World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

The role of international standards in shaping the legal framework for digital compliance

Aleksandra Kostoreva *

University of Georgia School of Law - Master of Laws, Athens, Georgia, USA.

World Journal of Advanced Research and Reviews, 2025, 26(03), 1527-1532

Publication history: Received on 27 April 2025; revised on 12 June 2025; accepted on 14 June 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.26.3.2323

Abstract

This article explores the role of international standards in shaping the legal framework for digital compliance amid the digitalization of the global economy. It examines current regulatory instruments such as BEPS, GDPR, and ISO standards, identifying key legal challenges related to the cross-border nature of digital operations, incompatibilities between national legal systems, and issues surrounding the practical applicability of these standards. The aim of the study is to define the function of international standards in forming the legal foundations of digital compliance and to analyze their influence on the development of national legal systems in the context of digital transformation. The methodological basis of the research includes comparative analysis of related studies. The article will be of interest to researchers analyzing and developing legal mechanisms for digital compliance, as well as to legal professionals, digital transformation specialists, and international regulation experts interested in integrating global standards into national legal frameworks. Drawing on an interdisciplinary approach, the article offers timely insights for those seeking to deepen their understanding of the complex interplay between international standards and the legal structures necessary for sustainable digital economic development in a globalized environment.

Keywords: International Standards; Digital Compliance; Digital Economy; Legal Regulation; Adaptive Governance; International Cooperation; BEPS; GDPR; ISO/IEC 27001

1. Introduction

The transformation of business models under the influence of digital technologies is generating new challenges for the regulation of economic activity, necessitating the creation of unified international standards capable of ensuring transparency, predictability, and fairness in law enforcement [1]. Recent research increasingly emphasizes that global regulatory initiatives such as BEPS and the GDPR play a key role in harmonizing the regulation of cross-border digital operations. However, their integration into national legal systems remains insufficiently developed [2]. While some studies focus on analyzing legal frameworks and regulatory adaptation in the context of digitalization, others examine the impact of the digital economy on economic structures and environmental conditions, thereby indirectly addressing issues of compliance.

In the scholarly literature, three broad categories of sources can be distinguished: normative-legal acts and standards; academic studies of models and mechanisms for regulating the digital environment; and works that elucidate the broader context of the digital economy and its impact on sectoral transformation.

The first category encompasses international and regional legal standards designed to unify approaches to data protection, information security, and cross-border data flows. A cornerstone document is Regulation (EU) 2016/679 of the European Parliament and of the Council [5], which establishes the framework for processing individuals' personal

* Corresponding author: Aleksandra Kostoreva Email: aleksandra.kostoreva@gmail.com

data and its free movement within the EU. Regulation (EU) 2023/1114 of the European Parliament and of the Council [10] sets out requirements for digital services with respect to algorithmic-decision transparency and compliance procedures in the digital-platform economy. At the level of international organizations, the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [8] articulate foundational principles that inform national legislation and corporate policy. Information-security management is standardized by ISO/IEC 27001:2022, which defines requirements for information-security management systems [6]. In the United States, the California Consumer Privacy Act (CCPA) delineates rights and obligations of data subjects and controllers in California [7], while sector-specific rules appear in the UK's Payment Services Act 2019 [9].

The second category comprises peer-reviewed articles that analyze and model legal and organizational approaches to digital compliance. Adelakun B. O. et al. [1] offer a financial perspective on tax compliance in the digital economy, emphasizing the need to harmonize tax rules and ensure transparency of digital transactions. Rehman Z. [2] examines international law and global governance in the digital era, highlighting the growing role of transnational legal mechanisms and intergovernmental collaboration to bridge jurisdictional gaps. Akpobome O. [3] develops a model of adaptive regulation in light of emerging technologies (blockchain, AI), proposing a methodology for combining "soft" sandbox-style instruments with "hard" legal norms. Babikian J. [4] focuses on human-rights dimensions, analyzing privacy and data-protection standards in the digital environment from both international and national legal perspectives.

