The Sovereign Loop: A Novel Model for Trust-Calibrated Human-Centered AI in Data-Scarce Environments

Fjolla Berisha, Leidiane Da Silva, Peter Mooney, Zohreh Pourzolfaghar, and Markus Helfert

Abstract The advancement of Human-Centered AI (HCAI) is dependent on access to large and diverse datasets. However, the mechanisms for acquiring this data are plagued by a fundamental crisis of trust and a lack of respect for data sovereignty, creating a vicious cycle that starves AI systems. This paper introduces the Sovereign Loop, a novel model that resolves this tension by architecting systems where trust is not a prerequisite but a dynamically generated outcome of human-centric design. We argue that embedding sovereignty-by-design is the critical first step in a virtuous cycle: it enables trust calibration, which facilitates the flow of high-quality, consented data. This data fuels the development of robust HCAI systems that are, by architectural imperative, designed to amplify human agency through explainable, collaborative interfaces. The positive experience of this human-AI partnership feedback is to strengthen trust, justifying further data sovereignty. We formalize this feedback loop and conceptually validate its hypotheses through an agent-based simulation. Our work illustrates how sovereignty can be the human dimension of HCAI by embedding agency and consent directly into system design.

F. Berisha (✉)
Computer Science, National University of Ireland Maynooth, Maynooth, Ireland
e-mail: fjolla.berisha.2024@mumail.ie

P. Mooney
Associate professor, Computer Science, National University of Ireland Maynooth, Maynooth, Ireland
e-mail: peter.mooney@mu.ie

L. Da Silva
School of Business, National University of Ireland Maynooth, Maynooth, Ireland
e-mail: LEIDIANE.GORETEDASILVA.2021@MUMAIL.IE

Z. Pourzolfaghar
Assistant professor, School of Business, National University of Ireland Maynooth, Maynooth, Ireland
e-mail: Zohreh.Pourzolfaghar@mu.ie

M. Helfert
Professor, School of Business, National University of Ireland Maynooth, Maynooth, Ireland
e-mail: markus.helfert@mu.ie

S. Misra et al. (eds.), *2nd International Conference on Digital Sovereignty*,
Springer Proceedings in Complexity, https://doi.org/10.1007/978-3-032-21524-6_2

1 Introduction

The grand promise of Human-Centered AI (HCAI) is a future where artificial intelligence amplifies human intelligence, creating partnerships that surpass the capabilities of either entity alone [1, 2]. From diagnostic assistants in medicine to collaborative design tools in engineering, the potential for positive transformation is vast [3, 4]. While AI systems offer significant potential benefits, their successful application remains a human-driven endeavor. Consequently, integrating AI into intricate human workflows necessitates embedding human-centered design principles at the core of both algorithmic research and implementation [5]. Guidelines for fostering human-AI interaction that encourage granular feedback and transparent communication of action consequences [3], offer valuable user-centric design principles. However, the realization of this promise is threatened by a foundational paradox. The sophisticated AI models that underpin effective collaboration are insatiably data hungry. Their performance, fairness, and robustness are directly correlated to the quantity, quality, and diversity of the data on which they are trained [6, 7]. Yet, the very ecosystems required to generate and share this data are crumbling under the weight of a pervasive crisis of trust [8, 9] and a growing demand for data sovereignty [10–12]. High-profile data breaches, the extractive practices of surveillance capitalism [13], and the opaque use of personal data have led to justifiable public skepticism [13, 14]. This has triggered a regulatory response, most notably the General Data Protection Regulation (GDPR) [13] in Europe and the evolving AI Act [6, 10], which promotes the principles of data sovereignty, the right of individuals and collectives to control their data [15]. Consequently, organizations find themselves caught between the need for more data and the increasing difficulty acquiring it ethically and legally [11, 16]. This creates a critical impediment: the need for data to build HCAI systems is inversely related to the ability to acquire that data in the absence of such systems. This is a cold-start problem for AI.

