REGULATORY GHOSTING: HOW DECENTRALIZED PLATFORMS EVADE GDPR ACCOUNTABILITY

Mariam PILISHVILI (*)

Abstract

The rise of decentralized financial technologies has created serious friction with existing data protection frameworks. While tools like non-custodial wallets are often marketed as enhancing privacy and user control, their real-world operation tells a more troubling story. This paper examines the 2023 Atomic Wallet breach, which resulted in the theft of over $100 million in user assets[1], as a case study in GDPR enforcement failure. Despite Atomic Wallet's public claim that it engaged in minimal data processing, its prior registration in Estonia[2] and ongoing targeting of EU users brought it squarely within the GDPR's extraterritorial reach under Article 3(2). The platform's collection of IP addresses, device identifiers, and behavioral metadata clearly falls under the definition of personal data, as clarified by the Court of Justice in Breyer v Germany (C-582/14). Its failure to notify affected users or supervisory authorities likely breached Articles 33 and 34. What makes this case especially revealing is not just the breach itself, but how easily the platform evaded responsibility. By dissolving its legal presence in the EU while continuing to operate, Atomic Wallet exposed a structural weakness in GDPR enforcement. The paper concludes by advocating for more robust jurisdictional and enforcement mechanisms to uphold data protection standards in decentralized finance.

Keywords: *GDPR, Data Protection, Crypto Regulation, Blockchain, Atomic Wallet, Decentralization, EU Law, Cybersecurity*

1. Introduction

Decentralized finance didn't just challenge traditional regulation, it bypassed it. As De Filippi and Wright[1] argue, existing legal tools were never designed for systems without a center. These platforms promise user autonomy and privacy. Yet they simultaneously disrupt established models of legal accountability in ways that financial oversight mechanisms cannot address[2]. The 2023 Atomic Wallet breach exemplifies this

(*) PhD Candidate, Géza Marton Doctoral School of Legal Studies, University of Debrecen (e-mail mariampilishvilii@gmail.com).

[1] Partz, H., *Atomic Wallet faces lawsuit over $100M crypto hack losses: Report*. Cointelegraph, 2023, Available at: https://cointelegraph.com/news/crypto-atomic-wallet-faces-class-action-over-100m-crypto-hack-losses, (Accessed: 11 October 2025).

[2] Wright, E., *2M of Suspicious Deposits Frozen on Centralised Exchanges*. Atomic Wallet, Academy Sources, 2025. Available at: https://atomicwallet.io/blog/articles/2m-of-suspicious-deposits-frozen-on-centralised-exchanges, (Accessed: 11 October 2025).

[1] De Filippi, P., Wright, A., *Blockchain and the Law: The Rule of Code*. Cambridge, MA: Harvard University Press, 2018.

[2] Finck, M., *Automated Decision-Making and Administrative Law*. Forthcoming, P. Cane et al. (eds), Oxford Handbook of Comparative Administrative Law, Oxford, Oxford University Press, 2019, Max Planck Institute for Innovation & Competition Research Paper No. 19-10, Available at SSRN: https://ssrn.com/abstract=3433684, (Accessed: 11 October 2025).

regulatory vacuum. Over $100 million in user assets vanished[3]. Affected users found no clear avenues for redress. Supervisory oversight was absent. No enforcement body intervened. This represents a fundamental breakdown of consumer protection in the digital age.

Contrary to prevailing assumptions about decentralized systems, the breach reveals how technical robustness and user control can actually undermine legal protections. When platforms operate outside traditional institutional boundaries, they avoid jurisdictional oversight entirely[4]. The immutable nature of blockchain records directly conflicts with GDPR provisions like the right to erasure, creating inherent compliance tensions[5].

Atomic Wallet's regulatory strategy was straightforward: claim non-involvement. The platform marketed itself as a non-custodial service, asserting it neither stored user funds nor processed personal data. This positioning supposedly shielded it from conventional financial and data protection obligations[6]. The reality proved far more complex.

Recent empirical research challenges the "hands-off" narrative that many cryptocurrency wallets promote. These platforms routinely engage in extensive user data processing, despite technical architectures that appear decentralized[7]. This suggests a structural flaw in how we conceptualize data control in distributed systems.

The jurisdictional implications are particularly troubling. Atomic Wallet was incorporated in Estonia and specifically targeted European users through marketing campaigns. This triggered GDPR's extraterritorial provisions under Article 3(2), which apply regardless of a company's physical location[8]. The regulation was designed to prevent exactly this kind of circumvention. The subsequent dissolution of Atomic Wallet's Estonian entity, while continuing EU operations, appears to constitute deliberate regulatory avoidance.

2. Legal Framework and Jurisdictional Challenges

Article 3(2) extends GDPR's scope beyond EU borders to prevent companies from circumventing data protection obligations through geographic arbitrage. The provision applies to any entity offering

[3] Chainalysis, *The 2023 Crypto Crime Report*, 2023, Chainalysis Inc, available at https://www.chainalysis.com/blog/2023-crypto-crime-report-introduction/ and Bizga, A., *Atomic Wallet Users Lose $35 Million Worth of Crypto Assets in Weekend Hack. Bitdefender*, 2023, available at: https://www.bitdefender.com/en-au/blog/hotforsecurity/atomic-wallet-users-lose-35-million-worth-of-crypto-assets-in-weekend-hack.

[4] Reyes, C. L., *Moving beyond Bitcoin to an endogenous theory of decentralized ledger technology regulation*. Villanova Law Review, 61(1), 2017, 191-234. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3048104, (Accessed: 11 October 2025).

[5] Berberich, M., Steiner, M., *Blockchain technology and the GDPR: How to reconcile privacy with distributed ledgers?* European Data Protection Law Review, 2(4), 2016, pp.422–426. Available at: https://edpl.lexxion.eu/article/edpl/2016/3/21, (Accessed: 11 October 2025).

[6] Zetzsche, D. A., Buckley, R. P., Arner, D. W., Föhr, L., Decentralized finance (DeFi). Journal of Financial Regulation, 6(2), 172-203, 2020. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3539194, (Accessed: 11 October 2025).

[7] Houy, S., Schmid, P., Bartel, A., *Security aspects of cryptocurrency wallets—a systematic literature review*. ACM Computing Surveys, 56(1), 2023, 1-31. Available at: https://dl.acm.org/doi/full/10.1145/3596906, (Accessed: 11 October 2025).

[8] Lynskey, O., *The Foundations of EU Data Protection Law*. Oxford University Press, 2015.

goods or services to EU data subjects, regardless of establishment location[9].

Applying this framework to decentralized platforms reveals immediate conceptual problems. Traditional interpretations of "offering goods or services" assume identifiable legal entities and structured commercial relationships. Decentralized platforms operate through diffuse governance arrangements. They present themselves as technical intermediaries rather than data controllers[10]. This ambiguity enables forms of regulatory avoidance that GDPR's drafters did not fully anticipate.

