IRSHAD International Journal of Law and Policy | Volume: 3, Issue: 12
2025

The Principle of Technological Neutrality into Technological Resilience in an Era of Data Growth and Technology Diversification

Rodionov Andrey Aleksandrovich
Tashkent State University of Law

Abstract

The principle of technological neutrality has long served as a cornerstone of digital regulation, mandating that laws neither favor nor discriminate against specific technologies. However, the function of technology has shifted from facilitative to constitutive nature, particularly in crypto assets where technology is integral to creating virtual assets themselves, fundamentally challenging this regulatory paradigm. This article examines the inadequacy of strict technological neutrality when confronting emergent technologies including artificial intelligence, blockchain systems, and quantum computing. Drawing upon comparative analysis of regulatory frameworks across multiple jurisdictions, we propose the principle of technological resilience as a conceptual evolution that maintains non-discrimination imperatives whilst enabling targeted regulatory intervention. The EU AI Act's deviations from technology neutrality, including specific provisions for general-purpose AI models, significantly improved its scope and future-proofness, demonstrating that technology neutrality and future-proof regulation should not be treated synonymously. This research offers a four-pillar framework for technological resilience and assesses its applicability to Uzbekistan's emerging digital economy.

Keywords: Technological Neutrality, Technological Resilience, Artificial Intelligence Regulation, Blockchain Governance, Quantum Computing, Adaptive Legal Frameworks

APA Citation:

Rodionov, A. (2025). The Principle of Technological Neutrality into Technological Resilience in an Era of Data Growth and Technology Diversification. *International Journal of Law and Policy, 3* (12), 68-84. https://doi.org/10.59022/ijlp.469

I. Introduction

Technology-neutral regulation represents a popular slogan in European digital lawmaking, present in the European Commission's Better Regulation Toolbox and explicitly referenced in instruments such as the Digital Services Act and the General Data Protection Regulation (Shadikhodjaev, 2021). The principle emerged from pragmatic necessity: legislators sought to create durable frameworks capable of governing rapidly evolving technological landscapes without requiring constant amendment. The basic principle of neutrality mandates that the state should remain neutral towards technology when regulating, following four rationales including non-discrimination, functional equivalence, and future-proofing. Traditional justifications emphasized competitive fairness, ensuring regulation would not arbitrarily advantage incumbent technologies over innovative alternatives, whilst simultaneously protecting against premature obsolescence of legislative instruments.

However, this regulatory philosophy confronts unprecedented challenges from technologies that fundamentally differ from their predecessors. Technology's function in crypto assets is not facilitative but constitutive technology is an integral part of creating virtual assets and services, brought into being by the technology itself (Schlagwein et al., 2025). This ontological shift destabilizes the functional equivalence assumption underpinning technological neutrality. Contemporary challenges from quantum computing's cryptographic threats, artificial intelligence's opacity and autonomous decision-making capabilities, and blockchain's immutable architectures demonstrate that strict adherence to neutrality principles may paradoxically impede effective governance. The EU Artificial Intelligence Act came into force in August 2024 and is already falling behind, not considering AI agents whilst still wrestling with generative AI and foundation models. This regulatory lag exemplifies the pressing necessity for paradigmatic reconsideration of foundational regulatory principles governing technological innovation.

The primary objective of this research is to conceptualize technological resilience as a principled evolution of technological neutrality, specifically addressing governance challenges posed by artificial intelligence, blockchain systems, and quantum computing. We examine regulatory frameworks including NIST's FIPS 203 draft cross-referenced with regulatory mandates like the EU's Digital Operational Resilience Act to propose a risk-tiered migration framework for financial institutions. Our investigation addresses three fundamental research questions: Can the technological neutrality principle adapt to accommodate constitutive technologies without abandoning its non-discriminatory core? What legal mechanisms effectively support regulatory resilience whilst maintaining innovation incentives? How should jurisdictions, particularly developing digital economies like Uzbekistan, respond to these challenges?

The article proceeds systematically through five sections. Following this

introduction, we detail our comparative legal methodology examining regulatory approaches across multiple jurisdictions. The results section articulates the problem definition, causative factors, consequences, and our proposed solution through the technological resilience framework. Subsequently, we discuss the significance and limitations of our findings alongside future regulatory trends. We conclude by synthesizing key insights and emphasizing practical implications for legislative reform. Uzbekistan's digital transformation initiatives position the nation to adopt innovative regulatory approaches informed by international experience whilst addressing distinctive national circumstances. This research contributes conceptual foundations for such efforts, offering actionable guidance for policymakers navigating technological governance complexities.

