©SHUTTERSTOCK.COM/MICHAEL TRAITOV

Compliance Operations Research: Navigating the Digital Regulation Revolution

Afonso Ferreira, Centre National de la Recherche Scientifique (CNRS)

Alfredo Goldman vel Lejbman, University of São Paulo (USP)

Nita Patel, Otis Elevator

This article explores how compliance operations may become pivotal in bridging the gap between technological innovation and regulatory requirements, ensuring that compliance is seamlessly embedded into operational workflows.

The European Union (EU) has emerged as a global leader in digital regulation. Through legislative frameworks, such as the General Data Protection Regulation (GDPR), the Artificial Intelligence Act (AI Act), the Digital Services Act (DSA), and the Digital Markets Act (DMA), the EU seeks to foster security, transparency, accountability, and fairness in the digital landscape. However, these laws also pose significant challenges for organizations, as they must operationalize compliance across dynamic and complex technological systems.

Historically, compliance has been approached as a series of periodic audits or checklists. Today, it has become an ongoing process embedded in every facet of an organization's operations.[1] To address this, a new field of compliance operations (ComplOps, for short) is emerging through the evolution of several related concepts, like RegTech, compliance-by-design, and compliance-as-code.[2,3] ComplOps will integrate regulatory adherence into organizations' technological practices, ensuring compliance is reactive and anticipatory. This anticipation will allow for better systems design and implementation.

This short article argues that ComplOps research will become indispensable for aligning innovation with

Digital Object Identifier 10.1109/MC.2025.3591937
Date of current version: 22 December 2025

regulation. By examining the EU's digital laws and using a case study from recent research, it demonstrates the value of embedding compliance within organizational systems. We use the EU's digital regulation as a main example, but the ComplOps concept can be applied to diverse regulatory ecosystems.

THE RISE OF A WORLD OF DIGITAL LAWS

The EU's regulatory push, exemplified by the GDPR, the DSA, the DMA, and the AI Act, among many others, is reshaping the digital landscape.[a] These laws aim to protect individual rights, promote online security, and ensure responsible digital transformation. Yet, they demand more than just technical solutions. They necessitate profound operational, cultural, and systemic shifts within organizations, not only in Europe but worldwide, as several EU's digital laws have extraterritoriality, for instance by regulating supply-chains.

The GDPR, introduced in 2018, revolutionized data privacy and security protocols, pushing organizations to rethink how they handle personal data. Compliance requires not only technical measures, such as encryption but also organizational transformations, including appointing data protection officers and conducting continuous privacy audits.

The DSA and DMA, enacted in 2022, impose stringent rules on online platforms to protect users and promote fairness. The DSA mandates content moderation and real-time reporting, while the DMA targets anticompetitive behavior by imposing additional responsibilities on gatekeeper platforms.

The AI Act, enacted in 2024, takes a forward-looking approach to regulating AI technologies. It introduces a risk-based framework for AI systems, demanding compliance not just in terms of technical safeguards but also regarding ethical and societal impact. Organizations must adopt a holistic approach, ensuring transparency, fairness, and accountability in AI systems. The cybersecurity of high-risk AI systems is further regulated by the Cyber Resilience Act, also from 2024.

> ComplOps will offer a framework for developing scalable systems that can evolve alongside regulatory changes.

These regulations reflect the EU's ambition to harmonize technology with human-centric values, creating a model for the world to follow. However, they also present a compliance maze, where organizations must navigate conflicting requirements and adapt swiftly to technological advancements.[3]

WHAT IS COMPLOPS, AND WHY WILL IT MATTER?

Compliance operations (ComplOps) will represent a paradigm shift in how organizations approach regulatory adherence. Rather than viewing compliance as a discrete function, ComplOps will integrate it into operational processes and leverage sophisticated, technology-enabled approaches necessary for the complex reality of modern regulatory environments. Organizations will be able to ensure that they are continuously aligned with evolving regulatory requirements by embedding compliance within the development cycle as in security operations, development operations (DevOps), machine learning operations (MLOps), and agile methodologies.

Therefore, ComplOps is the systematic integration of regulatory compliance requirements into software development and operations workflows through automated monitoring, adaptive systems, and continuous verification processes.