A review of the literature reveals a critical gap: the concepts of data sovereignty, trust, and Human-Centered AI (HCAI) are largely examined in isolation. While each field has advanced considerably, little research explores how these dimensions interact dynamically or how they can function as components of an integrated, self-reinforcing system. This paper addresses two interconnected challenges. The first is the cold-start problem in developing HCAI systems due to the fact that AI systems depend on user trust and participation, yet such trust cannot emerge without mechanisms that guarantee user control and sovereignty over data use [15]. The second challenge is the need to make sovereignty itself the human element in HCAI, embedding human agency, consent, and oversight directly into system design rather than treating them as external governance layers.

The main contribution of this paper is to reframe the cold-start paradox of Human-Centered AI as a problem of missing sovereignty. It argues that AI cannot become human-centered without first embedding mechanisms of control, consent, and participation that make human agency technically enforceable. The remainder of the paper is organized as follows: Section 2 presents the background, Sect. 3 outlines the methodology, Sect. 4 introduces the Sovereign Loop model along with the simulation, Sect. 5 discusses the limitations, and Sect. 6 concludes the paper.

2 Background

HCAI is best understood not as a form of automation but as a partnership between humans and AI [3, 17]. It moves beyond the paradigm of AI as a mere tool or an autonomous agent towards a framework of mixed-initiative interaction and shared autonomy [18]. Research in this domain emphasizes the critical importance of user agency and reliability [19]. Effective collaboration requires that humans remain in control, able to understand, predict, and override the AI's actions as argued by [20]. The field of Explainable AI (XAI) is a direct response to this need, seeking to make AI decision-making processes transparent and interpretable to human partners [21, 22]. According to [18], a practical way to realize the synergy between AI and humans is by pairing AI's rapid ability to process information with the intuitive judgment and deeper insight that humans excel at. As [19] note, Machine Learning (ML) alone is insufficient for critical domains such as medicine; humans must remain part of the ML loop. This need stems from two factors: ML models rely on high-quality, unbiased data, and human oversight is vital to detect flaws and build trust. Furthermore, humans' experiential judgment is indispensable for identifying new patterns and managing complex situations [19]. However, there remains limited understanding of how to navigate the trade-offs involved in combining human and artificial agency, as well as how such systems ought to be evaluated and made accountable, as argued by [23]. Without this agency and reliability, collaboration breaks down, and the system becomes one of subjugation or automation, not partnership [15, 23–25].

The concept of data sovereignty provides the mechanism to implement this agency within the data economy [12, 26]. While often discussed in terms of jurisdiction [15], its more profound implication lies in control and self-determination [15]. Scholarly work extends this principle to individuals, framing sovereignty as a capability, the power to grant and withdraw consent, to negotiate terms of use, and to derive benefit from one's own data [12, 27]. In this view, sovereignty is the practical portrayal of agency over one's digital self [17]. Furthermore, data sovereignty advances a model of agency in which clearly defined and enforceable data-use agreements enable controlled access and utilization [12]. Crucially, data sovereignty is enacted through dynamic usage control mechanisms that extend beyond static consent at collection, enabling continuous oversight of who accesses the data, how it is used, and for what purposes throughout its lifecycle [16]. It is this verifiable, technically enforced control that provides the foundation for the next critical component: trust.

Linking agency to collaboration is the concept of trust [9, 28]. Trust is a critical and extensively studied concept within the fields of Human-Computer Interaction (HCI) and Human-Centered AI (HCAI). It significantly influences how individuals interact with, adopt, and utilize technology, particularly AI systems [29]. In the context of automation and human-computer interaction, trust is not a monolithic concept but a calibratable state [8, 30]. Research differentiates between calculative trust, which is based on a rational assessment of risks and rewards, and relational trust, which is built over time through positive experiences and demonstrated reliability [30]. According to [8], performance-focused trust calibration feedback in automation aims to inform humans about what the system can and cannot do, rather than explaining its internal processes [8, 18].