II. Methodology

This investigation employs doctrinal legal analysis combined with comparative regulatory examination across multiple jurisdictions to develop the technological resilience framework. Our primary sources comprise legislative instruments, regulatory guidance documents, and judicial decisions from key jurisdictions including the European Union, United States, United Kingdom, and Singapore. We analyze regulatory benchmarks including the UK's National Quantum Strategy (2023), the US Executive Order on Quantum Computing (2022), and the EU's Cyber Resilience Act (2024) to identify best practices in encryption migration and systemic risk mitigation. Specific statutory provisions receive detailed examination: Article 36 of the EU Data Act (2023) establishing mandatory smart contract termination requirements, provisions within Regulation (EU) 2024/1689 laying down harmonized rules on artificial intelligence, and the General Data Protection Regulation requiring organizations to implement appropriate technical and organizational measures ensuring IT systems resilience. Secondary scholarly literature provides theoretical foundations, particularly works examining technology neutrality's conceptual underpinnings and practical limitations.

The research adopts an inductive methodology, examining specific technological challenges to derive general principles for regulatory resilience. We analyze three primary technological domains: quantum computing's threats to cryptographic infrastructures, artificial intelligence's opacity and autonomous characteristics, and blockchain's immutability conflicts with data protection regimes. Our comparative approach systematically evaluates regulatory responses across jurisdictions, identifying convergence points and divergent approaches. Case law analysis includes Ohio Telecom Association v. Federal Communications Commission (2025), wherein the Sixth Circuit held the FCC lacks authority to reinstate net neutrality following the Supreme Court's Loper Bright decision ending Chevron deference. We examine practical implementation initiatives including the Bank for International Settlements' Project Leap, wherein the Euro system Centre spearheads efforts to demonstrate how payment systems can be fortified against potential threats

posed by quantum computers. This investigation remains purely theoretical-analytical, eschewing empirical data collection through interviews or surveys. Instead, we synthesize insights from legislative texts, regulatory guidance, judicial reasoning, and academic commentary to construct a conceptual framework for technological resilience. The methodological approach facilitates systematic identification of regulatory patterns, assessment of their effectiveness addressing emergent technological challenges, and development of principled recommendations for legislative reform applicable across diverse jurisdictional contexts.

III. Results

A. The Inadequacy of Technological Neutrality

The technological neutrality principle confronts fundamental conceptual limitations when applied to contemporary digital technologies. Technology neutrality and future-proof regulation should not be treated synonymously, as strict adherence to neutrality may obscure the political choices and democratic agency essential for artificial intelligence regulation (Ojanen, 2025). Classical neutrality assumes functional equivalence between technologies: if two systems achieve identical outcomes, regulation should treat them identically regardless of underlying technical mechanisms. This assumption proves increasingly untenable. Artificial intelligence systems exhibit characteristics fundamentally distinguishing them from conventional software: opacity through deep learning architectures, autonomous decision-making capabilities, and unpredictable emergent behaviors resist straightforward regulatory categorization. Blockchain technologies present distinct challenges through architectural immutability conflicting with fundamental legal principles. Smart contracts store personal information, creating conflicts with global privacy regulations like GDPR and CCPA, as these laws often conflict with blockchain's transparency and immutability characteristics.

The European Court of Justice's interpretation of the “right to erasure” under Article 17 GDPR proves practically incompatible with blockchain's append-only data structures. Quantum computing introduces another dimension of disruption: quantum threats to SHA-256 hashing in Bitcoin, informed by Nakamoto's consensus model, demonstrate cryptographic vulnerabilities (Frantziou, 2014). Current asymmetric encryption systems including RSA and elliptic curve cryptography face existential threats from Shor's algorithm implementation on sufficiently powerful quantum computers. Regulatory fragmentation exacerbates these challenges. Regulations remain dichotomized with separate frameworks: the EU AI Act for artificial intelligence, Markets in Crypto-Assets for Web3, the Cybersecurity Act and Digital Operational Resilience Act for security. This fragmentation proves cumbersome for users and businesses whilst misaligning with actual product development, where solutions integrate multiple technologies subject to disparate regulatory regimes. Temporal mismatches compound these structural problems: computational power now doubles every six months rather than every two years, surpassing Moore's law, whilst

legislative cycles measure in years, creating widening regulatory gaps threatening legal certainty and effective governance.

B. Causative Factors: Why Neutrality Fails

Multiple converging factors explain technological neutrality's inadequacy for contemporary governance challenges. Technological convergence represents the foremost driver: quantum computing, artificial intelligence, blockchain, and cybersecurity are not developing in isolation but rather shaping each other, accelerating innovation and redefining foundations of trust, security, and digital transformation. Modern digital products rarely employ single technologies; instead, they integrate artificial intelligence for decision-making, blockchain for data integrity, and increasingly must prepare for quantum computing's cryptographic implications. Regulatory frameworks premised on technological separability prove structurally unsuited to this convergent reality. Innovation velocity constitutes another critical factor. Technology advances at the speed of light, having surpassed Moore's law with computational power doubling every six months rather than every two years (Markman et al., 2005).