During the past decades, software development has evolved considerably, in particular in order to avoid silos in its cycles. Two clear examples with direct benefits came from integrating procedures, usually scheduled at the end of the process, much earlier in the software development cycle. With this, automated tests are now performed during the development process, or sometimes even earlier when well-known techniques, such as test-driven development are used. The same happened to the homologation stage of software verification, which is now usually integrated using DevOps with continuous integration/continuous delivery. Nowadays, both changes are well accepted and do not compromise the resulting software quality.

The complexity and rapid evolution of legal landscapes are making ComplOps research a necessity. The high stakes of noncompliance—ranging from substantial fines to reputational damage—further underscore the need for adaptive compliance systems. ComplOps will offer a framework for developing scalable systems that can evolve alongside regulatory changes, providing a strategic advantage in fast-moving industries.

A more concrete example of the impact of policies on software

[a] Available at: https://www.nldigitalgovernment.nl/overview/europe-and-international/european-legislation-and-regulation/.

development can be found in the "Right to be Forgotten." When this policy was implemented, the impact on development was quite low, restricting its impact to the removal of personal data from Databases and from aggregated information. With the advance of ML, it is much more difficult to erase the data used in training.[4] So, the same policy has a larger impact nowadays.

> Collaboration between legal scholars, policymakers, and technologists is essential to bridging the regulatory theory and operational practice gap.

CASE STUDY: INSIGHTS FROM COMPLIANT-BY-DESIGN AI FOR THE EU MARKET

An example of what ComplOps could bring into practice can be found in the work by Canavese et al.[5] This study explores how organizations can integrate EU legal frameworks into AI development. The paper proposes a compliance-by-design approach, incorporating automated compliance checks into AI systems to ensure alignment with laws such as the AI and the CR Acts.

This case study highlights the importance of continuous monitoring and adaptive systems. By embedding compliance into the lifecycle of AI systems, organizations can ensure real-time compliance and swiftly respond to regulatory changes. Additionally, it underscores the value of cross-disciplinary collaboration, where legal scholars, engineers, and operational managers work together to translate regulatory requirements into actionable system features.

The insights obtained are that such legislation can now translate directly into functional, technical, and organizational requirements that impact the IT system to be deployed. In the case of the AI Act, examples of such requirements for AI systems that are meant to be sold in the EU market are as follows:

- *Traceability by logs*: To ensure a level of traceability of the functioning of a high-risk AI system [...] logging capabilities shall enable the recording of events relevant for: [...] identifying situations that may result in the high-risk AI system presenting a risk [...] facilitating the post-market monitoring [...] monitoring the operation of high-risk AI systems.
- *Data confidentiality:* [The system must] protect the confidentiality of stored, transmitted or otherwise processed data, personal or other.
- *Human oversight*: High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that can be effectively overseen by natural persons.

This research indicates that by automating compliance and fostering real-time adaptation, well designed and implemented ComplOps principles will certainly help organizations to remain compliant while innovating within regulatory frameworks.

A RESEARCH AGENDA FOR COMPLOPS

We believe that the best way to predict the future is by designing it. Therefore, we propose in the following several critical interdisciplinary research directions prioritized by impact (high, medium, or low) and timeline (short-term of 1–2 years, medium-term of 2–4 years, or long-term of 4+ years) to make ComplOps a reality in future:

- *Clear concept definition (high, short-term)*: ComplOps should receive a widely accepted interpretation. It is important to have a precise interpretation. Some other well-known terms, such as DevOps[6] or MLOps,[7] today still have ambiguous interpretations, which hampers their wider acceptance.
- *Metrics for compliance (high, short-term)*: Establishing frameworks to assess the efficiency and effectiveness of compliance systems and creating benchmarking frameworks.
- *Toolbox development (high, medium-term)*: Adapting current DevOps tools for ComplOps practices by developing compliance-as-code frameworks for automation and continuous monitoring.
- *Balancing legal interpretability with computational implementation (high, medium-term)*: Ensuring that complex legal texts are accurately translated into system requirements.
- *Compliant software development tools (medium, medium-term)*: integration of tools that ensure that the software being developed is compliant (for example, by accepting only libraries that are themselves compliant).
- *Automating regulatory updates (medium, medium-term)*: Developing systems capable of adapting to changes in the law, that is, the new compliance requirements can be tested and integrated in case of need.
- *Cross-jurisdictional compliance (medium, long-term)*: Addressing the challenges of managing compliance across conflicting regulations in global operations.
- *Audit and evidence management (medium, long-term)*:Development of cryptographically secured audit materials that create

tamper-proof records of all compliance-related activities, decisions, and changes.