The personal data definition under Article 4(1) encompasses any information that can directly or indirectly identify an individual. This includes IP addresses, device identifiers, and transactional metadata, elements that cryptocurrency wallets routinely process[11]. The Breyer decision[12] clarified that dynamic IP addresses constitute personal data when linkable to individuals through additional information.

This interpretation has profound implications for cryptocurrency platforms. Blockchain addresses, while pseudonymous, can often be re-identified using deanonymization techniques[13]. Transaction timing, network metadata, and behavioral patterns form identifiable data profiles that clearly fall within GDPR's scope. The "pseudonymous" label provides no regulatory shelter.

Atomic Wallet's data processing practices contradict its minimalist claims. The platform collected IP addresses for transaction broadcasting, device identifiers for software updates, and behavioral data for risk mitigation. Its privacy policy explicitly acknowledged these practices before recent amendments. Such activities constitute personal data processing under EU law.

Article 32 requires controllers to implement appropriate security measures. The breach's magnitude, affecting thousands of users with losses exceeding $100 million, raises serious questions about security

[9] Kuner, C., *Reality and illusion in EU data transfer regulation post-Schrems.* German Law Journal, 18, 2017, pp.881–918. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2732346, (Accessed: 11 October 2025); Purtova, N., *The law of everything: Broad concept of personal data and future of EU data protection law*. Law, Innovation and Technology, 10(1), 2018, 40-81. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3036355, (Accessed: 11 October 2025).

[10] Walch, A., The path of the blockchain lexicon (and the law). Review of Banking and Financial Law, 36(2), 2017, 713-765. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2940335, (Accessed: 11 October 2025).

[11] Politou, E., Alepis, E., Patsakis, C., *Forgetting personal data and revoking consent under the GDPR.* Journal of Cybersecurity, 4(1), 2019, tyy001. Available at: https://academic.oup.com/cybersecurity/article/4/1/tyy001/4954056?login=false, (Accessed: 11 October 2025).

[12] Court of Justice of the European Union (2016). *Patrick Breyer v Bundesrepublik Deutschland*. Case C-582/14. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62014CJ0582, (Accessed: 11 October 2025).

[13] Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., Savage, S., *A fistful of bitcoins: Characterizing payments among men with no names*. Proceedings of the 2013 Conference on Internet Measurement, 2013, pp. 127-140. Available at: https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf, (Accessed: 11 October 2025); Biryukov, A., Khovratovich, D., Pustogarov, I. *Deanonymisation of clients in bitcoin P2P network*. Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, 2014, pp. 15-29, Available at: https://www.researchgate.net/publication/262732923_Deanonymisation_of_Clients_in_Bitcoin_P2P_Network, (Accessed: 11 October 2025).

adequacy[14]. The breach notification requirements under Articles 33 and 34 are unambiguous. Controllers must inform supervisory authorities within 72 hours and notify affected individuals if the breach presents high risk to their rights and freedoms. Atomic Wallet satisfied neither obligation.

The platform's assertion that no personal data was involved is legally untenable. Even with encrypted private keys, the compromised metadata, transaction patterns, device information, behavioral data, qualifies as personal data under Article 4(1). The attackers' selective targeting of high-value accounts demonstrates access to individually identifiable information. The theft of $100 million clearly meets the "high risk" threshold under GDPR standards. Yet Atomic Wallet remained silent.

Worth noting, that victims from around the world mobilized to bring legal claims against Atomic Wallet. One notable attempt emerged in the United States, where plaintiffs filed a class-action lawsuit in Colorado. But in September 2024, U.S. District Judge Philip Brimmer dismissed the case outright, ruling that the Estonian-based company lacked sufficient ties to Colorado to establish jurisdiction[15]. The court emphasized that Atomic Wallet's software services did not deliberately target the state, nor did the company maintain a physical or economic presence. In the judge's words, without tangible connection software distribution alone does not create legal foothold.

A second legal push came from Europe, led by German lawyer Max Gutbord, who assessed the feasibility of pursuing claims against the company[16]. His investigation found that Atomic Wallet was likely insolvent or otherwise incapable of compensating users, and any legal effort would be met with aggressive resistance. Working with blockchain forensic experts, his team attempted to pressure the company into early settlement negotiations, but even victims with substantial claims failed to receive meaningful offers. Gutbord[17] concluded that the legal and financial realities made recovery impossible despite extensive effort.

These failed legal actions underscore the structural evasiveness of Atomic Wallet's architecture. By operating without fixed jurisdiction or legal entity alignment, the platform effectively shielded itself from both U.S. and European legal scrutiny. Victims were left with no remedy. The message is clear: in the absence of reform, decentralized platforms can externalize harm and sidestep accountability with alarming ease.

3. Methodology

This study employs doctrinal legal research methodology, examining statutory

[14] Choo K. K. R., *Cryptocurrency and virtual currency: Corruption and money laundering risks*, in Handbook of Digital Currency, 2015, pp. 283-307, Academic Press. Available at: https://www.researchgate.net/publication/282742025_Cryptocurrency_and_Virtual_Currency_Corruption_and_Money_LaunderingTerrorism_Financing_Risks, (Accessed: 11 October 2025).

[15] Dickinson v. Atomic Wallet et al., No. 1:23-cv-02031 (D. Colo. Sept. 10, 2024). Available at: https://www.govinfo.gov/content/pkg/USCOURTS-cod-1_23-cv-01582/pdf/USCOURTS-cod-1_23-cv-01582-1.pdf, (Accessed: 11 October 2025).

[16] Partz, H., *Atomic Wallet faces lawsuit over $100M crypto hack losses: Report*. Cointelegraph, 2023, Available at: https://cointelegraph.com/news/crypto-atomic-wallet-faces-class-action-over-100m-crypto-hack-losses, (Accessed: 11 October 2025).

[17] Personal communication with author, October 2024.

instruments, judicial decisions, and regulatory texts to evaluate GDPR applicability to decentralized financial technologies. The analysis combines traditional black-letter legal analysis with socio-legal insights to account for the interplay between normative structures and blockchain technology's technical features.

Primary materials include the GDPR text, European Data Protection Board guidance, Court of Justice case law, and relevant national instruments. These are supplemented by peer-reviewed articles, legal treatises, and policy reports from institutions specializing in data protection and financial regulation.

4. The Atomic Wallet Breach: Technical Realities vs. Legal Claims

The June 2023 breach exposed a disconnect between Atomic Wallet's marketed non-custodial architecture and operational realities revealed by the attack. Although the company claimed it held neither user data nor funds, the sophistication of the breach indicates that substantial user information was accessible to attackers.

Independent analysts attributed the incident to the Lazarus Group, a North Korea-linked entity known for advanced cryptocurrency attacks[18]. The breach didn't exploit a single vulnerability. Instead, it reflected knowledge of user-specific transaction behaviors and asset values, suggesting access to user-level data inconsistent with claims of minimal processing[19].