Trust and data sovereignty are foundational principles underpinning major European digital initiatives and policy frameworks, including Gaia-X, the International Data Spaces (IDS), FIWARE, and the EU Data Act [31, 32]. These initiatives share the goal of empowering users with greater control over their data, fostering secure and transparent data exchange, and promoting a competitive, innovation-driven digital ecosystem [22, 24, 32–34]. The Fraunhofer-led International Data Spaces (IDS) initiative provides a core technological foundation for secure and sovereign data sharing across sectors [24, 32]. Similarly, Gaia-X extends these principles to the cloud-infrastructure level, ensuring interoperability and trust among federated data spaces, while FIWARE supports their operationalization through open-source components for smart applications [24, 31, 34]. In parallel, MyData provides a user-centric governance model that allows individuals to express fine-grained data-use conditions, strengthening agency and transparency in data-sharing practices [31].

Together, these technological and governance initiatives align with the objectives of the European Data Strategy, which is further reinforced by regulatory instruments such as the Data Act and the Data Governance Act [22, 33]. The Data Act aims to foster a competitive and fair data market, enhance accessibility, and promote trust in data sharing across the European Union, working in concert with the Data Governance Act to create an integrated framework for secure, sovereign, and human-centric data exchange [22, 31].

3 Methodology

This research adopts a Design Science Research (DSR) methodology, which provides a structured framework for the creation and iterative evaluation of innovative artifacts [27]. The primary artifact developed in this study is the Sovereign Loop model, a theoretical model designed to address the dynamics between data scarcity, sovereignty, and trust in Human-Centered AI (HCAI) systems.

The DSR process in this study is applied at a conceptual and formative stage, focusing on the design and initial validation of the proposed model. It was conducted through three main phases to ensure methodological rigor and relevance:

Problem Identification & Motivational Foundation: This phase involved a literature synthesis across three domains: (a) Human-Centered AI (HCAI) and explainability, (b) data sovereignty and governance frameworks, and (c) trust in human–computer interaction [30, 35] from Scopus and Google Scholar.

Artifact Development: Guided by these insights, the Sovereign Loop model was conceptualized as a four-node feedback system linking sovereignty-by-design, trust calibration, data quality, and HCAI performance.

Artifact Evaluation: The model was evaluated through a computational simulation.

4 The Sovereign Loop: Model and Validation

The Sovereign Loop model presents a novel theoretical framework that integrates sovereignty, trust, data quality and HCAI into a dynamic feedback system. This model consists of four interconnected nodes that form a virtuous cycle, each dependent on the output of the previous one as seen in Fig. 1.

The first node, Sovereignty-by-Design Architecture, constitutes the foundational entry point of the loop. This moves beyond retrofitting privacy features onto existing systems. It mandates that technical and governance structures must hard-code sovereignty into their very blueprint as highlighted by literature [1, 11–13, 15, 16, 32, 36, 37]. This involves the implementation of Privacy-Enhancing Technologies (PETs) such as Federated Learning [35], which allows AI models to be trained on decentralized data without it ever leaving its source [16, 33], homomorphic encryption, which enables computation on encrypted data [16, 17, 36]. Governance is enforced through smart contracts that automatically execute consent agreements [36].

This sovereign architecture enables the second node: Trust Calibration. The presence of verifiable, sovereignty-by-design features allows for the initial establishment of calculative trust [8, 14, 26]. A user can rationally assess the system and determine that the architectural safeguards lower the risk of misuse or harm. This calculative trust is the permission slip that allows for the first, cautious data-sharing transactions.

The third node, High-Quality Data Generation, is activated by this trust. Willing participation, based on calculated trust and clear consent, generates a data stream of fundamentally consented and higher quality than data acquired through extraction or coercion. Because users are engaged willingly, they are more likely to provide accurate information and richer metadata. This high-quality data directly feeds the fourth