- *Patterns and good practices (low, long-term)*: Providing ways to discover and share the patterns and good practices to improve software development and maintenance.

Collaboration between legal scholars, policymakers, and technologists is essential to bridging the regulatory theory and operational practice gap. Industry case studies will be invaluable for testing ComplOps innovations in real-world settings.

The rapid evolution of digital laws, particularly in the EU, points to the advent of technically advanced compliance-by-design software development, highlighting the need for a robust ComplOps research agenda. ComplOps will offer a pathway to embedding compliance in the heart of organizational operations as the regulatory landscape becomes more complex. By blending cross-disciplinary collaboration into software engineering, ComplOps will transform compliance from a burden into an enabler of competitive advantage.

The computing community must lead the way in operationalizing compliance. By kickstarting ComplOps research, we will ensure that technology and regulation evolve in tandem, fostering a future where compliance is not just about adherence but also about enhancing the ethical and societal impact of digital transformation.

ACKNOWLEDGMENT

This work was conducted within the framework of the virtual laboratory “Techno-Human Systems of the Future” (THUS the Future) of the International Research Center (IRC) CNRS-USP. It was partially supported by both institutions and part of the CNRS International Research Project Megalopolis. The first author was partially supported by the European research projects H2020 LeADS (GA 956562) and Horizon Europe DUCA (GA 101086308), ARN TrustIn- Clouds, and CNRS IRN EU-CHECK. The second author was partially supported by the FAPESP project 19/26702-8 and by the CNPq Grant 308996/2022-4. The authors would like to thank Camila A. da Silva for her unwavering support.

REFERENCES

1. S. Sadiq and G. Governatori, “Managing regulatory compliance in business processes,” in *Handbook on Business Process Management 2: Strategic Alignment, Governance, People and Culture*, 2n ed., J. vom Brocke and M. Rosemann Eds., Berlin, Germany: Springer-Verlag, 2015, pp. 159–175.
2. “A user’s guide to RegTech: Navigating the challenges and what success looks like,” KPMG, Amstelveen, The Netherlands, 2022. [Online]. Available: https://assets.kpmg.com/content/dam/kpmg/uk/pdf/2022/11/innovate-finance-regtech-industry-and-adoption.pdf
3. Harvard Business Review Analytic Services, “Digitizing risk and compliance: How AI can help manage a growing challenge,” PwC, London, U.K. Accessed: Apr. 11, 2025. [Online]. Available: https://assets.ctfassets.net/29eiqqcixp18/436dExy1tJf2zlJXIDZ1cY/216aaa72c3d913de8962763b89baaf7a/Risk_Managing_risk_and_compliance_in_the_digital_age_eBook.pdf
4. C. Libera, L. Miranda, F. Bernardini, S. Mastelini, and J. Viterbo, “Right to be forgotten’: Analyzing the impact of forgetting data using K-NN algorithm in data stream learning,” in *Proc. Int. Conf. Electron. Government*, Cham, Switzerland: Springer-Verlag, 2022, pp 530–542.
5. D. Canavese, A. Ferreira, R. Laborde, and A. Benzekri, “Artificial intelligence systems in the European Union: Guidelines and architectures for compliance-by-design,” HAL, Lyon, France, 2024. [Online]. Available: https://hal.science/hal-04794994
6. L. Leite, C. Rocha, F. Kon, D. Milojicic, and P. Meirelles, “A survey of DevOps concepts and challenges,” *ACM Comput. Surv.*, vol. 52, no. 6, pp. 1–35, 2019, doi: 10.1145/3359981.
7. D. Kreuzberger, N. Kuhl and S. Hirschl, “Machine learning operations (MLOps): Overview, definition, and architecture,” *IEEE Access*, 11, pp. 31,866–31,879, 2023, doi: 10.1109/ACCESS.2023.3262138.

AFONSO FERREIRA is a Centre National de la Recherche Scientifique research director at the Toulouse Institute of Computer Science Research (IRIT), 31400 Toulouse, France. Contact him at afonso.ferreira@irit.fr.

ALFREDO GOLDMAN VEL LEJBMAN is a professor at the University of São Paulo, Institute of Mathematics and Statistics (IME), São Paulo, 05508-090, Brazil. Contact him at gold@ime.usp.br.

NITA PATEL is the vice president of engineering at Otis Elevator, Farmington, CT 06002 USA. Contact her at nita.patel@ieee.org.