Technical analysis undermines the platform's non-custodial framing. High-value accounts were systematically prioritized. This implies attackers had access to stored user profiles or behavioral data (C-582/14[20]. The temporal alignment with peak transaction periods indicates user behavior was being monitored, an activity qualifying as personal data processing under GDPR.

Atomic Wallet's public response lacked transparency. Initially, the company claimed only a small number of users were affected. Later, it conceded to far broader impact. It attributed the breach to unspecified "infrastructure issues" and insisted no personal data was compromised, despite substantial evidence suggesting otherwise.

The company's broader regulatory posture complicates matters. Atomic Wallet's dissolution of its Estonian legal entity while continuing to serve EU users exemplifies "regulatory arbitrage"[21]. This maneuver allowed EU market operation while sidestepping regulatory obligations.

[18] Chainalysis, *The 2023 Crypto Crime Report*. Chainalysis Inc, available at https://www.chainalysis.com/blog/2023-crypto-crime-report-introduction/, 2023 (Accessed: 11 October 2025).

[19] Conti, M., Kumar, E.S., Lal, C., *A survey on security and privacy issues of Bitcoin*. IEEE Communications Surveys & Tutorials, 20(4), 2018, pp.3416–3452. Available at: https://www.researchgate.net/publication/317356750_A_Survey_on_Security_and_Privacy_Issues_of_Bitcoin, (Accessed: 11 October 2025).

[20] European Data Protection Board (EDPB), *Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility-related applications*, adopted 28 January 2020. Available at: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012020-processing-personal-data-context_en, (Accessed: 11 October 2025).

[21] Avgouleas, E., Kiayias, A., *The promise of blockchain technology for global securities and derivatives markets*, European Business Organization Law Review, 20(1), 2019, 81-110. Available at:

https://www.researchgate.net/publication/331415256_The_Promise_of_Blockchain_Technology_for_Global_Securities_and_Derivatives_Markets_The_New_Financial_Ecosystem_and_the_'Holy_Grail'_of_Systemic_Risk_Containment, (Accessed: 11 October 2025).

Such cross-jurisdictional structuring exploits gaps between legal systems and weakens the EU's capacity for coordinated enforcement, a structural vulnerability highlighted in Ferran's analysis of post-crisis regulatory reforms[22].

This tactic highlights a key limitation in GDPR's architecture: its reliance on identifiable legal entities for enforcement. When such presence is absent or deliberately removed, supervisory authorities face significant obstacles in initiating investigations or imposing sanctions. This creates what Finck describes as a "regulatory void."

Years after the incident, users still lack basic information about the breach's scope, compromised data nature, or remediation measures. No formal audit has been published. No communication has been made to EU supervisory authorities. This suggests that Atomic Wallet's stated commitment to data minimization served primarily as branding rather than meaningful legal framework.

5. The Enforcement Vacuum: Why Current Mechanisms Fail

The Atomic Wallet case illustrates structural deficiencies in GDPR's enforcement framework[23]. Despite clear violations of breach notification duties and substantive obligations, no enforcement action has followed. This absence highlights the limitations of applying conventional enforcement models to platforms that are both decentralized and strategically evasive.

The case exposes multiple enforcement gaps. First, the 72-hour breach notification requirement becomes unenforceable when companies avoid supervisory scrutiny by lacking registered EU representatives. Second, the right to lodge complaints loses meaning in the absence of known data controllers. Third, administrative fines cease to deter when entities have no attachable assets or enforceable legal presence within the EU.

Existing cross-border cooperation tools were designed with traditional corporate actors in mind, firms with physical infrastructure and centralized operations[24]. Mutual legal assistance frameworks assume companies operate within coordinated legal jurisdictions. These assumptions are challenged by digital platforms employing offshore registrations and governance structures that intentionally obscure accountability.

For affected data subjects, this enforcement vacuum has tangible consequences. Users had no clear channel to file complaints, no identified entity against whom to seek redress, and no meaningful disclosure of what personal data was compromised. Without platform engagement, users are effectively excluded from the rights GDPR is meant to guarantee.

This regulatory inaction risks normalizing non-compliance. When companies face no material consequences

[22] Ferran, E., *Crisis-driven regulatory reform: Where in the world is the EU going?* In E. Ferran, N. Moloney, J. G. Hill, & J. C. Coffee (Eds.), The regulatory aftermath of the global financial crisis, 2012, pp. 1–64, Cambridge University Press. Available at: https://assets.cambridge.org/97811070/24595/excerpt/9781107024595_excerpt.pdf, (Accessed: 11 October 2025).

[23] Lynskey, O., *The Foundations of EU Data Protection Law*. Oxford University Press, 2015; Kuner, C., *Reality and illusion in EU data transfer regulation post-Schrems.* German Law Journal, 18, 2017, pp.881–918. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2732346, (Accessed: 11 October 2025).

[24] Bradford, A., *The Brussels Effect: How the European Union Rules the World*. Oxford University Press, 2020.

for avoiding GDPR obligations, it creates incentive structures that reward opacity. Compliant firms are placed at competitive disadvantage, while those sidestepping legal frameworks operate with reduced risk and lower cost.

6. Intermediary Accountability under the Digital Services Act

The European Union's Digital Services Act (DSA), adopted in 2022, represents the most significant recalibration of intermediary liability since the 2000 E-Commerce Directive (European Parliament and Council, 2000; European Parliament and Council, 2022). While primarily focused on illegal content, advertising transparency, and disinformation, the DSA establishes a general accountability framework for online intermediaries and platforms (e.g., marketplaces, social networks, app stores) that is relevant by functional analogy to crypto 'technical intermediaries.'[25] Although originally conceived to govern platforms hosting user-generated content, the DSA's broader regulatory logic extends to digital intermediaries whose technical design enables or conceals data flows relevant to users' rights and regulatory oversight[26]. Its relevance to the Atomic Wallet case lies not in categorical inclusion but in functional analogy: Atomic Wallet operated as a technical intermediary by mediating access between users and blockchain networks while disclaiming responsibility for both.

Under the DSA, such disclaimers would not absolve a platform from transparency and traceability obligations[27]. Articles 11 and 13 impose duties on providers to designate a legal representative within the Union and to ensure the accessibility of contact information for supervisory cooperation (DSA Articles 11 and 13). These provisions directly counter the kind of jurisdictional disappearance practiced by Atomic Wallet following the dissolution of its Estonian entity (Willman et al., 2024). Where the GDPR struggled to enforce accountability in the absence of establishment, the DSA seeks to institutionalize reachability as a precondition for lawful operation within the internal market.

By embedding legal responsibility into the technical and administrative architecture of intermediaries, the DSA narrows the space for regulatory ghosting[28].

---

[25] Under DSA Art. 3(g), 'intermediary services' comprise mere conduit, caching, and hosting. Wallets are not classic 'hosting' services; my analysis uses the DSA's accountability logic functionally rather than categorically.