Traditional legislative processes cannot maintain pace with such rapid technological evolution. By the time comprehensive regulatory frameworks receive parliamentary approval and enter force, the technological landscape may have fundamentally transformed. The philosophical foundations of technological neutrality emerged during the telecommunications and internet eras, when technologies primarily facilitated transactions in conventional assets and services. The United Nations Convention on the Use of Electronic Communications in International Contracts intended technological neutrality to provide coverage of all factual situations where information is generated, stored, or transmitted, irrespective of technology or medium. This approach assumed technologies remained tools rather than constitutive elements of regulated activities. Constitutional and institutional rigidities further impede effective adaptation. Traditional legislative amendment processes require extended deliberation, stakeholder consultation, and political compromise.

Whilst these procedural safeguards serve democratic legitimacy, they prove maladapted to governing rapidly evolving technologies. Legislative bodies frequently lack sufficient technical expertise to evaluate complex technological proposals effectively. Industry lobbying often emphasizes minimal regulatory intervention citing innovation concerns, whilst consumer protection advocates demand comprehensive oversight. Existing financial regulatory instruments remain technologically neutral, with the Digital Operational Resilience Act's provisions anchored in classical risk paradigms despite addressing digital operational risks. International coordination failures compound national-level challenges. China leads with approximately fifteen billion dollars in national quantum computing funding, followed by the European Union with seven point two billion dollars and the United Kingdom with two point

five billion dollars, yet an international regulatory architecture capable of keeping pace with this technical and institutional momentum remains underdeveloped. Divergent national approaches to artificial intelligence governance, cryptocurrency regulation, and data protection create regulatory arbitrage opportunities whilst impeding development of coherent global standards necessary for inherently transnational digital technologies.

C. Consequences: Manifestations of Regulatory Inadequacy

The failure of strict technological neutrality produces multiple adverse consequences across legal, economic, and security dimensions. Legal uncertainty pervades technology sectors subject to conflicting or ambiguous regulatory frameworks. Businesses cannot reliably predict compliance requirements when fundamental regulatory principles prove unsuited to technological realities they govern. The net neutrality regulatory oscillation exemplifies this dysfunction: the Federal Communications Commission's classification of internet services flip-flopped across administrations, with the Sixth Circuit's 2025 ruling holding that the FCC lacks authority to reinstate net neutrality following Loper Bright's termination of Chevron deference. This regulatory volatility undermines investment confidence and long-term planning whilst demonstrating how doctrinal principles like Chevron deference interacted with technological neutrality to produce incoherent governance. Security vulnerabilities represent particularly grave consequences of regulatory inadequacy.

Quantum computers have the potential to break many of the cryptographic algorithms that underpin current blockchain systems, posing a serious threat to their security and integrity. Without regulatory frameworks mandating cryptographic agility and post-quantum preparedness, critical infrastructures remain vulnerable to foreseeable technological disruption. Financial systems, healthcare databases, governmental communications, and blockchain-based assets all depend upon cryptographic protections facing obsolescence. Fundamental rights protections suffer erosion when regulatory frameworks cannot accommodate technological specificity. Smart contracts' compliance with regulations including GDPR and CCPA creates conflicts with blockchain transparency and immutability. The indefinite storage of personal data in immutable ledgers violates Article 17 GDPR's right to erasure. Courts interpreting technology-neutral data protection provisions struggle to apply principles developed for conventional databases to distributed ledger architectures. Competitive distortions emerge when early movers exploit regulatory grey areas unavailable to later entrants once authorities clarify ambiguous provisions. Innovation may suffer chilling effects: some argue the principle of technology neutrality has impeded regulation development, making lawmakers and regulators reluctant to define technology for regulatory purposes and create technology-specific regulation (Teo, 2025).

Jurisdictional fragmentation compounds these problems. Federal net neutrality rules remain repealed whilst state laws like those in California and Washington

continue in effect, creating patchwork regulatory landscapes where compliance requirements vary subnational. Systemic risks accumulate in inadequately regulated sectors. The Monetary Authority of Singapore's Financial Stability Review 2024 discusses the increasing relevance of emerging technologies including virtual assets, quantum technology, and artificial intelligence, emphasizing the importance of regulating virtual assets to mitigate risks associated with volatility and illicit activities. Consumer protection gaps and cross-border enforcement challenges round out the catalogue of consequences flowing from regulatory frameworks inadequately adapted to contemporary technological realities.

