SPECIFICS OF LEGAL REGULATION OF ELECTRONIC DATA CIRCULATION IN THE UNITED STATES: PROSPECTS FOR APPROXIMATION OF EXPERIENCE

Olefirenko Andriy

DOI: https://doi.org/10.61345/1339-7915.2024.6.10

Annotation. The article is devoted to the study of the specifics of legal regulation of electronic data circulation in the United States, focusing on the structure, scope, and practical implications of federal and state legislative frameworks. Attention was given to key federal regulations such as the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and the Electronic Communications Privacy Act (ECPA), which collectively establish sector-specific standards for data privacy and security across healthcare, financial, and communications sectors.

Investigated were the mechanisms of practical implementation and enforcement associated with the U.S. data circulation regulations, highlighting the roles of federal agencies, including the Federal Trade Commission (FTC), Federal Communications Commission (FCC), and the National Institute of Standards and Technology (NIST). The analysis revealed that these agencies, operating under distinct legislative mandates, significantly influence organizational compliance by issuing prescriptive guidelines, initiating enforcement actions, and promoting voluntary standards such as the NIST Cybersecurity Framework.

Found out were key differences and similarities between the U.S. data protection model and international data regulation frameworks, with comparative analysis focusing on the European Union's General Data Protection Regulation (GDPR) and emerging regulations across Asian jurisdictions. The investigation revealed that while the U.S. approach is characterized by a sectoral, decentralized structure favoring industry-specific solutions, the EU emphasizes comprehensive, rights-based data protection enforced through harmonized legislation.

Substantiated were recommendations for harmonizing data circulation laws while respecting local legal traditions and socio-economic contexts, emphasizing the importance of adopting a balanced approach that preserves fundamental rights without impeding technological progress. Proposed strategies included fostering international cooperation through bilateral and multilateral agreements, adopting hybrid regulatory models that combine U.S. sector-based principles with comprehensive privacy statutes, and enhancing the role of global standards bodies in shaping best practices.

Key words: electronic data circulation, legal regulation, data privacy, data security, federal regulations, data protection, enforcement mechanisms, data governance, international data regulation, sector-based approach, privacy rights, consumer protection, cybersecurity, legal harmonization, global data governance, data processors, data controllers, risk management.

1. Introduction.

The widespread digitalization of contemporary society has made electronic data circulation a critical area of legal and economic interest, prompting governments and institutions worldwide to establish comprehensive regulatory frameworks aimed at safeguarding the confidentiality, integrity, and availability of information. Against this backdrop, the United States stands out due to its extensive

experience in crafting laws, regulations, and policies that balance the demands of technological innovation with the imperative of protecting individual rights.

This dual focus on fostering economic growth and maintaining robust safeguards highlights the significance of examining American legal approaches and understanding how sector-specific rules, federal statutes, and state-level legislation converge to govern electronic data handling. The relevance of researching the specific characteristics of US regulation lies in the capacity of these norms to influence global policy discussions, given the United States' role as a hub for major technology companies and a primary driver of advanced digital services. Observing how federal agencies, such as the Federal Trade Commission, collaborate with various state authorities to enforce standards and oversee compliance provides valuable insights into potential pathways for developing nuanced data governance structures elsewhere.

Such research is also pivotal in identifying effective strategies for preventing data breaches, ensuring consumer rights, and clarifying responsibility for corporate entities that manage large-scale data operations. The study of American legal norms and their enforcement mechanisms can thus inform international discourse on standardizing electronic data circulation, helping policymakers evaluate the merits of aligning local regulations with best practices and adapt those lessons to address jurisdiction-specific challenges without compromising fundamental rights or stifling technological progress.

2. The methodological basis of the study.

The methodological basis of the study was a combination of general scientific and special legal research methods, as well as scientific articles by the authors of the case study (Bamberger K.A., Mulligan D.K., Caballero T.G., Palmieri N.F. III, Solove D.J., Hartzog W., Bowen P., Hash J., Wilson M., Mylavarapu S., Kuner C., Greenleaf G., Schwartz P.M., Peifer K.N.). The dialectical method was used to analyse the evolution of legal regulation of electronic data circulation in the United States. Comparative legal and formal legal methods allowed to study the differences between the US and international legal frameworks. Systemic and structural analyses were used to study legislative acts, law enforcement mechanisms and law enforcement practice.