[26] Sagar, S. and Hoffmann, T., Inter*mediary Liability in the EU Digital Common Market—From the E-Commerce Directive to the Digital Services Ac*t. IDP. Internet, Law and Politics, No. 34 (October) 2021, ISSN 1699-8154. Available at: https://www.researchgate.net/publication/357140122_Intermediary_Liability_in_the_EU_Digital_Common_Market, (Accessed: 11 October 2025). Kaushal, R., van de Kerkhof, J., Goanta, C., Spanakis, G. and Iamnitchi, A., *Automated Transparency: A Legal and Empirical Analysis of the Digital Services Act Transparency Database*. arXiv preprint arXiv:2404.02894 [cs.CY], 2024, Available at: https://arxiv.org/abs/2404.02894?, (Accessed: 11 October 2025).

[27] Wolters, P., Zuiderveen Borgesius, F., *The EU Digital Services Act: what does it mean for online advertising and adtech?* International Journal of Law and Information Technology, 33, eaaf004. doi: 10.1093/ijlit/eaaf004, 2025. Available at: https://academic.oup.com/ijlit/article/doi/10.1093/ijlit/eaaf004/8133991, (Accessed: 11 October 2025).

[28] Turillazzi, A., Taddeo, M., Floridi, L., Casolari, F., T*he Digital Services Act: an analysis of its ethical, legal, and social implications*. SSRN Electronic Journal, 2022. Available at:

As established in the preceding section, the DSA operationalizes jurisdictional reachability through concrete obligations such as the designation of contact points and legal representatives[29]. Building on that foundation, the Act's systemic risk and transparency framework signals a deeper transformation in EU digital governance; from a reactive, sanction-based model to one of continuous oversight and accountability by design[30]. Recent DSA enforcement actions against very large platforms over ad transparency and dark patterns underscore that these duties are being actively policed, strengthening the paper's claim that accountability can be engineered into platform governance[31]. While initially tailored to very large online platforms, these procedural mechanisms embody a regulatory logic that is functionally extensible to decentralized or hybrid intermediaries that process metadata, behavioral signals, or device identifiers[32].

Under this functional interpretation, entities like Atomic Wallet can no longer rely on decentralization as a shield against regulatory scrutiny. By framing such services as technical intermediaries that mediate risk and data flows within the Union, the DSA's governance rationale pierces the formal veil of decentralization, demanding ongoing traceability and transparency[33]. The absence of a legal representative or identifiable operational dependencies, central to Atomic Wallet's model, thus exemplifies the kind of opacity the DSA renders untenable for services targeting EU users[34].

In this broader sense, the DSA complements the GDPR not by replicating its substantive rights but by embedding its principle of accountability into institutional

https://www.researchgate.net/publication/357803324_The_Digital_Services_Act_An_Analysis_of_Its_Ethical_Legal_and_Social_Implications, (Accessed: 11 October 2025).

[29] (Willman et al., 2024).

[30] Leitão, M., Teles, G., Silva, S. D., and Associados, *Understanding the DSA: A Comprehensive Guide for Digital Operators*. Lisbon February, 2024, Available at: https://www.mlgts.pt/xms/files/site_2018/guias/2024/Understanding_the_DSA_-_A_comprehensive_guide_for_digital_operators.pdf, (Accessed: 11 October 2025); Tommasi, S., *The Risk of Discrimination in the Digital Market. From the Digital Services Act to the Future*. SpringerBriefs in Law, ISSN 2192-855X, 2023.

[31] Rankin, J., T*ikTok breached EU advertising transparency laws, commission says*. The Guardian, 15 May, 2025, Available at: https://www.theguardian.com/technology/2025/may/15/tiktok-breached-eu-advertising-transparency-laws-commission-says, (Accessed: 11 October 2025).

[32] Schwemer, S., F., *Digital Services Act: A reform of the e-Commerce Directive and much more*, 2022. Available at: https://www.researchgate.net/publication/363369108_Digital_Services_Act_A_reform_of_the_e-Commerce_Directive_and_much_more, (Accessed: 11 October 2025); Baistrocchi, P., *Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce*, Issue 1, Volume 19, 2003, Article 3, Santa Clara High Technology Law Journal. Available at:
https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1315&context=chtlj, (Accessed: 11 October 2025).

[33] Maetzler, A., Jokic, K., Mason, C., *The role of the legal representative under the Digital Services Act: Obligations for non-EU companies*. Lexology, 29 July 2024. Available at: https://www.lexology.com/library/detail.aspx?g=de93c3e5-8b87-45ea-a189-7ed05dac7571, (Accessed: 11 October 2025).

[34] Harcourt, A., *Brexit and the Digital Single Market*. Chapter 6. Platform Regulation and the Liability of Intermediaries, 2023, pp. 103–124, https://doi.org/10.1093/oso/9780192899378.003.0006.

architecture[35]. Where the GDPR defines what must be protected, the DSA determines how those protections are enforceable[36]. Together, they construct a dual regime in which technical configuration and jurisdictional presence become regulatory conditions rather than voluntary choices. This convergence reflects the EU's emerging model of digital governance: one that reconstitutes accountability at the level of function, ensuring that no intermediary, centralized or decentralized, can operate invisibly within the Union[37].

7. Lessons from Other Jurisdictions

Enforcement challenges exposed by the Atomic Wallet case are not unique to the European Union. However, several jurisdictions have adopted more assertive enforcement strategies that offer instructive models for EU reform.

In the United States, regulators such as the Department of Justice (DOJ) and Office of Foreign Assets Control (OFAC) have demonstrated a substance-over-form enforcement approach. Notably, the BitMEX case[38] led to criminal and civil charges for violating the Bank Secrecy Act[39], despite the platform's offshore registration[40]. Similarly, the sanctions against Tornado Cash[41], an ostensibly decentralized protocol, were premised on the Treasury's view that even decentralized entities can fall under U.S. jurisdiction when they facilitate illicit transactions or sanctions evasion[42].

In Singapore, the Payment Services Act 2019, administered by the Monetary Authority of Singapore (MAS), requires all crypto service providers to be licensed and

[35] Zanfir-Fortuna, G., Rovilos, V., *EU's Digital Services Act just became applicable: outlining ten key areas of interplay with the GDPR*. Future of Privacy Forum (Blog), 31 August 2023. Available at: https://fpf.org/blog/eus-digital-services-act-just-became-applicable-outlining-ten-key-areas-of-interplay-with-the-gdpr/, (Accessed: 11 October 2025).

[36] Celeste, E., Digital constitutionalism, *EU digital sovereignty ambitions and the role of the European Declaration on Digital Rights*, in Engel, A., Groussot, X. and Petursson, G.T. (eds.), *New Directions in Digitalisation: Perspectives from EU Competition Law and the Charter of Fundamental Rights*, Cham: Springer Nature Switzerland (European Union and its Neighbours in a Globalized World, vol. 13), 2025, pp. 255-273.