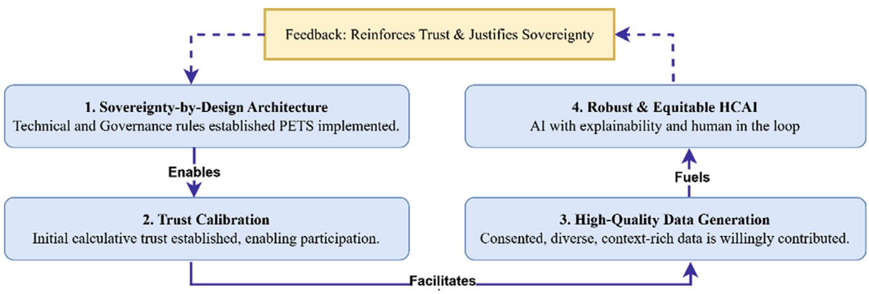

Fig. 1 Architectural diagram of the sovereign loop

node: Robust & Equitable HCAI. The HCAI models trained on this sovereign data are, by design, more likely to be accurate, less biased (due to more diverse and consented data sources), and more robust. Crucially, the HCAI system itself is designed to reinforce the principle of user agency that started the loop. This is achieved through explainable interfaces that make the HCAI's reasoning clear, through meaningful human override controls [38], and through collaborative workflows where the AI acts as a true assistant rather than an oracle [6, 20]. This positive HCAI experience completes the loop by creating a powerful feedback mechanism. The users may be willing to share more data, under the same sovereign protections, thus reinforcing the first node and perpetuating a virtuous cycle of improvement, trust, and collaboration [16].

4.1 Model Formalization and Hypotheses

To clarify the causal relationships within the Sovereign Loop and provide a foundation for computational testing, the model is expressed as a simple iterative framework that links four core variables: Sovereignty (S), Trust (T), Data Quality (Q), and AI Performance (P). All variables are normalized in the range [0, 1], representing proportions or relative intensities.

Core variables:

- S_t: Level of sovereignty-by-design at time t (0 = no control, 1 = full control)
- T_t: Mean user trust (0 = no trust, 1 = complete trust)
- Q_t: Quality of contributed data (0 = poor, 1 = excellent)
- P_t: Performance of the HCAI system (0 = inaccurate, 1 = highly accurate)

Dynamic relationships:

1. **Sovereignty → Trust**: Sovereignty features such as transparency and usage-control enforcement increase calculative trust:

$$T_{t+1} = T_{\text{base}} + (\alpha \times S_t) + (\delta \times P_t)$$

where T_{base} is the initial baseline trust, α is the *trust-gain factor* from sovereignty, and δ is the *reinforcement factor* from AI performance.

2. **Trust → Data Quality**: Users contribute data in proportion to their trust and the potential value of their information:

$$Q_t = T_t \times Q_{\text{potential}}$$

where $Q_{\text{potential}}$ represents the maximum inherent quality of the data a user could provide under ideal conditions of complete trust and cooperation.

3. **Data Quality → AI Performance**: The HCAI system improves through learning from higher-quality data:

$$P_{t+1} = P_t + (\gamma \times Q_t)$$

where γ is the *learning rate* reflecting how efficiently the system converts data quality into improved performance.

4. **AI Performance → Trust (Feedback)**

Positive AI outcomes reinforce relational trust, completing the feedback loop captured in the previous equation through the $\delta \times P_t$ term.

These relationships form a continuous, reinforcing feedback cycle $S_t \rightarrow T_t \rightarrow Q_t \rightarrow P_t \rightarrow T_{t+1}$ illustrating how sovereignty-by-design can trigger and sustain trust-based collaboration in Human-Centered AI.

From the model, we can derive several key hypotheses that invite empirical validation:

H1: Systems implementing sovereignty-by-design architectures will exhibit faster trust calibration over time compared to functionally equivalent systems without such mechanisms.

H2: Data acquired through the sovereign loop will exhibit higher quality compared to data acquired through low-sovereignty means. This proposition posits that consented participation yields fundamentally better data than reluctant contribution, challenging the notion that quantity alone determines dataset value.

H3: The performance of HCAI models trained on data from the sovereign loop will reach target accuracy levels faster than models trained on data from low-sovereignty systems. This proposition tests the feedback effect, suggesting that the combination of higher trust, willing participation, and superior data quality creates a virtuous cycle that accelerates AI development.

