Interoperability in Complex and Socio-Technical Information Systems: A Critical Challenge for the Next Decade

Rita Suzana Pitangueira Maciel[1], José Maria N. David[2], Elisa Yumi Nakagawa[3]

[1]Federal University of Bahia (UFBA) Campus de Ondina –
Salvador – BA – Brazil

[2] Universidade Federal de Juiz de Fora (UFJF)
Juiz de Fora - MG - Brasil

[3]Universidade de São Paulo (USP)
São Paulo - SP - Brasil

rita.suzana@ufba.br, jose.david@ufjf.br, elisa@icmc.usp.br

Abstract: *Socio-technical information systems integrate software, hardware, people, and organizations, and operate in dynamic environments with emergent behaviors that complicate predictability and control. Interoperability in these systems extends beyond technical aspects to legal, cultural, and organizational dimensions. Regulatory frameworks must adapt to AI-driven decision-making, cultural factors influence platform adoption, and organizations must restructure to support autonomous workflows. Despite various attempts to address interoperability challenges, issues persist due to proprietary technologies, inconsistent data models, and regulatory barriers. The lack of widely adopted standards in cloud computing, IoT, and blockchain exacerbates these difficulties. Socio-technical interoperability requires comprehensive solutions that address legal, ethical, and organizational concerns while ensuring trust, accountability, and transparency. Research areas include legal policy, cultural implications, organizational adaptation, and AI-driven interoperability mechanisms. Addressing these challenges is critical to prevent fragmented ecosystems, regulatory bottlenecks, and declining trust in digital services, and to position Brazil as a leader in sustainable and interoperable socio-technical systems.*

Palavras-chave*: Socio-technical Information Systems, Interoperability, Regulatory frameworks, Organizational adaptation, Ethical and legal challenges.*

1. The Challenge

Socio-technical information systems are complex systems characterized by the interaction of multiple heterogeneous components — such as software, hardware, people, and organizations — operating within dynamic and often unpredictable environments. These systems also exhibit emergent behaviors that arise from the interactions among their components, making their outcomes difficult to predict and control. As technology

advances, software systems are increasingly assuming tasks that were traditionally performed by humans, further intensifying their complexity (Hajjaji et al., 2021).

In socio-technical information systems (Cafezeiro et al, 2017), interoperability is not limited to technical concerns; it also encompasses legal, cultural, social network, and organizational dimensions (Maciel et al., 2024). These dimensions emerge from the need to support new ways for the interaction between the various elements of these systems. For instance, regulatory frameworks must be adapted to the integration of AI-driven decision-making processes, cultural differences must be considered as they influence the adoption of digital platforms, and organizational structures must evolve to accommodate distributed and autonomous workflows. As these systems expand and interconnect, ensuring seamless collaboration among them and among their diverse components becomes essential for achieving intended goals and functions.

Since information systems started to be developed, several proposals and solutions have been proposed to solve interoperability issues. However, interoperability remains a persistent, critical, and open challenge (Maciel et al., 2017). Technical and syntactic interoperability issues persist due to the lack of widely adopted de facto standards, particularly for more recent but increasingly adopted technologies, including cloud computing, Internet of Things (IoT), and blockchain platforms. These issues often arise due to competing proprietary technologies, divergent data models, and inconsistent communication protocols. The industry has attempted to address these technical issues through the adoption of standards, common agreements, and translation mechanisms. However, particularly, socio-technical interoperability cannot rely solely on these approaches, as its challenges are deeply embedded in human, organizational, and regulatory contexts.

The growing dependence of diverse industries — e.g., healthcare, finance, public administration, transportation, and smart cities — on complex information systems has increasingly demanded effort to improve interoperability at multiple levels, from technical and syntactic to organizational, legal, and cultural. Without significant advancements, these systems risk becoming fragmented, leading to inefficiencies, security vulnerabilities, and lost opportunities for innovation.

From a regulatory perspective, a lack of interoperability can create legal bottlenecks that hinder data sharing and cross-border collaborations. For example, privacy regulations such as the General Data Protection Regulation (GDPR) (European Union, 2016) in Europe and Brazil's General Data Protection Law (LGPD) (Brazil, 2018) impose strict requirements on data exchange. Yet, there is no universally accepted framework for ensuring compliance while enabling seamless interoperability. Cultural differences also complicate interoperability efforts, as software solutions designed for one region may not align with the values, behaviors, or linguistic nuances of another. In an organizational context, interoperability issues can result in inefficiencies and missed

opportunities for automation and digital transformation. Social networks and digital platforms also introduce new forms of socio-technical interoperability challenges, as interactions between users, automated agents, and organizations require mechanisms for trust, accountability, and transparency.