D. Proposed Solution: The Technological Resilience Principle

We propose technological resilience as a principled evolution of technological neutrality, addressing identified inadequacies whilst preserving core non-discrimination commitments. Technological resilience represents the ability of systems to continue operating and recover swiftly under adverse conditions, achieved not through after-the-fact bolt-on solutions but by fostering cultures enabling resilience to be built into systems from the beginning. This definition extends beyond technical system characteristics to encompass regulatory frameworks themselves, conceptualizing adaptive governance architectures maintaining effectiveness amid technological change. The technological resilience principle comprises four foundational pillars. First, adaptive regulation establishes a structured approach for continuous assessment and monitoring, integrating real-time insights with regular review of security controls, policies, and compliance requirements (Sullivan-Taylor, 2025).

Rather than static legislative instruments amended through protracted parliamentary processes, adaptive regulation employs sunset clauses, mandatory periodic reviews, and delegated regulatory authority enabling technical specifications to evolve alongside technological developments. Second, technology-specific modules supplement general principles with targeted provisions addressing unique characteristics of artificial intelligence, blockchain systems, quantum computing, and future technologies. This approach acknowledges that whilst non-discrimination remains valuable, meaningful regulation sometimes requires technology-specific interventions. Article 36 of the EU Data Act exemplifies this approach, establishing mandatory termination mechanisms specifically for smart contracts rather than attempting technology-neutral formulations incapable of addressing blockchain's immutability. Third, risk-tiered regulatory intensity calibrates oversight proportionally to identified hazards (Wu et al., 2025). The AI Act employs a risk-based approach wherein the level of regulation depends on risks involved with different uses of AI systems. High-risk applications including biometric identification or critical infrastructure control face stringent requirements, whilst low-risk applications encounter minimal regulatory burden.

This graduated approach balances innovation incentives against protection

imperatives more effectively than uniform requirements. Fourth, mandatory sunset and review clauses institutionalize regulatory adaptability. Legislative instruments include specific provisions requiring reassessment at defined intervals, ensuring frameworks do not ossify as technologies evolve. These reviews should incorporate technical expert input, stakeholder consultation, and empirical assessment of regulatory effectiveness and unintended consequences. Technological resilience thus moves beyond neutrality's rationales of non-discrimination, functional equivalence, and future-proofing towards active, adaptive governance recognizing that every solution integrates many technologies whilst each technology component has separate regulations, requiring comprehensive approaches. The principle incorporates continuous cycles guiding organizations through resilient solution implementation: assessing risks, developing strategies, testing, and monitoring as ongoing processes rather than one-time compliance exercises (Cheng et al., 2024).

E. Operationalizing Resilience

Effective implementation of technological resilience requires carefully designed legislative architectures, institutional frameworks, and compliance mechanisms. The legislative architecture should adopt a hybrid model combining general principles legislation establishing overarching resilience requirements with modular technology-specific annexes. The general act would establish fundamental principles: non-discrimination between functionally equivalent technologies, proportional regulatory intensity calibrated to assessed risks, mandatory cryptographic agility requirements, data protection by design obligations, and periodic mandatory review clauses. Technology-specific modules would provide detailed requirements for particular systems. The artificial intelligence module might specify transparency obligations for algorithmic decision-making, human oversight requirements for high-risk applications, and testing standards for bias detection (Radanliev, 2025). The blockchain module would address immutability conflicts with data protection regimes, establish smart contract audit requirements, and mandate governance mechanisms for protocol updates.

The quantum computing module would require post-quantum cryptographic migration plans, specify standards for quantum-resistant algorithms, and establish timelines for legacy system transitions. Regulatory sandbox provisions would enable controlled experimentation with novel technologies under supervisory oversight, generating empirical evidence informing regulatory refinement. Institutional frameworks require specialized technical capacity within regulatory agencies. The Australian Securities and Investments Commission created a central coordination function to oversee regulation of digital assets, tokenization, and decentralized finance, providing a model for jurisdictions establishing technology assessment capabilities. A Technology Assessment Office would monitor emerging technologies, evaluate regulatory gaps, coordinate across sectoral regulators, and provide technical expertise supporting legislative development. Cross-sectoral coordination mechanisms

prevent regulatory fragmentation whilst enabling specialized expertise. Compliance mechanisms must balance enforceability with flexibility. Risk-tiered migration frameworks cross-reference technical standards like NIST FIPS 203 with regulatory mandates including DORA, providing clear pathways for organizations transitioning to quantum-resistant cryptography. Auditability through robust audit trails and documentation practices enables effective demonstration of compliance.