4.2 Computational Validation of Model Dynamics via Agent-Based Simulation

To validate the Sovereign Loop model, we developed an agent-based simulation using the Mesa framework in Python. Agent-based modeling is established methodology for testing complex system dynamics prior to empirical validation [36, 39].

The simulation comprises 100 heterogeneous agents and an AI platform interacting over 500 timesteps. Each agent has three attributes: **(1)** dynamic trust level (initial = 0.3), **(2)** immutable risk aversion (randomly distributed 0.2–0.8, **(3)** data quality potential (0.7–1.0). At each timestep, agents decide whether to participate based on trust, risk aversion, sovereignty level, and AI performance. The AI platform starts at 30% accuracy and improves proportionally to the quality of contributed data, with learning rate $\gamma = 0.03$.

Table 1 Hypothesis testing results (n = 30 runs per condition)

Hypothesis	Metric	Baseline	Ideal	Effect	p-value
H1: Trust calibration	Time to 90% trust (timesteps)	106.9 ± 2.4	42.7 ± 1.2	2.5× faster	<0.001
H2: Data quality	Final quality (0–1)	0.468 ± 0.006	0.722 ± 0.007	+54%	<0.001
H3: AI improvement	Time to 80% accuracy (timesteps)	110.0 ± 1.1	66.2 ± 0.7	1.66× faster	<0.001

We tested four conditions: Baseline (no sovereignty, weak incentives), Partial Sovereignty (medium), High Sovereignty (maximum sovereignty, strong incentives), and Ideal (maximum sovereignty and incentives). Each condition was run 30 times with different random seeds for statistical rigor.

We measured three outcomes: (H1) time to reach 90% of maximum trust (trust calibration speed), (H2) final data quality at $t = 500$, and (H3) time to reach 80% AI accuracy (performance improvement speed).

Table 1 presents the main results. Sovereignty-by-design enabled 2.5× faster trust calibration (42.7 versus 106.9 timesteps/iterations, $p < 0.001$), produced 54% higher quality data (0.722 vs 0.468, $p < 0.001$), and achieved 1.66× faster AI improvement to target performance (66.2 vs 110.0 timesteps, $p < 0.001$).

5 Limitations

This model abstracts complex socio-technical dynamics into a simplified feedback loop. The simulation uses limited behavioral parameters (trust, risk aversion, quality potential) that may not capture full human decision-making complexity. Real-world implementation faces significant challenges including computational costs of privacy-enhancing technologies, interoperability across heterogeneous systems, and coordination among diverse stakeholders with differing priorities. Future empirical studies will validate these hypotheses with real users and deployed systems.

6 Conclusion

This paper presents a theoretical model supported by formal mathematical relationships and computational validation. The agent-based simulation provides synthetic evidence of the model's internal logic, illustrating the conditions under which the virtuous cycle of sovereignty, trust, data quality, and Human-Centered AI performance emerges. This foundational work establishes a rigorous basis and clear hypotheses for future empirical studies, showing that data scarcity is best addressed not by bypassing sovereignty but by embracing it as the engine of trustworthy innovation. Together, these hypotheses operationalize the proposed resolution to the cold-start problem in Human-Centered AI, showing how sovereignty-by-design can initiate the conditions for trust, participation, and data availability.

Acknowledgements This research was supported by the EnTrust project: Next Generation of Trustworthy Agri-Data Management, funded under the Marie Skłodowska-Curie Actions (MSCA) Doctoral Network as part of Horizon Europe (Grant Agreement No. 101073381). The authors would like to thank the industrial supervisor Dr. Paul O'Keeffe from Airfield Estate.

Disclaimer The authors used Grammarly to improve language clarity and correctness. All suggestions were reviewed to ensure accuracy and originality, and the authors take full responsibility for the originality of the final content.

Disclosure of Interests Authors declare no conflict of interest.