[37] *Idem.*

[38] U.S. Department of Justice, *Global Cryptocurrency Exchange BitMEX Fined $100 Million for Violating Bank Secrecy Act*. U.S. Attorney's Office, Southern District of New York, 2025. Available at: https://www.justice.gov/usao-sdny/pr/global-cryptocurrency-exchange-bitmex-fined-100-million-violating-bank-secrecy-act?, (Accessed: 11 October 2025).

[39] U.S. Department of Justice, *Founders of Cryptocurrency Exchange Plead Guilty to Bank Secrecy Act Violations*. U.S. Attorney's Office, Southern District of New York, 2022. Available at: https://www.justice.gov/usao-sdny/pr/founders-cryptocurrency-exchange-plead-guilty-bank-secrecy-act-violations?, (Accessed: 11 October 2025).

[40] Zetzsche, D. A., Buckley, R. P., Arner, D. W., Föhr, L., Decentralized finance (DeFi). Journal of Financial Regulation, 6(2), 172-203, 2020. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3539194, (Accessed: 11 October 2025).

[41] Egan, B.J., Evangelista, A.D., Fisch, E.J., Cannon, J., C*ourt Victory for Treasury and Indictment of Tornado Cash Founders Highlights AML and Sanctions Risks for DeFi Crypto Platforms*. Skadden, Arps, Slate, Meagher & Flom LLP, 2023. Available at: https://www.skadden.com/insights/publications/2023/09/court-victory-for-treasury-and-indictment, (Accessed: 11 October 2025).

[42] Gensler, G., *Remarks before the Aspen Security Forum.* U.S. Securities and Exchange Commission, 2022, Available at: https://www.sec.gov/news/speech/gensler-aspen-security-forum-2022, (Accessed: 11 October 2025).

to maintain a physical operational presence. As Avgouleas and Kiayias note in 2019[43], this legal framework reduces "regulatory ghosting" by anchoring compliance within territorial boundaries.

The United Kingdom, under the Financial Conduct Authority (FCA), enforces a robust regime for crypto-asset firms. Registration with the FCA is mandatory, and companies are subject to continuous anti-money laundering (AML) scrutiny. The FCA also maintains a public register of approved firms, fostering both transparency and accountability[44].

These jurisdictions share essential features lacking in the EU framework: mandatory registration, domestic accountability requirements, and enforcement grounded in economic substance rather than formal structure. Crucially, they treat decentralization as a technical configuration, not as a jurisdictional shield[45].

By contrast, enforcement in the EU remains highly dependent on voluntary cooperation and the presence of a legal entity within EU territory. As Kaminski and Malgieri[46] argue, this leaves a significant enforcement vacuum, particularly when platforms dissolve their EU presence or operate via opaque corporate structures. This disparity fosters the perception that GDPR violations carry lower legal risk within the EU, thus undermining the regulation's deterrent force in global digital governance.

8. Proposed Reforms: Strengthening Enforcement Against Decentralized Platforms

The Atomic Wallet case illustrates that existing GDPR enforcement mechanisms are ill-equipped to address decentralized platforms structured to avoid regulatory oversight. The following proposals address specific gaps exposed by this case.

- Strengthening EU Representation Requirements

Currently, Article 27 of the GDPR requires non-EU data controllers to appoint a representative within the Union. However, this requirement does not apply to companies that dissolve their EU entities after prior establishment. This loophole has been exploited by platforms like Atomic

[43] Avgouleas, E., Kiayias, A., *The promise of blockchain technology for global securities and derivatives markets*, European Business Organization Law Review, 20(1), 2019, 81-110. Available at: https://www.researchgate.net/publication/331415256_The_Promise_of_Blockchain_Technology_for_Global_Securities_and_Derivatives_Markets_The_New_Financial_Ecosystem_and_the_'Holy_Grail'_of_Systemic_Risk_Containment, (Accessed: 11 October 2025).

[44] (FCA, 2023; see also Zetzsche, D. A., Buckley, R. P., Arner, D. W., Föhr, L., Decentralized finance (DeFi). Journal of Financial Regulation, 6(2), 172-203, 2020. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3539194, (Accessed: 11 October 2025).

[45] Finck, M., *Automated Decision-Making and Administrative Law*. Forthcoming, P. Cane et al. (eds), Oxford Handbook of Comparative Administrative Law, Oxford, Oxford University Press, 2019, Max Planck Institute for Innovation & Competition Research Paper No. 19-10, Available at SSRN: https://ssrn.com/abstract=3433684, (Accessed: 11 October 2025); Bacon, J., Michels, J., Millard, C., *Blockchain demystified: A technical and legal introduction to distributed and centralised ledgers*. Richmond Journal of Law & Technology, 25(1), 2018, pp.1–34. Available at: https://scholarship.richmond.edu/jolt/vol25/iss1/2/, (Accessed: 11 October 2025).

[46] Kaminski, M.E., Malgieri, G., Al*gorithmic impact assessments under the GDPR*. International Data Privacy Law, 11(1), 2021, pp.1–21. Available at: https://academic.oup.com/idpl/article/11/2/125/6024963, (Accessed: 11 October 2025).

Wallet. As Lynskey[47] and Kuner[48] emphasize, legal presence is essential for supervisory authority engagement. A revised Article 27 should close this gap by mandating that any platform targeting EU users or processing their data, regardless of incorporation status, maintain an EU-based representative with full legal capacity to respond to regulatory requests and complaints.

- Asset-Based Enforcement Powers

Decentralized platforms often hide behind fragmented jurisdictions and offshore asset holdings. Kaminski and Malgieri[49] have argued for enhancing the remedial reach of data protection enforcement. The GDPR must be paired with asset-freezing powers modeled on tools from EU financial law, such as those applied in AML enforcement under the 5th Anti-Money Laundering Directive[50]. Without financial levers, the threat of GDPR sanctions is illusory for actors who can simply vanish their operations.

- Technical Enforcement Mechanisms

Traditional enforcement assumes a territorial presence. Decentralized platforms challenge that foundation. As Finck[51] and Zetzsche et al.[52] point out, regulators should consider non-legal sanctions such as network-level restrictions or de-platforming mechanisms in cooperation with financial intermediaries. These measures raise legitimate concerns about proportionality and overreach, but in cases of sustained evasion, such technical sanctions may be the only way to enforce rights.

- Criminal Liability for Deliberate Evasion

Where regulatory evasion is intentional, administrative fines are insufficient. Reyes[53] has shown how crypto ecosystems exploit jurisdictional complexity to frustrate enforcement. Member States should criminalize systematic data protection avoidance, for example, through deliberate dissolution of legal entities, refusal to disclose data processing practices, or misrepresentation of decentralization.

These actions constitute regulatory sabotage and should be treated accordingly. Criminal liability would also unlock mutual legal assistance treaties (MLATs), enabling cooperation with third-country prosecutors and regulators.

---

[47] Lynskey, O., *The Foundations of EU Data Protection Law*. Oxford University Press, 2015.