Safe harbor provisions protect organizations making good-faith compliance efforts from liability when unforeseen technological developments create retrospective non-compliance. International coordination remains essential given digital technologies' inherently transnational character. Responsible innovation principles designed to span all technologies internationally apply to any technology existing today and future, offering frameworks for multilateral cooperation. Standards integration through NIST's three post-quantum cryptography standards demonstrates how technical standards bodies contribute to regulatory harmonization. Dynamic updating mechanisms through delegated authority enable regulatory specifications to evolve without requiring primary legislation amendments for technical details, balancing democratic accountability with adaptive capacity necessary for governing rapidly evolving technologies.

F. Why Resilience Surpasses Neutrality

Technological resilience offers multiple advantages over strict technological neutrality whilst preserving core non-discrimination principles. Enhanced future-proofing represents the primary benefit. Unlike static neutrality treating all technologies identically, resilience emphasizes preparedness and adaptability across architectural and operational pillars, enabling frameworks to accommodate unforeseen technological developments. Mandatory review clauses and modular architectures facilitate updates as understanding evolves, avoiding premature obsolescence plaguing technology-neutral instruments. Targeted intervention capacity enables effective governance of technologies with distinctive characteristics. The AI Act's specific provisions for general-purpose AI models significantly improved its scope and future-proofness, demonstrating that strategic departures from absolute neutrality enhance rather than undermine regulatory effectiveness.

Article 36 of the EU Data Act establishes smart contract termination requirements specifically addressing blockchain immutability, providing regulatory clarity impossible through purely technology-neutral formulations. Quantum preparedness exemplifies resilience advantages. Regulatory lag creates strategic windows for early adopters to shape standards and avoid costly retrofits as quantum-resistant technologies scale across energy, defense, and finance sectors. Proactive resilience frameworks mandating cryptographic agility and post-quantum migration planning position jurisdictions ahead of disruption rather than reactively responding after cryptographic failures occur. Technological synergy recognition improves governance quality. Artificial intelligence supports Web3 by enhancing smart contract

execution accuracy and efficiency whilst blockchain assists responsible AI through transparency, traceability, and tamper-resistance. Resilience frameworks acknowledging these interdependencies enable coherent regulation of integrated technological systems rather than fragmenting oversight across siloed regulatory domains. Risk proportionality operationalizes protective principles effectively. GDPR requires appropriate technical measures, whilst NIST's Cybersecurity Framework provides guidelines for identifying critical systems and establishing backup and recovery processes.

Resilience frameworks translate these principles into concrete operational requirements calibrated to identified hazards. Innovation enabling represents another crucial advantage. Resilience frameworks balance regulatory and market-driven solutions under shift-left culture and new regulatory requirements, avoiding both regulatory capture and innovation-stifling overregulation. Regulatory sandboxes, safe harbor provisions, and clear compliance pathways reduce uncertainty inhibiting investment whilst maintaining essential safeguards. Legal certainty improves when frameworks explicitly address technological specificity rather than leaving courts to interpret technology-neutral provisions applicable to unanticipated circumstances. Rights protection strengthens through targeted interventions. Blockchain decentralization eliminates single points of failure whilst post-quantum cryptography integration maintains resilience, but realizing these protections requires regulatory frameworks specifically addressing both characteristics. Technology-neutral provisions prove inadequate for protecting fundamental rights in technologically distinctive contexts requiring tailored safeguards.

G. Integration into Uzbekistan's Legal System

Uzbekistan's evolving digital economy presents opportunities for innovative regulatory approaches informed by international experience whilst addressing distinctive national circumstances. Current legal framework assessment reveals gaps in comprehensive technology governance. Existing legislation addresses specific sectors including electronic commerce, personal data protection, and telecommunications regulation, but lacks overarching frameworks for artificial intelligence governance, blockchain regulation, or quantum computing preparedness. Uzbekistan's digital transformation initiatives including e-government infrastructure development and smart city projects create practical imperatives for modernized regulatory architectures. The proposed adaptation strategy centers on drafting a Technology Resilience Act of Uzbekistan embodying principles articulated in this research. The Act would establish general resilience principles applicable across technological domains whilst incorporating modular provisions addressing artificial intelligence, blockchain systems, and cryptographic standards. Integration with existing e-government infrastructure ensures coherent digital governance rather than fragmentary approaches.