Failing to address these issues may have significant consequences. Fragmented software ecosystems can stifle economic growth, as businesses struggle to scale their digital operations across different platforms and jurisdictions. Regulatory bottlenecks can slow down innovation, preventing companies from leveraging emerging technologies, such as AI, blockchain, and IoT. Additionally, a lack of interoperability can reduce public trust in digital services, particularly in areas such as e-government, digital identity, and healthcare.

In the software development context, teams must deal with diverse challenges (Amershi et al., 2019), such as distributed devices and sensors, heterogeneous behavior configuration, intrinsic characteristics, and interoperability with other sensors and systems (Motta, De Oliveira and Travassos, 2018). IoT systems (which often involve several heterogeneous devices and utilize AI techniques) require a significant amount of computational resources to process large volumes of data while still requiring complex qualities, such as sustainability and carbon footprint reduction.

As we need to deal with the continuous changes imposed by these information systems (and their quality attributes), interoperability solutions also need to be rethought. In this context, the solutions proposed for traditional information systems, aimed at supporting full interoperability, should not be discarded but adapted to complex and social-technical information systems. Additionally, new challenges arise to adapt them to new technologies and emerging quality attributes, such as sustainability and carbon neutrality. New interoperability solutions must continually address these attributes.

While technical interoperability relies on standardization and agreement on protocols, socio-technical interoperability requires a more comprehensive approach that integrates legal, cultural, organizational, and social dimensions. The Brazilian Information Systems community must take a leading role in defining conceptual and technological frameworks to enable comprehensive interoperability in the next decade (Cafezeiro et al., 2017).

Some key areas for research and development include:

1. **Legal and Policy Frameworks** – Developing policies and legal frameworks that facilitate data sharing and interoperability while ensuring compliance with privacy and security regulations.

2. **Cultural and Ethical Considerations** – Investigating how cultural differences impact the adoption and interoperability of digital platforms and proposing strategies for inclusive and context-aware system design.

3. **Organizational Adaptation** – Exploring new business models and organizational structures that promote interoperability and collaboration across different social-technical systems.

4. **Socio-Technical Infrastructure** – Designing architectures that incorporate mechanisms for trust, accountability, and transparency in socio-technical interactions, such as verifiable digital identities and decentralized governance models.

5. **Technological Solutions** – Advancing technologies, such as AI-driven interoperability agents, semantic web techniques, and smart contracts, to facilitate seamless interactions across heterogeneous systems.

The challenge of socio-technical interoperability intersects with several other critical areas, including cybersecurity, digital governance, ethics in AI, and sustainable digital transformation. For instance, interoperability solutions must align with cybersecurity frameworks to ensure that data exchanged across systems remains secure and tamper- proof. Additionally, interoperability is closely linked to technological advancements in cloud computing, IoT, and blockchain. These platforms serve as a backbone of modern digital information systems ecosystems, yet their interoperability challenges remain unsolved. Addressing these issues requires coordinated efforts from academia, industry, and policymakers to develop interoperable frameworks that enable seamless data exchange and service integration.

2. Conclusion

Interoperability in complex and social-technical information systems is one of the most pressing challenges for the Brazilian Information Systems community over the next decade. As these systems become more pervasive and essential to economic and social development, overcoming interoperability barriers is critical to ensuring their effectiveness, security, and inclusivity.

If left unaddressed, interoperability issues may lead to fragmented ecosystems, regulatory hurdles, and reduced trust in digital services. To mitigate these risks, a multidisciplinary approach is necessary, bringing together expertise from various domains to define comprehensive interoperability frameworks and solutions. By leading efforts in this area, Brazil will have the opportunity to position itself as an innovator in designing and implementing interoperable and sustainable socio- technical systems that could benefit society.

References

Amershi, S. et al. (2019) “Software engineering for machine learning: A case study”. In: 2019 IEEE/ACM 41st International Conference on Software Engineering: Software Engineering in Practice (ICSE-SEIP). 2019. p. 291-300.

Cafezeiro, I. et al. (2017) “Strengthening of the Sociotechnical Approach in Information Systems Research”. Grand Research Challenges in Information Systems in Brazil 2016-2026. p. 133-147.

Hajjaji, Y. et al. (2021) “Big data and IoT-based applications in smart environments: A systematic review”. Computer Science Review, v. 39, p. 100318.

Motta, R. et al. (2018) “On challenges in engineering IoT software systems”. In: XXXII Brazilian Symposium on Software Engineering (SBES). p. 42-51.

Maciel, R. et al. (2024) “Systems Interoperability Types: A Tertiary Study”. ACM Computing Survey 56, 10, Article 254, 37 pages. https://doi.org/10.1145/3659098

Maciel, R. et al. (2017) “Full interoperability: Challenges and opportunities for future information systems”. Grand Research Challenges in Information Systems in Brazil 2016-2026, p. 107–116.

European. Union (2016) “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46,” Off. J. European Union, v. 59, n. 1–88, p. 294.

Brasil, (2018) “Lei Geral de Proteção de Dados Pessoais (LGPD),”. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm