ComplOps Research: Navigating the Digital Regulation Revolution

Afonso Ferreira, Alfredo Goldman

ComplOps Research: Navigating the Digital Regulation Revolution

AFONSO FERREIRA
Centre National de la Recherche Scientifique (CNRS)
Institut de Recherches en Informatique de Toulouse
France
https://www.linkedin.com/in/cyberfuture/

ALFREDO GOLDMAN
Instituto de Matemática e Estatística
Universidade de São Paulo (USP)
Brasil
gold@ime.usp.br

Abstract — *With the European Union leading a regulatory transformation through laws like the General Data Protection Regulation (GDPR), the Artificial Intelligence Act (AI Act), the Digital Services Act (DSA), and the Cyber Resilience Act (CRA), organizations face unprecedented compliance challenges. In this context, the nascent field of Compliance Operations (ComplOps) is critical for aligning technological systems with ever-evolving regulatory demands. This paper explores how ComplOps can bridge the gap between technological innovation and regulatory requirements, ensuring that compliance is seamlessly embedded into operational workflows. A case study from recent research demonstrates how compliance can be operationalized in AI systems.*

Index Terms — Digital legislation, EU Regulation, Compliance, Software Regulation, Software Development

1. INTRODUCTION

The European Union 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, the field of ComplOps is emerging through the evolution of several related concepts, like

RegTech, Compliance-by-Design, and Compliance-as-Code [2, 3]. ComplOps integrates regulatory adherence into the technological practices of organizations, ensuring that compliance is not only reactive but anticipatory. This anticipation allows for better systems design and implementation.

This short article argues that ComplOps research is indispensable for aligning innovation with 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.

2. 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[1]. These laws aim to protect individual rights, promote on-line 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 (DPOs) 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 anti-competitive behaviour by imposing additional responsibilities on gatekeeper platforms.

The AI Act 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 (CRA), enacted in 2024, as was the case of the AI Act.

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].

3. WHAT IS COMPLOPS, AND WHY DOES IT MATTER?

Compliance Operations (ComplOps) represents a paradigm shift in how organizations approach regulatory adherence. Rather than viewing compliance as a discrete function, ComplOps integrates it into operational processes. Organizations can ensure that they are continuously aligned with evolving regulatory requirements by embedding compliance within the development cycle as in SecOps, DevOps, MLOps, and agile methodologies.

During the past decades, software development evolved considerably, in particular in order to avoid silos in its cycles. Two clear examples with direct benefits came from integrating procedures,

---

[1] #Dydlodeoh#dw#kwwsv=22zzz1qgljlwdojryhuqphqw1qr2ryhuylhz2hxursh0dqg0lqwhuqdwlrqdo2hxurshdq0ohjlvodwlrq0dqg0uhjxodwlrq2###

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 TDD (Test Driven Development) are used. The same happened to the homologation stage of software verification, which is now usually integrated using DevOps with CI/CD (Continuous Integration/Continuous Delivery). Nowadays, both changes are well accepted and do not compromise the resulting software quality.

More recently, several techniques have been proposed for systems involving Machine Learning in MLOps. Here, the silos could be found in the way specialists in ML were dedicated to creating and training models, while the developers would then use the models afterward to develop their systems. This approach would work well if the ML models did not evolve, which is far from reality. Therefore, MLOps brings together ML experts and software developers early in the systems development phase.

ComplOps research is urgent due to the complexity and rapid evolution of legal landscapes. The high stakes of non-compliance – ranging from substantial fines to reputational damage – further underscore the need for adaptive compliance systems. ComplOps should 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 Development can be found in the "Right to be Forgotten". When this policy was implemented, the impact on development was quite low, restricting the 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.

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

A key example of ComplOps in practice can be found in [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 they 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 should help organizations to remain compliant while innovating within regulatory frameworks.