Alignment with the EU's Cyber Resilience Act (2024) and Digital Operational

Resilience Act providing binding ICT risk duties facilitates international cooperation and cross-border data flows, essential for Uzbekistan's economic integration objectives. Implementation would proceed through four phases. Phase One encompasses legislative drafting incorporating resilience principles, stakeholder consultation with technology sector representatives, academic institutions, and civil society organizations, and comparative analysis of international best practices. Phase Two establishes institutional capacity for technology assessment through specialized units within existing regulatory agencies, technical expertise development through training programs and international partnerships, and coordination mechanisms ensuring coherent oversight across sectoral regulators. Phase Three deploys regulatory sandboxes enabling controlled experimentation with artificial intelligence applications, blockchain-based services, and other innovative technologies under supervisory oversight, generating empirical evidence informing regulatory refinement (Gulyamov, 2024).

Phase Four adapts the Bank for International Settlements' Project Leap approach demonstrating how payment systems can be fortified against quantum computing threats to Uzbekistan's financial infrastructure, prioritizing cryptographic agility in critical systems. Stakeholder engagement proves essential for effective implementation. Technology sector consultation ensures regulatory frameworks remain practically implementable whilst achieving policy objectives. Academic institutions contribute technical expertise and research capacity supporting evidence-based policymaking. International cooperation following the Commonwealth Strategus AI model for policy development support provides technical assistance and best practice sharing. Expected benefits include positioning Uzbekistan as a regional leader in technology governance, attracting foreign investment through regulatory clarity and protection, safeguarding citizens' digital rights through comprehensive frameworks, and enabling participation in global innovation agendas prioritizing post-quantum readiness. Resource requirements encompass technical expertise development through training and recruitment, international partnership establishment for knowledge sharing and capacity building, and legislative resources for comprehensive drafting and stakeholder consultation processes. Successful implementation positions Uzbekistan advantageously in emerging digital economy whilst establishing protective frameworks safeguarding fundamental rights and national interests.

IV. Discussion

This research contributes conceptual frameworks bridging theoretical technology neutrality scholarship and practical regulatory challenges confronting contemporary governance. Technology neutrality operationalization suffers from various challenges, not least a lack of consensus about what neutrality means in the first place (Frahm et al., 2022). Our technological resilience principle offers a coherent evolutionary pathway preserving non-discrimination imperatives whilst enabling

targeted interventions addressing distinctive technological characteristics. The theoretical advancement lies in articulating active, adaptive governance paradigms transcending passive neutrality assumptions. Several limitations warrant acknowledgement. The conceptual nature of this research requires empirical validation through implementation and assessment of practical effectiveness. Acute shortages in skilled quantum-capable personnel impede sectoral preparedness, affecting implementation feasibility across jurisdictions, particularly developing economies with limited technical capacity. Resource intensiveness of establishing technology assessment offices, developing specialized expertise, and maintaining continuous monitoring regimes may exceed capacities of jurisdictions with constrained administrative resources.

The absence of current post-quantum blockchain regulations creates opportunities but also generates uncertainties about optimal regulatory approaches. Potential regulatory capture by technology companies possessing superior technical expertise and lobbying resources poses risks requiring vigilant attention to democratic accountability and public interest protection. Balancing regulatory oversight against innovation incentives remains perpetually challenging, requiring context-sensitive calibration difficult to achieve through general principles. Addressing potential critiques, some may argue that abandoning strict technological neutrality surrenders valuable non-discrimination protections. However, strict adherence to neutrality may obscure political choices and democratic agency essential for effective regulation.

Technological resilience preserves non-discrimination for functionally equivalent technologies whilst acknowledging that not all technologies prove functionally equivalent in legally relevant respects. Others might contend that technology-specific provisions create regulatory complexity. We respond that complexity inherent in technological reality cannot be eliminated through regulatory simplification; frameworks must possess sufficient granularity addressing actual governance challenges rather than pursuing elegance at the cost of effectiveness. Contextual factors affecting technological resilience implementation include institutional capacity, political will for comprehensive reform, stakeholder cooperation, and international coordination. Effectiveness depends substantially upon regulators possessing sufficient technical expertise, political systems maintaining stability enabling long-term planning, technology sectors engaging constructively rather than obstructively, and international partners coordinating approaches addressing inherently transnational technologies (Shao et al., 2024). Generalizability beyond Uzbekistan requires jurisdictional adaptation reflecting distinctive legal traditions, institutional structures, economic development levels, and technological adoption patterns. The underlying principles adaptive regulation, risk-proportionality, technology-specific modules, and mandatory review possess universal applicability requiring contextual operationalization.