The third category addresses general trends in the digital economy that influence the rationale behind evolving standards and legal norms. Xu S. et al. [11] investigate the spatial relationship between the digital economy and environmental pollution, calling for the integration of ecological standards into digital regulations. Yu W. [12] assesses the digital economy at the regional level, proposing comprehensive indicators for monitoring its development. Yuan H., Zhao L., and Yue H. [13] analyze how digitalization drives transformation and modernization of industrial structures, demonstrating how digital technologies accelerate the shift toward high-tech sectors. Zhang K. et al. [14], in the context of startups, explore the interplay between dynamic capabilities and business-model innovation in the digital age—insights that are vital for identifying which technological solutions require specialized regulatory frameworks.

In summary, despite the breadth of research, the literature reveals several contradictions. Questions remain insufficiently addressed regarding the effective integration of international recommendations into the national legal systems of developing countries and the challenge of cross-jurisdictional liability when digital-compliance breaches occur. Empirical studies examining how standards impact real-world security and privacy metrics within business processes—and the oversight mechanisms needed to enforce these norms in a rapidly evolving technological environment—are also scarce.

The objective of this article is to analyze international standards in the formation of the legal framework for digital compliance.

The scientific novelty of this work lies in the first-ever comparative analysis of the mechanisms by which ISO/IEC standards and the GDPR are transposed into the CCPA/CPRA, highlighting the characteristics of their hybrid integration.

The author's hypothesis posits that embedding international standards within national legal systems enhances transparency, reduces opportunities for regulatory arbitrage, and creates conditions for effective digital compliance—thereby improving law-enforcement practice and stimulating the development of the digital economy.

The research methodology is founded on a comparative analysis of existing studies and relevant international standards, enabling a comprehensive examination of the legal landscape governing digital standards.

2. Theoretical Foundations of Digital Compliance and International Standards

Digital compliance encompasses the system of processes, technologies, and organizational measures aimed at ensuring that a company's digital operations conform to applicable legal, regulatory, and industry requirements. According to Babikian J. [4], digital compliance represents a suite of risk-management and data-subject-protection measures in the digital environment, encompassing both internal accountability (governance, risk management) and external accountability (reporting, audit, interaction with regulators).

ISO/IEC 27001:2022 [6] refines the notion of "compliance obligations" as "the requirements to which an organization must adhere in the design, operation, and improvement of its information-security management system." Translated to the context of digital business, this approach adds the following elements:

- Processes – assessment of compliance gaps relative to laws and policies (compliance-gap analysis)
- Technologies – automated monitoring tools, DLP systems, SIEM
- Internal accountability – roles such as CISO, compliance officers, risk committees
- External accountability – engagement with regulators, mandatory reporting, audits [1, 4]

International standards are formalized documents that establish requirements and recommendations to ensure uniformity and quality at the global level. They can be divided into three major categories, as shown in Table 1.

Table 1 Classification of international standards and examples [1, 4, 5, 6, 10]

Category	Description	Example	Organization
Intergovernmental Acts	Mandatory or advisory norms adopted by intergovernmental bodies	GDPR (Regulation (EU) 2016/679)	EU, UN
ISO/IEC Standards	Voluntary technical specifications and guidelines for information-security management systems and related areas	ISO/IEC 27001	ISO/IEC
Industry Codes	Requirements developed by industry stakeholders and trade associations	PCI DSS; HIPAA Security Rule	PCI SSC; HHS (USA)

Intergovernmental acts establish the legal framework at the level of states and regional blocs [2, 4], while ISO/IEC standards provide the technical and organizational methodologies to implement it. Industry codes supplement these with specialized requirements [6].

GDPR has already become a de facto global benchmark for non-EU national laws due to its extraterritorial reach and stringent principles of personal-data processing (the so-called "benchmark effect"). Its core tenets (purpose limitation, data minimization, data-subject rights) have been reinterpreted in CCPA/CPRA [7] and PIPL [8], demonstrating a "domino effect." ISO/IEC 27001 and ISO/IEC 27701 serve as the technical foundation for developing digital-compliance procedures [2, 3]. Together, GDPR and ISO/IEC standards enable organizations to construct a robust digital-compliance framework that combines legal precision with technical granularity.

