personal data, instead of literal deletion. The broader implication is that data-protection law must continue to develop through sustained dialogue between legal doctrine and technical design. Technical architectures influence the extent to which legal rights can be realised in practice, just as legal norms and regulatory expectations shape the trajectory of technological development.

The demand for legal and technological communication is growing as blockchain systems spread and take on more intricate social and economic roles. The practical impacts that suppression mechanisms are supposed to give should be evaluated empirically in future research. It should also investigate whether decentralised governance mechanisms may internalise fundamental rights without outside legal pressure, as well as how courts handle effective forgetfulness within judicial reasoning. In addition to demonstrating that privacy protection in decentralised contexts is not only feasible but also essential if technological progress is to continue to be compatible with individual autonomy and constitutional rights, this dissertation offers the conceptual and analytical framework for that investigation.

The conceptual and analytical framework for that work is provided by this dissertation, which shows that privacy protection in decentralised systems is not only feasible but also necessary to guarantee that technological innovation does not compromise individual autonomy and constitutional rights under EU data protection law.

UNIVERSITY AND NATIONAL LIBRARY
UNIVERSITY OF DEBRECEN
H-4002 Egyetem tér 1, Debrecen
Phone: +3652/410-443, email: publikaciok@lib.unideb.hu

Registry number: DEENK/222/2026.PL
Subject: PhD Publication List

Candidate: Mariam Pilishvili
Doctoral School: Géza Marton Doctoral School of Legal Studies
MTMT ID: 10085445

List of publications related to the dissertation

Articles, studies (7)

1. **Pilishvili, M.**: How Schrems II Judgment Affected The Personal Data Flow Between The European Union and Third Countries?
   Public goods & governance. *10* (1), 21-28, 2025. ISSN: 2498-6453.
   DOI: http://dx.doi.org/10.21868/PGnG.2025.1.2.

   Level of HAS Committee on Legal and Political Sciences: C

2. **Pilishvili, M.**: Permacrisis: blockchain's plan to fix the normative challenges in EU data protection law.
   Jog, állam, politika. *17* (3), 81-92, 2025. ISSN: 2060-4580.
   DOI: http://dx.doi.org/10.58528/JAP.2025.17-3.81

   Level of HAS Committee on Legal and Political Sciences: A

3. **Pilishvili, M.**: Regulatory Ghosting: How Decentralized Platforms Evade GDPR Accountability.
   Lex ET Scientia International Journal. *32* (2), 61-77, 2025. ISSN: 2066-1886.

4. **Pilishvili, M.**: The PNR Directive: An Essential Security Mechanism for the EU or a Tool for the Breach of Personal Data and the Private Life of Individuals?
   Public goods & governance. *9* (1), 84-96, 2024. ISSN: 2498-6453.
   DOI: http://dx.doi.org/10.21868/PGnG.2024.1.5.

   Level of HAS Committee on Legal and Political Sciences: C

5. **Pilishvili, M.**: Cookie Consent through the Case Planet49.
   In: Law in Times of Crisis : Selected doctoral studies / Bándi Gyula, Pogácsás Anett, Pázmány Press, Budapest, 188-197, 2023, (Doktorandusz tanulmányok, ISSN 2064-4078 ; 7) ISBN: 9789633084656

6. Takašvili, S., **Pilishvili, M.**, Bendeliani, A.: Legal Personality of a Foreign Company's Branch in Georgian Court Practice.
   Kavkasiis Universitetis prop'esor mascavlebelt'a samec'niero šromebis krebuli. *2022*, 26-31, 2022. ISSN: 1987-8869.

UNIVERSITY AND NATIONAL LIBRARY
UNIVERSITY OF DEBRECEN
H-4002 Egyetem tér 1, Debrecen
Phone: +3652/410-443, email: publikaciok@lib.unideb.hu

7. **Pilishvili, M.**: Multinational Corporations as a Primary Players in the Global Economy and Issues of Protection of Personal Data.
In: Additional Learning Materials for Study Course in Business Law. Ed.: Tengiz Taktakishvili, Georgian Natonal University, Tibilisi, 136-147, 2022.

By the directives of HAS Committee on Legal and Political Sciences:
Publications in periodicals level „A": 1, related to the dissertation: 1.
Publications in periodicals level „C": 2, related to the dissertation: 2.

The Candidate's publication data submitted to the Tudóstér have been validated by DEENK on the basis of the Journal Citation Report (Impact Factor) database.

24 April, 2026

DEBRECENI EGYETEM Egyetemi és Nemzeti Könyvtár