[48] Kuner, C., *Reality and illusion in EU data transfer regulation post-Schrems.* German Law Journal, 18, 2017, pp.881–918. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2732346, (Accessed: 11 October 2025).

[49] Kaminski, M.E., Malgieri, G., A*lgorithmic impact assessments under the GDPR*. International Data Privacy Law, 11(1), 2021, pp.1–21. Available at: https://academic.oup.com/idpl/article/11/2/125/6024963, (Accessed: 11 October 2025).

[50] Directive (EU) 2018/843.

[51] Finck, M., *Automated Decision-Making and Administrative Law*. Forthcoming, P. Cane et al. (eds), Oxford Handbook of Comparative Administrative Law, Oxford, Oxford University Press, 2019, Max Planck Institute for Innovation & Competition Research Paper No. 19-10, Available at SSRN: https://ssrn.com/abstract=3433684, (Accessed: 11 October 2025).

[52] Zetzsche, D. A., Buckley, R. P., Arner, D. W., Föhr, L., Decentralized finance (DeFi). Journal of Financial Regulation, 6(2), 172-203, 2020. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3539194, (Accessed: 11 October 2025).

[53] Reyes, C. L., *Moving beyond Bitcoin to an endogenous theory of decentralized ledger technology regulation*. Villanova Law Review, 61(1), 2017, 191-234. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3048104, (Accessed: 11 October 2025).

9. Conclusion

The Atomic Wallet breach offers more than a cautionary tale; it reveals a structural flaw in the EU's current data protection enforcement framework. Despite clear evidence of violations under the GDPR, including the platform's failure to notify supervisory authorities or affected individuals after a massive breach of user assets and metadata, no regulatory body has taken action. This absence is not incidental. It reflects a systemic incapacity to enforce rules when platforms are designed to obscure jurisdictional anchors.

What Atomic Wallet exploited, and what others will likely emulate, is not a loophole but a governance blind spot. After dissolving its Estonian entity, the company continued targeting EU users without designating a representative or ensuring local oversight. In doing so, it bypassed Article 27's representation requirement, exploiting what Kuner[54] describes as the "territorial dependency" of EU enforcement architecture.

Such structuring is deliberate. As Zetzsche et al.[55] have shown, decentralized platforms increasingly engage in what they call "regulatory escape engineering," designing their operational and legal architectures to elude formal accountability. The GDPR was not crafted with these evasive realities in mind.

The idea that decentralized technical architecture exempts platforms from regulatory scrutiny is legally baseless. As the Court of Justice of the EU confirmed in Breyer v Germany[56], even IP addresses can constitute personal data if they can be linked to an individual. Wallets like Atomic collect device identifiers, behavioral analytics, and transaction patterns , all of which clearly fall under the GDPR's definition of personal data[57]. Technological novelty does not nullify legal responsibility.

This case also reveals a deeper legitimacy crisis. When non-compliant platforms face no consequences, while compliant ones shoulder the cost of regulation, the EU creates a perverse incentive structure. As Kaminski and Malgieri[58] argue, uneven enforcement not only erodes trust among data subjects, it distorts the entire compliance ecosystem.

Addressing this challenge requires more than rhetorical commitment. It demands concrete regulatory reform. First,

---

[54] Kuner, C., *Reality and illusion in EU data transfer regulation post-Schrems.* German Law Journal, 18, 2017, pp.881–918. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2732346, (Accessed: 11 October 2025).

[55] Zetzsche, D. A., Buckley, R. P., Arner, D. W., Föhr, L., Decentralized finance (DeFi). Journal of Financial Regulation, 6(2), 172-203, 2020. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3539194, (Accessed: 11 October 2025).

[56] Court of Justice of the European Union (2016). *Patrick Breyer v Bundesrepublik Deutschland*. Case C-582/14. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62014CJ0582, (Accessed: 11 October 2025).

[57] Politou, E., Alepis, E., Patsakis, C., *Forgetting personal data and revoking consent under the GDPR.* Journal of Cybersecurity, 4(1), 2019, tyy001. Available at: https://academic.oup.com/cybersecurity/article/4/1/tyy001/4954056?login=false, (Accessed: 11 October 2025). Berberich, M., Steiner, M., *Blockchain technology and the GDPR: How to reconcile privacy with distributed ledgers?* European Data Protection Law Review, 2(4), 2016, pp.422–426. Available at: https://edpl.lexxion.eu/article/edpl/2016/3/21, (Accessed: 11 October 2025).

[58] Kaminski, M.E., Malgieri, G., A*lgorithmic impact assessments under the GDPR*. International Data Privacy Law, 11(1), 2021, pp.1–21. Available at: https://academic.oup.com/idpl/article/11/2/125/6024963, (Accessed: 11 October 2025).

as Lynskey[59] emphasizes, platforms serving EU users should be required to maintain a legally responsible presence within the Union. Second, enforcement must be empowered with cross-border asset-freezing capabilities and harmonized investigative procedures, modeled after financial crime enforcement strategies such as those under the Fifth Anti-Money Laundering Directive. Third, regulatory bodies must offer clear, binding guidance on how GDPR applies to decentralized architectures, rather than relying on general principles.

Designations like "non-custodial" must not be allowed to substitute for legal substance. Reyes[60] and Finck[61] caution against allowing blockchain's decentralization mystique to obscure real-world data flows and control. Regulators should assess not how a platform describes itself, but how it operates, and whether it facilitates, processes, or profits from personal data.

If the EU wishes to preserve the integrity of its data protection model, it must act. The GDPR was rightly hailed as a gold standard. But gold tarnishes when it is not enforced. The Union's role as a leader in digital rights depends not just on principled design, but on practical capability. Without it, the rights enshrined in law risk becoming purely aspirational and unenforceable where they are needed most.

References

- Avgouleas, E., Kiayias, A., The promise of blockchain technology for global securities and derivatives markets. European Business Organization Law Review, 20(1), 2019, 81-110. Available at:https://www.researchgate.net/publication/331415256_The_Promise_of_
- Blockchain_Technology_for_Global_Securities_and_Derivatives_Markets_The_New_Financial_Ecosystem_and_the_'Holy_Grail'_of_Systemic_Risk_Containment, (Accessed: 11 October 2025).
- Bacon, J., Michels, J., Millard, C., *Blockchain demystified: A technical and legal introduction to distributed and centralised ledgers*. Richmond Journal of Law & Technology, 25(1), 2018, pp.1–34. Available at: https://scholarship.richmond.edu/jolt/vol25/iss1/2/, (Accessed: 11 October 2025).
  Baistrocchi, P., *Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce*. Issue 1, Volume 19, 2003, Article 3, Santa Clara High Technology Law Journal. Available at: https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1315&context=chtlj, (Accessed: 11 October 2025).
- Berberich, M., Steiner, M., *Blockchain technology and the GDPR: How to reconcile privacy with distributed ledgers?* European Data Protection Law Review, 2(4), 2016, pp.422–426. Available at: https://edpl.lexxion.eu/article/edpl/2016/3/21, (Accessed: 11 October 2025).
- Biryukov, A., Khovratovich, D., Pustogarov, I. *Deanonymisation of clients in bitcoin P2P network.* Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, 2014, pp. 15-29, Available at:

[59] Lynskey, O., *The Foundations of EU Data Protection Law*. Oxford University Press, 2015.