3. The aim of the work is

to analyze the specific features of the legal regulation of electronic data circulation in the United States, with a particular focus on understanding the structure, mechanisms, and practical implications of the existing regulatory framework.

4. Review and discussion.

The legal framework for electronic data circulation in the United States encompasses a diverse array of statutory instruments, regulatory initiatives, and enforcement mechanisms that collectively shape the way information is collected, transferred, stored, and protected in both private and public sectors [1]. At the federal level, three pivotal legislative acts have gained particular prominence due to their targeted approaches toward distinct categories of data: the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and the Electronic Communications Privacy Act (ECPA). HIPAA, which covers healthcare providers, insurers, and related entities, outlines detailed protocols for safeguarding electronic health records and imposes stringent requirements on data handling, including the implementation of administrative, technical, and physical safeguards that minimize vulnerabilities. These requirements, along with mandatory risk assessments and breach notification obligations, reflect a broader philosophy of ensuring that personal health information remains strictly confidential and that any entity processing such records maintains an elevated standard of data security.

GLBA, by contrast, targets the financial sector and imposes obligations upon banks, insurance companies, and other financial institutions to disclose their information-sharing practices to

consumers while ensuring that sensitive information is protected through risk-based measures and robust data security programs. This statute, which grants individuals limited rights over how their financial data is collected and processed, underscores the importance of transparency and accountability in an environment where financial transactions increasingly rely on electronic channels of communication [2]. ECPA, originally introduced to address the interception and disclosure of electronic communications, has evolved into an essential safeguard of digital privacy, although ongoing debates highlight the need for modernized provisions that reflect the complexities of social media, cloud computing, and other contemporary technologies.

In parallel with these federal laws, state-level regulations exert a profound influence on how electronic data circulation occurs, since states enjoy considerable latitude to adopt more protective or more stringent standards than those mandated by federal statutes. California, through legislation that confers significant privacy rights upon consumers, has emerged as a leader in shaping national discussions related to data privacy, given that companies operating nationwide must ensure compliance with divergent sets of rules. This patchwork of state requirements, which may encompass additional rights of access, deletion, or opt-out features, illustrates how legislative innovation at the state level can drive organizations to refine data handling practices and adopt consistent policies across multiple jurisdictions [3]. Other states have followed a similar trajectory, indicating that national data circulation policies are not solely the product of federal initiatives but rather the culmination of overlapping legal regimes that can sometimes create compliance challenges for businesses seeking uniform approaches. Nevertheless, such interplay between federal and state standards fosters a dynamic legal environment capable of adapting to novel technological developments and emerging threats to personal data. The resultant mosaic of statutes and regulations underscores the fact that data governance in the United States is an ongoing negotiation between federal authorities, state legislatures, industry stakeholders, and advocacy groups seeking to safeguard privacy while enabling innovation.

Supervisory oversight by federal agencies further differentiates the American framework for electronic data circulation. The Federal Trade Commission (FTC) acts as a primary watchdog for consumer protection in various domains, relying on its authority to pursue entities that engage in unfair or deceptive data practices. Under Section 5 of the Federal Trade Commission Act, the FTC has initiated numerous enforcement actions that culminate in consent decrees, fines, and imposed requirements related to privacy disclosures and the adoption of robust security measures [4]. The Federal Communications Commission (FCC) extends this regulatory umbrella into the realm of telecommunications and internet service providers by imposing restrictions and guidelines that protect consumers from unauthorized uses of their personal data, thereby ensuring that communication channels remain safe and secure.