5. A RESEARCH AGENDA FOR COMPLOPS

To advance ComplOps, several critical interdisciplinary research directions should be prioritized:

- *Clear concept definition* — Compliance Operations should receive a widely accepted interpretation. In this text we provided some basic background for it. However, it is very important to have a precise interpretation. Some other well-known terms, such as Dev-Ops [6] or MLOps [7], today still have ambiguous interpretations, which hampers their wider acceptance.
- *Automating regulatory updates* — Developing systems capable of adapting to changes in the law, i.e., the new compliance requirements can be tested and integrated in case of need.
- *Toolbox development* — Adapting current DevOps tools for ComplOps practices.
- *Integration of tools that ensure that the software being developed is compliant* (e.g. by accepting only libraries that are themselves compliant) — Complex systems are composed of many different pieces like libraries or modules, each of which may have specific licenses and compliance rules. This can leverage a difficult problem in software evolution, as the licenses or compliance requirements may change for new library or module versions. This problem is also known as software supply chains.
- *Balancing legal interpretability with computational implementation* — Ensuring that complex legal texts are accurately translated into system requirements.
- *Cross-jurisdictional compliance* — Addressing the challenges of managing compliance across conflicting regulations in global operations.
- *Metrics for compliance* — Establishing frameworks to assess the efficiency and effectiveness of compliance systems.
- *Patterns and good practices* — 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 gap between regulatory theory and operational practice. Industry case studies will be invaluable for testing ComplOps innovations in real-world settings.

6. CONCLUSION

The rapid evolution of digital laws, particularly in the EU, highlights the need for a robust ComplOps research agenda. As the regulatory landscape becomes more complex, ComplOps offers a pathway to embedding compliance in the heart of organizational operations. By blending cross-disciplinary collaboration into software engineering, ComplOps can transform compliance from a burden into an enabler of competitive advantage.

The computing community must lead the way in operationalizing compliance. By prioritizing ComplOps research, we can 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.

ACKNOWLEDGMENTS

This work was conducted within the framework of the virtual laboratory "Techno-Human Systems of the Future" (THUS the Future) of the International Research Centre (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". *Handbook on Business Process Management* 2: Strategic Alignment, Governance, People and Culture, Second Edition, 2015. https://doi.org/10.1007/978-3-642-01982-1_8 (Book Chapter)

2. KPMG. "A user's guide to RegTech" https://assets. kpmg.com/content/dam/kpmg/uk/pdf/2022/11/innovate-finance-regtech-industry-and-adoption.pdf (URL)

3. Harvard Business Review Analytic Services. "Digitizing Risk and Compliance: How AI Can Help Manage a Growing Challenge". Sponsored by PwC. https://assets.ctfassets.net/29eiqqcixp18/436dExy1tJf2zlJXIDZ1cY/216aaa72c3d913de8962763b89baaf7a/Risk_Managing_risk_and_compliance_in_the_digital_age_eBook.pdf (White paper)

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: Janssen, M., et al. *Electronic Government*. EGOV 2022. Lecture Notes in Computer Science, vol 13391. Springer, Cham. https://doi.org/10.1007/978-3-031-15086-9_34 (Conference paper)

5. D. Canavese, A. Ferreira, R. Laborde and A. Benzekri, "Artificial Intelligence Systems in the European Union: Guidelines and Architectures for Compliance-by-Design," 2024. *HAL*. https://hal.science/hal-04794994 (URL)

6. L. Leite, C. Rocha, F. Kon, D. Milojicic, and P. Meirelles, "A Survey of DevOps Concepts and Challenges". ACM Comput. Surv. 52, 6, Article 127, 2019 , 35 pages, https://doi.org/10.1145/3359981

7. D. Kreuzberger, N. Kuhl and S. Hirschl, "Machine Learning Operations (MLOps): Overview, Definition, and Architecture," *IEEE Access*, 11, 2023. https://doi.org/10.1109/ACCESS.2023.3262138