[60] Reyes, C. L., *Moving beyond Bitcoin to an endogenous theory of decentralized ledger technology regulation*. Villanova Law Review, 61(1), 2017, 191-234. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3048104, (Accessed: 11 October 2025).

[61] Finck, M., *Automated Decision-Making and Administrative Law*. Forthcoming, P. Cane et al. (eds), Oxford Handbook of Comparative Administrative Law, Oxford, Oxford University Press, 2019, Max Planck Institute for Innovation & Competition Research Paper No. 19-10, Available at SSRN: https://ssrn.com/abstract=3433684, (Accessed: 11 October 2025).

https://www.researchgate.net/publication/262732923_Deanonymisation_of_Clients_in_Bitcoin_P2P_Network, (Accessed: 11 October 2025).

- Bizga, A., *Atomic Wallet Users Lose $35 Million Worth of Crypto Assets in Weekend Hack*. Bitdefender, 2023, Available at: https://www.bitdefender.com/en-au/blog/hotforsecurity/atomic-wallet-users-lose-35-million-worth-of-crypto-assets-in-weekend-hack, (Accessed: 11 October 2025).
- Bradford, A., *The Brussels Effect: How the European Union Rules the World*. Oxford University Press, 2020.
- Celeste, E., *Digital constitutionalism, EU digital sovereignty ambitions and the role of the European Declaration on Digital Rights.* in Engel, A., Groussot, X. and Petursson, G.T. (eds.), *New Directions in Digitalisation: Perspectives from EU Competition Law and the Charter of Fundamental Rights*. Cham: Springer Nature Switzerland (European Union and its Neighbours in a Globalized World, vol. 13), 2025, pp. 255-273.
- Chainalysis, *The 2023 Crypto Crime Report*. Chainalysis Inc, available at https://www.chainalysis.com/blog/2023-crypto-crime-report-introduction/, 2023 (Accessed: 11 October 2025).
  Choo K. K. R., Cry*ptocurrency and virtual currency: Corruption and money laundering risk*s, in Handbook of Digital Currency, 2015, pp. 283-307, Academic Press. Available at: https://www.researchgate.net/publication/282742025_Cryptocurrency_and_Virtual_Currency_Corruption_and_Money_LaunderingTerrorism_Financing_Risks, (Accessed: 11 October 2025).
- Conti, M., Kumar, E.S., Lal, C., *A survey on security and privacy issues of Bitcoin*. IEEE Communications Surveys & Tutorials, 20(4), 2018, pp.3416–3452. Available at: https://www.researchgate.net/publication/317356750_A_Survey_on_Security_and_Privacy_Issues_of_Bitcoin, (Accessed: 11 October 2025).
- Court of Justice of the European Union (2016). *Patrick Breyer v Bundesrepublik Deutschland*. Case C-582/14. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62014CJ0582, (Accessed: 11 October 2025).
- De Filippi, P., Wright, A., *Blockchain and the Law: The Rule of Code*. Cambridge, MA: Harvard University Press, 2018.
- Dickinson v. Atomic Wallet et al., No. 1:23-cv-02031 (D. Colo. Sept. 10, 2024). Available at: https://www.govinfo.gov/content/pkg/USCOURTS-cod-1_23-cv-01582/pdf/USCOURTS-cod-1_23-cv-01582-1.pdf, (Accessed: 11 October 2025).
- Egan, B.J., Evangelista, A.D., Fisch, E.J., Cannon, J., C*ourt Victory for Treasury and Indictment of Tornado Cash Founders Highlights AML and Sanctions Risks for DeFi Crypto Platforms*. Skadden, Arps, Slate, Meagher & Flom LLP, 2023. Available at: https://www.skadden.com/insights/publications/2023/09/court-victory-for-treasury-and-indictment, (Accessed: 11 October 2025).
- European Data Protection Board (EDPB), *Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility-related applications*, adopted 28 January 2020. Available at: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012020-processing-personal-data-context_en, (Accessed: 11 October 2025).
- European Union, *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)*. Official Journal of the European Union, L 178, 17 July 2000. Available at: https://eur-lex.europa.eu/eli/dir/2000/31/oj/eng, (Accessed: 11 October 2025).

- European Union, *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act)*. Official Journal of the European Union, L 277, 2022. Available at: https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng (Accessed: 11 October 2025).
- Ferran, E., *Crisis-driven regulatory reform: Where in the world is the EU going?* In E. Ferran, N. Moloney, J. G. Hill, & J. C. Coffee (Eds.), The regulatory aftermath of the global financial crisis, 2012, pp. 1–64, Cambridge University Press. Available at: https://assets.cambridge.org/97811070/24595/excerpt/9781107024595_excerpt.pdf, (Accessed: 11 October 2025).
- Finck, M., *Blockchains and Data Protection in the European Union*. European Data Protection Law Review. Volume 4, Issue 1. pp. 17–35, 2018. Available at: DOI https://doi.org/10.21552/edpl/2018/1/6, (Accessed: 11 October 2025).
- Finck, M., *Automated Decision-Making and Administrative Law*. Forthcoming, P. Cane et al. (eds), Oxford Handbook of Comparative Administrative Law, Oxford, Oxford University Press, 2019, Max Planck Institute for Innovation & Competition Research Paper No. 19-10, Available at SSRN: https://ssrn.com/abstract=3433684, (Accessed: 11 October 2025).
- Gensler, G., *Remarks before the Aspen Security Forum*. U.S. Securities and Exchange Commission, 2022, Available at: https://www.sec.gov/news/speech/gensler-aspen-security-forum-2022, (Accessed: 11 October 2025).
- Harcourt, A., *Brexit and the Digital Single Market*. Chapter 6. Platform Regulation and the Liability of Intermediaries, 2023, pp. 103–124, https://doi.org/10.1093/oso/9780192899378.003.0006.
- Houy, S., Schmid, P., Bartel, A., *Security aspects of cryptocurrency wallets—a systematic literature review*. ACM Computing Surveys, 56(1), 2023, 1-31. Available at: https://dl.acm.org/doi/full/10.1145/3596906, (Accessed: 11 October 2025).
- Kaminski, M.E., Malgieri, G., Al*gorithmic impact assessments under the GDPR*. International Data Privacy Law, 11(1), 2021, pp.1–21. Available at: https://academic.oup.com/idpl/article/11/2/125/6024963, (Accessed: 11 October 2025).
- Kaushal, R., van de Kerkhof, J., Goanta, C., Spanakis, G. and Iamnitchi, A., *Automated Transparency: A Legal and Empirical Analysis of the Digital Services Act Transparency Database*. arXiv preprint arXiv:2404.02894 [cs.CY], 2024, Available at: https://arxiv.org/abs/2404.02894?, (Accessed: 11 October 2025).
- Koops, B.-J., *The trouble with European data protection law*. International Data Privacy Law, 4(4), 2014, pp.250–261. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2505692, (Accessed: 11 October 2025).
- Kuner, C., *Reality and illusion in EU data transfer regulation post-Schrems.* German Law Journal, 18, 2017, pp.881–918. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2732346, (Accessed: 11 October 2025).
- Kuner, C., Bygrave, L. A., Docksey, C., *The EU General Data Protection Regulation (GDPR): A Commentary/Update of Selected Articles* (May 4, 2021). Available at SSRN: https://ssrn.com/abstract=3839645 or http://dx.doi.org/10.2139/ssrn.3839645, (Accessed: 11 October 2025).
- Lynskey, O., *The Foundations of EU Data Protection Law*. Oxford University Press, 2015.
- Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., Savage, S., *A fistful of bitcoins: Characterizing payments among men with no names*. Proceedings of the