The National Institute of Standards and Technology (NIST), although not traditionally recognized as an enforcement body, supplements these efforts by publishing widely respected guidelines and frameworks pertaining to cybersecurity risk management and privacy. The NIST Cybersecurity Framework, which offers a voluntary but comprehensive structure for identifying, protecting, detecting, responding to, and recovering from cyber threats, has become a de facto benchmark for private and public organizations endeavoring to safeguard sensitive data. This triad of agencies, each operating under distinct legislative mandates, reflects a multifaceted and evolving approach to data governance that seeks to reconcile rapid technological progress with foundational principles of individual autonomy, consumer trust, and systemic resilience [5]. The outcome is a continually shifting legal and regulatory ecosystem in which businesses and public institutions must invest in ongoing compliance strategies, maintain organizational awareness of emerging legal standards, and embrace robust data protection protocols that anticipate future developments in technology and policy.

Mechanisms for ensuring data privacy and security stem from a broad spectrum of technical, organizational, and procedural measures that span the entire information lifecycle, beginning with initial data collection and concluding with eventual disposal or anonymization. Federal guidelines and industry standards underscore the importance of robust encryption, secure authentication methods, continuous vulnerability assessments, and structured incident response protocols, all of which

must be seamlessly integrated into overarching corporate governance. Multifactor authentication, tokenization, zero-trust architectures, and the adoption of privacy-by-design principles underscore the evolving philosophy that data confidentiality and integrity should be maintained at every layer of an organization's operations [6]. Intrusion detection systems, behavioral analytics, and continuous monitoring tools further strengthen resilience by identifying irregular data flows or suspicious access patterns. Risk-based frameworks published by the National Institute of Standards and Technology serve as points of reference for entities seeking to align their cybersecurity measures with evolving threats, while sector-specific regulations mandate additional safeguards commensurate with the sensitivity of the data in question.

Compliance obligations for businesses and data processors encompass a broad range of responsibilities imposed by federal and state legislation, which stipulate transparency in data handling procedures, adherence to security benchmarks, and prompt reporting of breaches to relevant authorities. Entities governed by the Health Insurance Portability and Accountability Act must ensure that protected health information remains confidential through administrative controls, technical safeguards, and workforce training that emphasizes ethical data stewardship. Organizations subject to the Gramm-Leach-Bliley Act are required to develop and maintain information security programs proportionate to the complexity of their operations, as well as to inform customers regarding data sharing practices in a manner that promotes trust and accountability. Sector-agnostic requirements reinforced by consumer protection mandates often demand that companies adopt user-friendly privacy disclosures, implement mechanisms that allow individuals to exercise opt-out or deletion rights, and maintain detailed records of all data transfers. Penalties for noncompliance may entail substantial fines, injunctions against continued unlawful activities, and formal consent decrees that compel targeted improvements to data governance practices, thereby raising the stakes for entities that fail to meet established norms. Businesses engaged in interstate commerce face additional challenges due to jurisdictional variability, since compliance strategies must account for divergent state requirements that define personal data, outline permissible uses, and designate enforcement authority.

Case studies illustrating enforcement actions and regulatory compliance shed light on the manner in which federal and state agencies respond to perceived violations of data protection mandates, often through investigations that result in sanctions, public settlements, and prescriptive guidelines intended to deter similar incidents in the future. One noteworthy situation involved an extensive breach of consumer financial records, where the Federal Trade Commission intervened with a combination of hefty monetary penalties and mandated security reforms, sparking industry-wide conversations about vulnerabilities in centralized data repositories [7]. Another high-profile situation revolved around the unauthorized disclosure of personal health information, prompting enforcement authorities to highlight the importance of continuous workforce training, encryption of stored data, and rigorous access management. Actions undertaken by state attorneys general add further layers of scrutiny, thereby reinforcing the notion that compliance must be approached from a holistic perspective, encompassing both federal and local mandates. Organizations that proactively engage in self-assessment, align their systems with best-practice frameworks, and collaborate with regulatory bodies to refine internal policies often discover that a proactive stance yields reduced liability, enhances brand reputation, and fosters stronger stakeholder trust in an increasingly data-driven economy.