Future regulatory trajectories suggest accelerating technological change

demanding increasingly adaptive governance frameworks. The immediate horizon from 2025 through 2027 will witness continuing implementation of existing major frameworks including the EU AI Act, assessment of practical effectiveness and unintended consequences, and potential amendments addressing identified shortcomings. The United Nations has proclaimed 2025 to be the International Year of Quantum Science and Technology, with increased qubit counts, improvements in error correction, and cloud access to quantum platforms, heightening quantum computing's practical relevance and urgency of post-quantum cryptographic transitions. The UK's National Quantum Strategy consolidates academic-industry collaboration through dedicated research hubs in Oxford, Birmingham, and Glasgow whilst embedding quantum resilience into critical infrastructure planning, offering models for other jurisdictions developing quantum computing strategies. Artificial Intelligence Act implementations will reveal practical challenges including enforcement complexities, compliance cost implications, and innovation impacts, informing subsequent regulatory refinements (AllahRakha, 2025a).

The medium term spanning 2027 through 2030 anticipates substantial technological convergence effects. Eighty-six percent of enterprises anticipate AI-driven transformations by 2030, with tools like ChatGPT catalyzing infrastructure investments in quantum-safe systems. The convergence of quantum computing, artificial intelligence, blockchain, and cybersecurity accelerates innovation whilst redefining foundations of trust, security, and digital transformation. Post-quantum cryptography standards will mature from initial NIST publications toward widespread implementation across critical infrastructures. Enhancement of digital and data resilience across the financial sector to mitigate risks associated with technology-enabled financial services, cybersecurity breaches, and artificial intelligence misuse in financial decision-making will drive sectoral regulatory developments.

International coordination efforts may yield multilateral frameworks harmonizing approaches across jurisdictions, reducing regulatory arbitrage opportunities whilst facilitating cross-border digital commerce. Long-term trajectories beyond 2030 face substantial uncertainty given accelerating technological change. Potential quantum computing breakthroughs achieving practical advantage for commercially relevant problems may require renewed regulatory adaptation. New paradigms of artificial intelligence architectures will emerge addressing generative AI limitations through robotics and virtual reality integration, presenting governance challenges requiring frameworks capable of accommodating architectural innovations. Global regulatory convergence toward resilience-based models may occur as jurisdictions recognize technological neutrality's limitations, though path dependencies and jurisdictional competition may impede harmonization. Integration with climate governance, social policy, and corporate governance frameworks will likely occur as digital technologies' pervasive effects across policy domains demand holistic rather than siloed approaches. The technological resilience principle offers conceptual foundations capable of accommodating these evolving governance challenges through

adaptive architectures maintaining relevance amid continuing technological transformation (Rashed et al., 2025).

Practical implications extend across stakeholder categories. Legislators receive actionable frameworks balancing innovation incentives against protection imperatives through risk-proportional approaches avoiding both regulatory capture and innovation-stifling overregulation. Businesses adopting proactive resilience approaches reduce costs of fixing issues whilst building reliable, robust systems meeting regulatory requirements through design-stage integration rather than retrofitting. Citizens gain enhanced digital rights protections against quantum computing threats to cryptographic security underpinning financial systems, healthcare databases, and governmental communications. The international community benefits from comprehensive, evergreen regulatory approaches ensuring safety and building global trust in technology through jurisdictional cooperation addressing inherently transnational digital technologies.

Practical significance lies in bridging technical cryptographic advancements with regulatory compliance, offering roadmaps absent in siloed technical or policy studies. This research issues a call to action: jurisdictions must immediately initiate legislative drafting processes, stakeholder consultation mechanisms, and international cooperation efforts. Delay risks accumulating vulnerabilities whilst technological capabilities advance, particularly concerning quantum computing's cryptographic threats and artificial intelligence's autonomous decision-making implications (AllahRakha, 2025b). The ultimate vision encompasses resilient digital ecosystems supporting sustainable technological development, protecting fundamental rights, enabling economic innovation, and maintaining adaptability accommodating future technological transformations. Uzbekistan and similarly positioned jurisdictions possess opportunities to position themselves advantageously through forward-looking regulatory frameworks informed by international best practices whilst addressing distinctive national contexts. Technological resilience offers conceptual foundations capable of achieving these objectives through principled evolution of regulatory approaches meeting contemporary governance challenges.

Conclusions

Technological neutrality, whilst historically valuable for preventing discriminatory regulation favoring incumbent technologies over innovations, confronts fundamental limitations when applied to contemporary digital technologies. Technology's logic is increasingly tested as technology becomes constitutive of products and services rather than merely facilitative. Artificial intelligence's opacity and autonomous characteristics, blockchain's architectural immutability, and quantum computing's cryptographic disruption resist governance through frameworks assuming functional equivalence between technological alternatives. This research has articulated technological resilience as a principled evolution maintaining non-

discrimination imperatives whilst enabling targeted regulatory interventions addressing distinctive technological characteristics. The AI Act's deviations from technology neutrality including specific provisions for general-purpose AI models significantly improved its scope and future-proofness, demonstrating that technology neutrality and future-proof regulation should not be treated synonymously.