References

1. Nodehi, N.R., Berisha, F., Da Silva, L., Pourzolfaghar, Z., Helfert, M.: Integrating cybersecurity, data sovereignty and trustworthiness in Agri-data sharing environments: a conceptual framework. In: 2024 Cyber Research Conference–Ireland (Cyber-RCI), pp. 1–8. IEEE (2024)
2. Riedl, M.O.: Human-centered artificial intelligence and machine learning. Hum. Behav. Emerg. Technol. **1**(1), 33–36 (2019)
3. Amershi, S., Dan, W., Vorvoreanu, M., et al.: Guidelines for human-AI interaction. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, pp. 1–13. ACM (2019)
4. Davis, J.P., Eisenhardt, K.M., Bingham, C.B.: Developing theory through simulation methods. Acad. Manag. Rev. **32**(2), 480–499 (2007)
5. Wang, D., Churchill, E., Maes, P., et al.: From human-human collaboration to human-AI collaboration. In: Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems, pp. 1–6. CHI '20: CHI Conference on Human Factors in Computing Systems, ACM (2020)
6. Balcioğlu, Y.S., Çelik, A.A., Altindağ, E.: A turning point in AI: Europe's human-centric approach to technology regulation. J. Responsible Technol. **23**, 100128 (2025)
7. Tran, N., Chen, H., Bhuyan, J., Ding, J.: Data curation and quality evaluation for machine learning-based cyber intrusion detection. IEEE Access. **10**, 121900–121923 (2022)
8. Tatasciore, M., Loft, S.: Calibrating reliance on automated advice: transparency and trust calibration feedback. Int. J. Hum. Comput. **1–11** (2025)
9. Wagner, P.G.: Trustworthy Distributed Usage Control Enforcement in Heterogeneous Trusted Computing Environments, 2025
10. Dwivedi, R., Dave, D., Naik, H., et al.: Explainable AI (XAI): Core ideas, techniques, and solutions. ACM Comput. Surv. **55**(9), 1–33 (2023)
11. Giese, T., Anderl, R.: Maintaining control over distributed data through a data sovereignty model. In: In: 2022 IEEE 7th International Conference on Information Technology and Digital Applications (ICITDA). IEEE (2022)
12. Jarke, M., Otto, B., Ram, S.: Data sovereignty and data space ecosystems. Bus. & Amp; Inf. Syst. Eng. **61**(5), 549–550 (2019)
13. Pandit, H.J.: Making sense of solid for data governance and GDPR. Information. **14**(2), 114 (2023)