Thus, digital compliance is viewed as an integrated system of managerial, technological, and organizational measures that ensure a company's adherence to a comprehensive set of legal, regulatory, and industry requirements in the digital environment. At its core lies a methodology for risk management and data-subject protection (compliance-gap analysis; automated DLP and SIEM solutions), a clear delineation of internal responsibilities (CISO, compliance officers, risk committees), and external obligations (regulatory engagement, audit, reporting). International standards create the legal framework, technical methodologies, and specialized requirements—GDPR serving as the de facto global reference—which together yield a reliable digital-compliance framework that melds strict legal regulation with detailed technical procedures.

3. Key International Standards and Their Influence on National and Californian Legal Frameworks

Regulation (EU) 2016/679 of the European Parliament and of the Council [5] was the first comprehensive legal act to establish uniform rules for the processing of personal data across all Member States of the Union. Its core principles include:

- lawfulness, fairness, and transparency of processing;
- purpose limitation and data minimization;
- accuracy and retention limitations;
- data-subject rights (access, portability, erasure).

GDPR has profoundly influenced data-protection laws in other jurisdictions, as evidenced by the adoption of its key principles and mechanisms outside Europe.

In California, data-protection requirements began to take shape with the California Consumer Privacy Act (CCPA) of 2018. The original CCPA granted residents rights of access, deletion, and opt-out of "sale" of their personal information

but did not introduce a GDPR-style legal-basis framework. The 2020 California Privacy Rights Act (CPRA) amended and expanded CCPA's scope by:

- establishing a new category of "sensitive personal information";
- strengthening notice and corporate-reporting obligations;
- creating the California Privacy Protection Agency with enforcement and sanctioning powers [7].

In the People's Republic of China, the Personal Information Protection Law (PIPL) came into force in 2021 and mirrors many GDPR elements. PIPL applies extraterritorially (its "long arm"), requires foreign data controllers handling information on Chinese residents to appoint a representative within China, and enshrines principles of lawfulness, data minimization, and data-subject rights—alongside mandatory data-protection impact assessments (DPIAs) and, in certain cases, data localization [9].

Below, Table 2 presents a comparative overview of GDPR, PIPL, CCPA, and CPRA.

Table 2 Comparative Characteristics of GDPR, PIPL, CCPA, and CPRA [3, 5, 7, 9, 10**]**

Standard / Law	**Territorial Scope**	**Core Processing Principles**	**Supervisory Authority & Sanctions**
GDPR	EU Member States and extraterritorially ("long arm")	lawfulness; transparency; data minimization; data-subject rights	national data-protection authorities (e.g., CNIL)
PIPL	China and extraterritorially for data on Chinese residents	correction; deletion; DPIA; data localization	Cyberspace Administration of China
CCPA	California (businesses that sell or share personal information)	right to know; right to delete; opt-out of sale	California Department of Justice
CPRA	extends CCPA (adds extraterritorial reach)	sensitive personal information; DPIA; Privacy by Design	California Privacy Protection Agency

MiCA, adopted in May 2023 and partially in force as of June 2024 (Sections III–IV), establishes a unified regulatory framework for the issuance and trading of crypto-assets within the European Union. It introduces a clear three-fold token classification—electronic money tokens, asset-referenced tokens, and utility tokens—and requires developers to publish a white paper detailing the project and assessing associated risks. The regulation also mandates authorization and supervision of crypto-asset service providers (CASPs), obliging them to maintain a registered office and a director within the EU.

In California, the Digital Financial Assets Law (DFAL) will come into effect on July 1, 2026, introducing mandatory licensing of cryptocurrency activities through the Department of Financial Protection and Innovation (DFPI). Firms must register via the NMLS system, maintain a prescribed bond level, and submit regular reports. Specific provisions cover cryptocurrency-exchange kiosks, which also require DFPI registration and approval [4].

At the federal level in the United States, the FIT21 bill (H.R. 4763) proposes assigning oversight of "decentralized" blockchain assets to the Commodities Futures Trading Commission (CFTC) and all other crypto-instruments to the Securities and Exchange Commission (SEC). This division aims to create clear functional boundaries while providing carve-outs for stablecoins.

Beyond these statutes, digital compliance rests on international and technical standards. The OECD's 1980 Guidelines laid down principles of purpose limitation and fair use in cross-border data flows [11, 12].

Thus, ISO/IEC standards define the requirements for information-security management systems and extend them to personal-data governance, prescribing a suite of technical and organizational measures to protect and control information flows. The "Privacy by Design" principle, enshrined in the California Consumer Privacy Act, complements these norms by requiring data-protection measures to be integrated at every stage of a service's lifecycle. Together, these instruments form a modular approach to digital compliance that combines legal rigor with technical flexibility across multiple jurisdictions.

4. Practical Consequences, Harmonization Challenges, and Future Outlook

The widespread adoption of GDPR and ISO/IEC standards fosters harmonization of digital-compliance requirements by creating a common "language" for companies and regulators. This convergence reduces transaction costs in cross-border business and simplifies the scaling of international compliance programmes. However, a strict uniform approach also risks "over-engineering" local regulations and overlooking jurisdiction-specific nuances, potentially leading to regulatory fragmentation and increased burdens on businesses [2, 4].

Table 3 summarises the advantages and disadvantages of harmonization versus fragmentation of international standards.

Table 3 Advantages and Disadvantages of Harmonization vs. Fragmentation [4]

Aspect	Harmonization (GDPR / ISO)	Fragmentation (Local Norms)
Regulatory Consistency	Single requirements and approaches across industries and jurisdictions	Tailored to specific market characteristics and sector risks
Legal Predictability	Clear international rules familiar to global corporations	Varied interpretations and uneven enforcement practices
Compliance Costs	Lower costs when scaling compliance programmes	Higher expenses adapting to each region's unique requirements
Flexibility	Centralised updates, often slow	Rapid local legislative responses to emerging challenges
Innovation	May be constrained by rigid frameworks	Encourages pilot projects and adaptive, experimental solutions

When organisations adapt international information-security and data-protection standards, they confront fundamental tensions. On one hand, guidance such as ISO/IEC 27001 and the OECD privacy principles is voluntary and inherently "soft"; on the other hand, GDPR and CCPA/CPRA impose mandatory legal sanctions for non-compliance. As a result, companies must simultaneously build flexible internal processes and ensure strict adherence to binding regulatory requirements, generating significant legal and organisational uncertainty [14].

Extraterritorial mechanisms within GDPR and CPRA further compound complexity. Although these regulations envisage close intergovernmental cooperation among regulators, in practice national authorities often prioritise their own jurisdictions and do not exchange information in real time. The lack of a centralised coordination platform leads to duplicated investigations and reduces overall enforcement effectiveness [4, 13].

A promising path forward is the further unification of ISO/IEC standards through a modular approach that integrates key GDPR and CCPA requirements into new ISO/IEC revisions. In parallel, the work of ISO/TC 307 on blockchain standards could serve as a foundation for embedding "digital-compliance" norms within the financial sector.

As a practical mechanism, regulators and legislators might develop discrete "modules" drawn from GDPR (for example, Data Protection Impact Assessments and Privacy by Design) and CPRA (enhanced protection of sensitive personal data and expanded supervisory powers) for adoption into the national laws of emerging economies. This "pick-and-choose" strategy would allow jurisdictions to combine leading international practices with local regulatory needs.

At the level of intergovernmental agreements, it would be advisable to leverage the UNCITRAL Model Law on Electronic Transferable Records and the EU's MiCA framework to negotiate a global memorandum of understanding on mutual recognition of digital-compliance licenses and procedures. Such an accord would harmonise requirements for crypto- and fintech companies and lower barriers to cross-border service provision.