Four pillars, adaptive regulation through continuous assessment, technology-specific modules supplementing general principles, risk-tiered regulatory intensity, and mandatory sunset and review clauses, provide operational frameworks translating conceptual principles into implementable governance architectures. Implementation requires comprehensive cultural shifts embedding resilience throughout system development lifecycles, continuous monitoring, and validation processes rather than one-time compliance exercises. Uzbekistan possesses opportunities to adopt innovative approaches benefiting from international experience whilst addressing distinctive national circumstances through carefully designed Technology Resilience Act and supporting institutional developments.

Bibliography

AllahRakha, N. (2025a). Cross-Border E-Crimes: Jurisdiction and Due Process Challenges. *ADLIYA: Jurnal Hukum Dan Kemanusiaan*, *18*(2), 153–170. https://doi.org/10.15575/adliya.v18i2.38633

AllahRakha, N. (2025b). National Policy Frameworks for AI in Leading States. *International Journal of Law and Policy*, *3*(1), 38–51. https://doi.org/10.59022/ijlp.270

Cheng, Z. M., Bonetti, F., de Regt, A., Ribeiro, J. Lo, & Plangger, K. (2024). Principles of responsible digital implementation: Developing operational business resilience to reduce resistance to digital innovations. *Organizational Dynamics*, *53*(2), 101043. https://doi.org/10.1016/j.orgdyn.2024.101043

Frahm, N., Doezema, T., & Pfotenhauer, S. (2022). Fixing Technology with Society: The Coproduction of Democratic Deficits and Responsible Innovation at the OECD and the European Commission. *Science, Technology, & Human Values*, *47*(1), 174–216. https://doi.org/10.1177/0162243921999100

Frantziou, E. (2014). Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos. *Human Rights Law Review*, *14*(4), 761–777. https://doi.org/10.1093/hrlr/ngu033

Gulyamov, S. (2024). Application of Computational Law and Artificial Intelligence Methods for Sharia Compliance Analysis of E-Waste Management Systems Based on Blockchain. *Suhuf*, *36*(1), 21–32. https://doi.org/10.23917/suhuf.v36i1.4447

Markman, G. D., Gianiodis, P. T., Phan, P. H., & Balkin, D. B. (2005). Innovation speed: Transferring university technology to market. *Research Policy*, *34*(7), 1058–1075. https://doi.org/10.1016/j.respol.2005.05.007

Ojanen, A. (2025). Technology Neutrality as a Way to Future-Proof Regulation: The Case of the Artificial Intelligence Act. *European Journal of Risk Regulation*, 1–16. https://doi.org/10.1017/err.2025.10024

Radanliev, P. (2025). Privacy, ethics, transparency, and accountability in AI systems for wearable devices. *Frontiers in Digital Health*, *7*. https://doi.org/10.3389/fdgth.2025.1431246

Rashed, Md., Uddin, Md. K., Islam, M. F., Faisal-E-Alam, Md., Tushar, H., & Ahmed, M. E. (2025). Building Resilient Organizations: The Role of Technological Capability, Innovation Leadership, and Sustainability. *Global Journal of Flexible Systems Management*, *26*(4), 963–995. https://doi.org/10.1007/s40171-025-00471-x

Schlagwein, D., Gozman, D., & Manusu, A. P. (2025). Cryptocurrency frames of reference: a case study of accepting 'Bitcoin-as-X.' *European Journal of Information Systems*, 1–36. https://doi.org/10.1080/0960085X.2025.2530456

Shadikhodjaev, S. (2021). Technological Neutrality and Regulation of Digital Trade: How Far Can We Go? *European Journal of International Law*, *32*(4), 1221–1247. https://doi.org/10.1093/ejil/chab054

Shao, H., Wang, Y., Lee, C.-C., & Wen, H. (2024). How does political stability affect renewable energy finance? International evidence. *Energy*, *313*, 133829. https://doi.org/10.1016/j.energy.2024.133829

Sullivan-Taylor, P. (2025). Adaptive Approaches to Integrated Care Regulation, Assessment, and

Inspection. In *Handbook of Integrated Care* (pp. 467–487). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-96286-8_13

Teo, S. A. (2025). Artificial intelligence and its 'slow violence' to human rights. *AI and Ethics*, *5*(3), 2265–2280. https://doi.org/10.1007/s43681-024-00547-x

Wu, D., Cai, H., & Li, T. (2025). Food Safety Risk Prediction and Regulatory Policy Enlightenment Based on Machine Learning. *Systems*, *13*(8), 715. https://doi.org/10.3390/systems13080715