The pursuit of approximating United States legal approaches in other jurisdictions demands a nuanced understanding of the diverse cultural, economic, and legal contexts that shape data protection and privacy standards worldwide, with particular attention to the balance between individual rights, commercial interests, and government oversight. A comparative analysis with frameworks observed in the European Union and various Asian nations illustrates that regulatory philosophies can diverge on core principles, such as the scope of data subject rights, the degree of governmental intervention in corporate data handling, and the permissible breadth of data transfers beyond national borders. The General Data Protection Regulation (GDPR) in the European Union, grounded in fundamental rights to privacy and data portability, imposes a harmonized approach that transcends individual member states and establishes stringent obligations for data controllers, breach notification requirements, and extraterritorial reach that extends to entities outside the EU

offering services to EU-based data subjects [8]. Certain Asian markets exhibit a range of strategies, as evidenced by jurisdictions that have enacted comprehensive legislation with strong consent requirements and data localization mandates, while others have implemented more fragmented rules reflective of local privacy traditions, economic priorities, and governmental policy objectives. In these contexts, approximating US legal practices can involve reconciling the sectoral, agency-driven model prevalent in the United States with the omnibus, rights-centric orientation characteristic of the GDPR, or integrating specific American enforcement tools into jurisdictions that place greater emphasis on pre-emptive regulatory clearance.

Opportunities and challenges in adapting the US model emerge from the interplay between flexibility and fragmentation, since the American experience underscores the potential for innovation spurred by industry-specific regulations and decentralized, market-driven solutions, yet it also reveals complications arising from patchwork legislation that can create a complex compliance environment. Some jurisdictions may find value in implementing the US strategy of assigning different oversight responsibilities to specialized agencies, leveraging their expertise to establish targeted guidelines that address unique risks within healthcare, finance, telecommunications, and other high-stakes sectors. This sectoral approach, guided by robust enforcement from entities such as the Federal Trade Commission, may prove attractive to nations that prioritize adaptive regulatory mechanisms capable of accommodating evolving technologies [9]. However, replicating US practices may be hampered by divergences in constitutional or statutory foundations, since certain jurisdictions maintain uniform privacy laws that emphasize data minimization, strong user consent, and the principle of accountability in a more comprehensive manner. Policymakers navigating these cross-jurisdictional differences must confront the tension between harmonizing rules in a way that facilitates seamless data flows, and preserving local regulatory traditions that may give precedence to civil liberties or national security considerations. Moreover, implementing American modes of enforcement and compliance requirements could raise concerns regarding the efficacy of purely reactive penalties compared to preventive approaches favored in jurisdictions that require data protection impact assessments or official approvals prior to data processing.

Recommendations for harmonizing data circulation laws while respecting local contexts revolve around tailoring legislative frameworks that selectively incorporate elements of the US model in conjunction with best practices drawn from other systems, aiming to preserve core values of privacy, autonomy, and public trust. Authorities crafting legislation may wish to assess whether adopting a sector-based scheme can deliver the level of clarity and responsiveness needed for data-intensive industries, while still ensuring sufficient protections for individuals through centralized oversight or enhanced consumer rights. A viable strategy could involve forging international data transfer agreements that adopt salient American concepts, such as technology-neutral guidelines and robust enforcement mechanisms, but couple them with the rigorous governance structures seen in jurisdictions with omnibus privacy statutes. Cross-border dialogue among legislators, regulators, and industry representatives can serve as a catalyst for refining the interplay of technical standards, supervision, and enforcement strategies, thereby minimizing regulatory fragmentation and facilitating consistent safeguards for personal information across geographical boundaries.

In addition, knowledge transfer initiatives and capacity-building programs could deepen mutual understanding of how US actors handle breach reporting, consent management, and data subject redress, thus allowing emerging or reforming data protection regimes to adopt balanced solutions that reflect both the adaptability of US practice and the structured rigor of global standards. Such hybrid models, when thoughtfully aligned with local constitutional principles, market dynamics, and social expectations, hold promise for strengthening the collective resilience of international data ecosystems, reinforcing user confidence in digital platforms, and promoting interoperable privacy frameworks that can evolve in tandem with technological innovation.