14. Koedel, U., Schuetze, C., Fischer, P., et al.: Challenges in the evaluation of observational data trustworthiness from a data producers viewpoint (FAIR+). Front. Environ. Sci. **9** (2022)
15. von Scherenberg, F., Hellmeier, M., Otto, B.: Data sovereignty in information systems. Electron. Mark. **34**(1) (2024)
16. Zrenner, J., Möller, F.O., Jung, C., Eitel, A., Otto, B.: Usage control architecture options for data sovereignty in business ecosystems. J. Enterp. Inf. Manag. **32**(3), 477–495 (2019)
17. Seco-Aguirre, I., Regueiro, C., Jacob, E., et al.: Extending Self-Sovereign Identity Using Fully Homomorphic Encryption to Enhance the Privacy of Verifiable Credentials. Elsevier BV (2025)
18. Jarrahi, M.H.: Artificial intelligence and the future of work: human-ai symbiosis in organizational decision making. Bus. Horiz. S. **61**(4), 577–586 (2018)
19. Maadi, M., Khorshidi, H.A., Aickelin, U.: A review on human–AI interaction in machine learning and insights for medical applications. Int. J. Environ. Res. Public Health. **18**(4), 2121 (2021)
20. Capel, T., Brereton, M.: What is human-centered about human-centered AI? A map of the research landscape. In: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems, pp. 1–23. ACM (2023)
21. Holzinger, A., Schweier, J., Gollob, C., et al.: From industry 5.0 to forestry 5.0: bridging the gap with human-centered artificial intelligence. Curr. For. Rep. **10**(6), 442–455 (2024)
22. Karagiannis, V., Simhandl, G., Ignjatović, D., Bürger, B., Drobics, M.: The role of data spaces in the internet of things. E+i Elektrotechnik Und Informationstechnik. **142**(3–4), 221–227 (2025)
23. Tocchetti, A., Corti, L., Balayn, A., et al.: A.I. Robustness: a human-Centered perspective on technological challenges and opportunities. ACM Comput. Surv. **57**(6), 1–38 (2025)
24. Lopes, P.M., Guimarães, P., Pereira, T.F., Machado, R.J.: Gaia-X & amp; fiware: implementation of a federated data platform in smart cities. Procedia Comput. Sci. **239**, 1506–1515 (2024)
25. Rafsanjani, H.N., Nabizadeh, A.H.: Towards human-Centered artificial intelligence (AI) in architecture, engineering, and construction (AEC) industry. Comput. Hum. Behav. Rep. **11**, 100319 (2023)
26. Fierens, M., Pandit, H.J., Tamo-Larrieux, A., Garcia, K.: A solid use case to empower and protect data subjects: responsibilities under GDPR for governance of personal data stores. Comput. Law & Amp; Secur. Rev. **57** (2025)
27. Hevner, M., Park, J., Ram, S.: Design science in information systems research. MIS Q. **28**(1), 75 (2004)
28. Ruckstuhl, K.: Trust in Scholarly Communications and Infrastructure: indigenous data sovereignty. Front. Res. Metr. Anal. **6** (2022)
29. Marusich, L.R., Files, B.T., Bancilhon, M., Rawal, J.C., Raglin, A.: Trust calibration for joint human/AI decision-making in dynamic and uncertain contexts. In: Lecture Notes in Computer Science. Springer Nature Switzerland (2025)
30. Mayer, R.C., Davis, J.H., Schoorman, F.D.: An integrative model of organizational trust. Acad. Manag. Rev. **20**(3), 709 (1995)
31. Akaichi, I., Kirrane, S.: A comprehensive review of usage control frameworks. Comput Sci Rev. **56**, 100698 (2025)
32. Gabellini, M., Civolani, L., Ronchi, M., Naldi, L.D., Regattieri, A.: Data spaces in manufacturing and supply chains: a review and insights from european initiatives. Appl. Sci. **15**(11), 5802 (2025)
33. Hellmeier, M., Pampus, J., Qarawlus, H., Howar, F.: Implementing data sovereignty: requirements & amp; challenges from practice. In: Proceedings of the 18th International Conference on Availability, Reliability and Security, pp. 1–9. ARES 2023: The 18th International Conference on Availability, Reliability and Security. ACM (2023)
34. Martella, C., Martella, A., Longo, A.: European data spaces for urban digital twins: user-and implementation-driven recommendations. In: In 2024 IEEE International Conference on Big Data (BigData). 2024 IEEE International Conference on Big Data (BigData). IEEE (2024)
35. Gulati, S., McDonagh, J., Sousa, S., Lamas, D.: Trust models and theories in human–computer interaction: a systematic literature review. Comput. Hum. Behav. Rep. **16**, 100495 (2024)

36. Del Re, E.: Technologies of data protection and institutional decisions for data sovereignty. Information. **15**(8), 444 (2024)
37. Tao, Y., Yang, S., Ge, H.: Comparative study on data sovereignty guarantee technology. In: In 2022 IEEE 13th International Symposium on Parallel Architectures, Algorithms and Programming (PAAP). 2022 IEEE 13th International Symposium on Parallel Architectures, Algorithms and Programming (PAAP). IEEE (2022)
38. Nikiforidis, K., Kyrtsoglou, A., Vafeiadis, T., et al.: Enhancing transparency and trust in AI-powered manufacturing: a survey of explainable AI (XAI) applications in smart manufacturing in the era of industry 4.0/5.0. ICT Express. **11**(1), 135–148 (2025)
39. Gilbert, N.: Agent-based models. SAGE Publications, Inc. (2008)