2013 Conference on Internet Measurement, 2013, pp. 127-140. Available at: https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf, (Accessed: 11 October 2025).

- Leitão, M., Teles, G., Silva, S. D., and Associados, *Understanding the DSA: A Comprehensive Guide for Digital Operators.* Lisbon February, 2024, Available at: https://www.mlgts.pt/xms/files/site_2018/guias/2024/Understanding_the_DSA_-_A_comprehensive_guide_for_digital_operators.pdf, (Accessed: 11 October 2025).
- Maetzler, A., Jokic, K., Mason, C., *The role of the legal representative under the Digital Services Act: Obligations for non-EU companies*. Lexology, 29 July 2024. Available at: https://www.lexology.com/library/detail.aspx?g=de93c3e5-8b87-45ea-a189-7ed05dac7571, (Accessed: 11 October 2025).
- Partz, H., *Atomic Wallet faces lawsuit over $100M crypto hack losses: Report*. Cointelegraph, 2023, Available at: https://cointelegraph.com/news/crypto-atomic-wallet-faces-class-action-over-100m-crypto-hack-losses, (Accessed: 11 October 2025).
- Politou, E., Alepis, E., Patsakis, C., *Forgetting personal data and revoking consent under the GDPR*. Journal of Cybersecurity, 4(1), 2019, tyy001. Available at: https://academic.oup.com/cybersecurity/article/4/1/tyy001/4954056?login=false, (Accessed: 11 October 2025).
- Purtova, N., *The law of everything: Broad concept of personal data and future of EU data protection law*. Law, Innovation and Technology, 10(1), 2018, 40-81. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3036355, (Accessed: 11 October 2025).
- Rankin, J., T*ikTok breached EU advertising transparency laws, commission says*. The Guardian, 15 May, 2025, Available at: https://www.theguardian.com/technology/2025/may/15/tiktok-breached-eu-advertising-transparency-laws-commission-says, (Accessed: 11 October 2025).
- Reyes, C. L., *Moving beyond Bitcoin to an endogenous theory of decentralized ledger technology regulation*. Villanova Law Review, 61(1), 2017, 191-234. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3048104, (Accessed: 11 October 2025).
- Sagar, S. and Hoffmann, T., Inter*mediary Liability in the EU Digital Common Market—From the E-Commerce Directive to the Digital Services A*ct. IDP. Internet, Law and Politics, No. 34 (October) 2021, ISSN 1699-8154. Available at: https://www.researchgate.net/publication/357140122_Intermediary_Liability_in_the_EU_Digital_Common_Market, (Accessed: 11 October 2025).
- Schwemer, S., F., *Digital Services Act: A reform of the e-Commerce Directive and much more*, 2022. Available at: https://www.researchgate.net/publication/363369108_Digital_Services_Act_A_reform_of_the_e-Commerce_Directive_and_much_more, (Accessed: 11 October 2025).
- Tommasi, S., *The Risk of Discrimination in the Digital Market. From the Digital Services Act to the Future*. SpringerBriefs in Law, ISSN 2192-855X, 2023.
  Turillazzi, A., Taddeo, M., Floridi, L., Casolari, F., T*he Digital Services Act: an analysis of its ethical, legal, and social implications*. SSRN Electronic Journal, 2022. Available at: https://www.researchgate.net/publication/357803324_The_Digital_Services_Act_An_Analysis_of_Its_Ethical_Legal_and_Social_Implications, (Accessed: 11 October 2025).
- U.S. Department of Justice, *Founders of Cryptocurrency Exchange Plead Guilty to Bank Secrecy Act Violations*. U.S. Attorney's Office, Southern District of New York, 2022. Available

at: https://www.justice.gov/usao-sdny/pr/founders-cryptocurrency-exchange-plead-guilty-bank-secrecy-act-violations?, (Accessed: 11 October 2025).

- U.S. Department of Justice, *Global Cryptocurrency Exchange BitMEX Fined $100 Million for Violating Bank Secrecy Act*. U.S. Attorney's Office, Southern District of New York, 2025. Available at: https://www.justice.gov/usao-sdny/pr/global-cryptocurrency-exchange-bitmex-fined-100-million-violating-bank-secrecy-act?, (Accessed: 11 October 2025).
- Walch, A., The path of the blockchain lexicon (and the law). Review of Banking and Financial Law, 36(2), 2017, 713-765. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2940335, (Accessed: 11 October 2025).
- Wilman, F., Kalėda, S.L., Loewenthal, P-J., *The EU Digital Services Act: A Commentary*. Oxford: IRL Press at Oxford University Press, 2024.
- Wolters, P., Zuiderveen Borgesius, F., *The EU Digital Services Act: what does it mean for online advertising and adtech?* International Journal of Law and Information Technology, 33, eaaf004. doi: 10.1093/ijlit/eaaf004, 2025. Available at: https://academic.oup.com/ijlit/article/doi/10.1093/ijlit/eaaf004/8133991, (Accessed: 11 October 2025).
- Wright, E., *2M of Suspicious Deposits Frozen on Centralised Exchanges*. Atomic Wallet, Academy Sources, 2025. Available at: https://atomicwallet.io/blog/articles/2m-of-suspicious-deposits-frozen-on-centralised-exchanges, (Accessed: 11 October 2025).
- Zanfir-Fortuna, G., Rovilos, V., *EU's Digital Services Act just became applicable: outlining ten key areas of interplay with the GDPR*. Future of Privacy Forum (Blog), 31 August 2023. Available at: https://fpf.org/blog/eus-digital-services-act-just-became-applicable-outlining-ten-key-areas-of-interplay-with-the-gdpr/, (Accessed: 11 October 2025).
- Zetzsche, D. A., Buckley, R. P., Arner, D. W., Föhr, L., Decentralized finance (DeFi). Journal of Financial Regulation, 6(2), 172-203, 2020. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3539194, (Accessed: 11 October 2025).