5. Conclusion

The study confirmed the hypothesis that adapting international ISO/IEC standards and GDPR-based approaches within California's CCPA/CPRA framework enhances the effectiveness of digital-compliance programs. It was shown that

blending stringent legal norms (GDPR, CPRA) with modular technical specifications (ISO/IEC) yields a resilient, scalable compliance structure capable of addressing both cross-border and local risks.

Further integration of ISO/IEC standards—through revisions that explicitly incorporate digital-privacy requirements drawn from GDPR and CPRA—will reinforce the alignment between technical processes and legal mandates.

International agreements on mutual recognition of licenses and compliance procedures in the digital-asset sector (leveraging UNCITRAL and MiCA) will establish a favorable regime for cross-border exchange of services and information.

Future research should focus on developing methodologies to evaluate the effectiveness of these hybrid compliance models across different industries, as well as exploring the application of emerging digital technologies (blockchain, AI) to automate compliance monitoring and auditing. In the long term, creating universal "trust mechanisms" among regulators from diverse jurisdictions will be essential to building a global, inclusive, and secure digital ecosystem.

References

[1] Adelakun B. O. et al. Legal frameworks and tax compliance in the digital economy: a finance perspective. – 2024. – Vol. 6 (3). – pp.26- 35. DOI: 10.51594/ijae.v6i3.900/.

[2] Rehman Z. Beyond borders: International law and global governance in the digital age //Journal of Accounting & Business Archive Review. – 2023. – Vol. 1 (1). – pp. 1-12.

[3] Akpobome O. The Impact of Emerging Technologies on Legal Frameworks: A Model for Adaptive Regulation //International Journal of Research Publication and Reviews. – 2024. – Vol. 5 (10). – pp. 5046-5060.

[4] Babikian J. Securing Rights: Legal Frameworks for Privacy and Data Protection in the Digital Era //Law Research Journal. – 2023. – Vol. 1 (2). – pp. 91-101.

[5] Regulation (EU) 2016/679 of the European parliament and of the council of 27 April 2016 [Electronic resource] Access mode: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L:2016:119:FULL (date of request: 05/14/2025).

[6] Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO/IEC 27001:2022 [Electronic resource] Access mode: https://www.iso.org/standard/27001 (date of request: 05/15/2025).

[7] California Consumer Privacy Act (CCPA) [Electronic resource] Access mode: https://www.sidley.com/en/us/sidley-pages/ccpa-text/ (date of request: 05/13/2025).

[8] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [Electronic resource] Access mode: https://www.oecd.org/en/publications/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en.html (date of request: 05/09/2025).

[9] Payment Services Act 2019 [Electronic resource] Access mode: https://en.wikipedia.org/wiki/Payment_Services_Act_2019 (date of request: 05/10/2025).

[10] Regulation (EU) 2023/1114 of the European parliament and of the council of 31 May 2023 [Electronic resource] Access mode: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1114 (date of request: 05/11/2025).

[11] Xu S. et al. Interaction between digital economy and environmental pollution: New evidence from a spatial perspective //International Journal of Environmental Research and Public Health. – 2022. – Vol. 19 (9). – pp. 5074. DOI: 10.3390/ijerph19095074.

[12] Yu W. Comprehensive measurement of digital economy in Anhui province. Frontiers in Business Economics and Management. – 2023. – Vol. 8(3). – pp. 163-166.

[13] Yuan H., Zhao L., Yue H. Impact of Digital Economy on the Transformation and Upgrading of Industrial Structure. – 2022. – pp. 1-12. DOI: 10.36689/uhk/hed/2022-01-087.

[14] Zhang K. et al. Start-up's road to disruptive innovation in the digital era: The interplay between dynamic capabilities and business model innovation //Frontiers in Psychology. – 2022. – Vol. 13. – pp. 1-12. DOI: 10.3389/fpsyg.2022.925277.