5. Conclusions.

The analysis of the specific features of the legal regulation of electronic data circulation in the United States, alongside its potential approximations in other jurisdictions, demonstrates that sectoral

legislation, federal-state interplay, and the pivotal role of regulatory agencies have collectively produced a robust yet fragmented framework that seeks to balance privacy protection, commercial innovation, and consumer interests. This intricate legal environment underscores the importance of dynamic oversight mechanisms, transparent disclosure requirements, and risk-based approaches to data governance, all of which form an evolving response to technological progress and to mounting public expectations of accountability. Although divergences between federal statutes and state-level rules can complicate compliance efforts, they also encourage legislative innovation, foster nuanced enforcement strategies, and catalyze industry-driven solutions that address emerging cybersecurity threats and respond to shifting societal demands.

Prospects for further research lie in examining how these American practices can be more effectively harmonized with international standards and incorporated into wider global initiatives for data protection and cross-border information sharing. Comparative inquiry involving regions such as the European Union, Asia, and other jurisdictions can yield insights into common principles that underpin comprehensive privacy regimes and elucidate how local legal traditions can be preserved while integrating select elements of the US model. Further scholarly attention may explore the evolving role of artificial intelligence and machine learning in shaping data governance, along with the impact of transnational regulatory cooperation on establishing consistent and enforceable norms that bolster digital trust.

References:

1. Bamberger, K.A., & Mulligan, D.K. (2011). Privacy on the Books and on the Ground. *Stanford Law Review*, *63*(2), 247–315. Retrieved from: http://www.jstor.org/stable/41105400 [in English].
2. Caballero, T.G. (2024). Promoting Due Diligence: The Role of the Gramm-Leach-Bliley Act and Information Security Standards on Financial Institutions Protecting Consumers' Non-Public Personal Information (NPI). *2024 Spring Honors Capstone Projects,* 23. Retrieved from https://mavmatrix.uta.edu/cgi/viewcontent.cgi?article=1023&context=honors_spring2024 [in English].
3. Nicholas F. Palmieri III, *Who Should Regulate Data?: An Analysis of the California Consumer Privacy Act and Its Effects on Nationwide Data Protection Laws*, 11 Hastings Sci. & Tech. L.J. 37 (2020). Retrieved from: https://repository.uclawsf.edu/hastings_science_technology_law_journal/vol11/iss1/4 [in English].
4. Solove, D.J., & Hartzog, W. (2014). The FTC and the New Common Law of Privacy. *Columbia Law Review,* 114(3), 583–676. Retrieved from https://columbialawreview.org/wp-content/uploads/2016/04/Solove-Hartzog.pdf [in English].
5. Bowen, P., Hash, J., & Wilson, M. (2006). Information Security Handbook: A Guide for Managers. NIST Special Publication 800-100. *National Institute of Standards and Technology.* Retrieved from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf [in English].
6. Mylavarapu S. (2024). The Zero Trust Security Model and Cybersecurity in the Industries. *Journal of Student Research*, 13(1). Retrieved from: https://doi.org/10.47611/jsr.v13i1.2370 [in English].
7. About the Federal Trade Commission. *FTC*. Retrieved from: https://www.ftc.gov/about-ftc [in English].
8. Kuner, Christopher, Transborder Data Flows and Data Privacy Law (2013). *Oxford*. Retrieved from: https://academic.oup.com/book/5440 [in English].
9. Graham Greenleaf, The influence of European data privacy standards outside Europe: implications for globalization of Convention 108 (2012). *International Data Privacy Law*, Volume 2, Issue 2, pp. 68–92. Retrieved from: https://academic.oup.com/idpl/article-abstract/2/2/68/755358?redirectedFrom=fulltext [in English].

10. Schwartz, P.M., & Peifer, K.N. (2017). Transatlantic Data Privacy Law. *Georgetown Law Journal*, 106(1), 115–179. Retrieved from: https://www.law.georgetown.edu/georgetown-law-journal/wp-content/uploads/sites/26/2019/10/Transatlantic-Data-Privacy-Law_Schwartz-and-Peifer.pdf [in English].

Andriy Olefirenko,
PhD in Law,
Doctoral student of the PJSC «Higher Educational Institution
«Interregional Academy of Personnel Management»
ORCID: 0009-0005-1400-1172