big data and cognitive computing

MDPI

Article

Trustworthy AI for Whom? GenAI Detection Techniques of Trust Through Decentralized Web3 Ecosystems

Igor Calzada [1,2,3,4,5,6,7,*], Géza Németh [7] and Mohammed Salah Al-Radhi [7]

1 Public Policy & Economic History Department, Faculty of Economy and Business, University of the Basque Country, UPV-EHU, Oñati Square 1, 20018 Donostia-San Sebastián, Spain
2 Basque Foundation for Science, Ikerbasque, Plaza Euskadi 5, 48009 Bilbao, Spain
3 Wales Institute of Social and Economic Research and Data (WISERD), School of Social Sciences, Social Science Research Park (Sbarc/Spark), Cardiff University, Maindy Road, Cathays, Cardiff CF24 4HQ, UK
4 Decentralization Research Centre, 545 King St. W, Toronto, ON W5V 1M1, Canada
5 Fulbright Scholar-In-Residence (S-I-R), US-UK Fulbright Commission, Unit 302, 3rd Floor Camelford House, 89 Albert Embankment, London SE1 7TP, UK
6 Astera Institute, 2625 Alcatraz Ave #201, Berkeley, CA 94705, USA
7 Department of Telecommunications and Artificial Intelligence, Budapest University of Technology and Economics, ENFIELD Horizon, BEM, 1117 Budapest, Hungary
* Correspondence: igor.calzada@ehu.eus; Tel.: +34-630-752876

Abstract: As generative AI (GenAI) technologies proliferate, ensuring trust and transparency in digital ecosystems becomes increasingly critical, particularly within democratic frameworks. This article examines decentralized Web3 mechanisms—blockchain, decentralized autonomous organizations (DAOs), and data cooperatives—as foundational tools for enhancing trust in GenAI. These mechanisms are analyzed within the framework of the EU's AI Act and the Draghi Report, focusing on their potential to support content authenticity, community-driven verification, and data sovereignty. Based on a systematic policy analysis, this article proposes a multi-layered framework to mitigate the risks of AI-generated misinformation. Specifically, as a result of this analysis, it identifies and evaluates seven detection techniques of trust stemming from the action research conducted in the Horizon Europe Lighthouse project called ENFIELD: (i) federated learning for decentralized AI detection, (ii) blockchain-based provenance tracking, (iii) zero-knowledge proofs for content authentication, (iv) DAOs for crowdsourced verification, (v) AI-powered digital watermarking, (vi) explainable AI (XAI) for content detection, and (vii) privacy-preserving machine learning (PPML). By leveraging these approaches, the framework strengthens AI governance through peer-to-peer (P2P) structures while addressing the socio-political challenges of AI-driven misinformation. Ultimately, this research contributes to the development of resilient democratic systems in an era of increasing technopolitical polarization.

Keywords: generative AI; decentralization; Web3; trustworthy AI; blockchain; DAOs; data cooperatives; big data; detection techniques; democracy

check for updates

Academic Editor: Domenico Ursino

Received: 10 January 2025
Revised: 17 February 2025
Accepted: 1 March 2025
Published: 6 March 2025

Citation: Calzada, I.; Németh, G.; Al-Radhi, M.S. Trustworthy AI for Whom? GenAI Detection Techniques of Trust Through Decentralized Web3 Ecosystems. *Big Data Cogn. Comput.* **2025**, *9*, 62. https://doi.org/10.3390/bdcc9030062

1. Introduction: Trustworthy AI for Whom?

The rise of generative artificial intelligence (GenAI) has introduced transformative tools capable of generating complex, human-like content in text, imagery, and sound [1,2]. While these technologies hold vast potential for innovation across industries, they also pose significant risks related to trust, authenticity, and accountability. As the European Commission has globally advanced the AI Act framework to regulate and assure "trustworthy AI", the question of clarifying for whom it should be trustworthy becomes increasingly urgent [3,4]. This inquiry is foundational, especially as GenAI tools permeate sensitive sectors such as healthcare, law enforcement, and governance, where misuse could erode democratic principles, spread misinformation and disinformation, or reinforce biases [5–20].

Generally speaking, the evolution of artificial intelligence (AI), particularly in its generative forms (GenAI), has sparked both admiration for its potential and concerns over its societal impact [21–23]. GenAI's ability to autonomously create text, images, and other forms of content challenges not only the boundaries of creativity but also the very foundations of truth and trust in the digital era [24,25]. GenAI has often been portrayed as a technological marvel, capable of revolutionizing industries and improving efficiencies [11,12]. However, the "elephant in the room", to borrow a metaphor, is the potential for AI to erode democratic systems by flooding information channels with highly persuasive, fabricated content [15,24]. As Amoore et al. highlighted [7], the political logic of GenAI transcends mere technicality, embedding itself into the political fabric of societies by altering how information is produced, disseminated, and consumed. This shift challenges democratic institutions that rely on transparency, accountability, and trust in information, prompting urgent questions about the governance of GenAI in decentralized systems [26–41].

Against this backdrop, the European Commission's AI Act, alongside the Draghi Report [3,4], provides a comprehensive policy framework aimed at balancing innovation with ethical oversight in AI systems. The AI Act introduces a risk-based classification model, categorizing AI applications into unacceptable, high, limited, and minimal risk levels, with tailored regulatory measures for each category. This ensures that high-stakes sectors adhere to stringent requirements for transparency, accountability, and human oversight. Complementing this, the Draghi Report emphasizes AI as a strategic enabler of economic resilience, competitiveness, and sustainability within the European Union, framing AI technologies as infrastructure essential for diverse sectors. It underscores the importance of innovation sandboxes, fostering experimentation while ensuring compliance with ethical standards. Together, these policy frameworks advocate for the development of trustworthy AI systems that align technical standards with societal values, addressing challenges such as data sovereignty, democratic resilience, and public trust in AI-driven systems. The convergence of these policies represents Europe's commitment to navigating the complexities of digital transformation while safeguarding democratic integrity and equity [42–50].

In parallel to regulatory efforts, the evolving competition between open-source and proprietary AI models underscores the importance of access, decentralization, and computing power in shaping AI's trajectory [51–56]. The recent emergence of Deepseek, an open-source model from China, has reignited debates over the accessibility of AI capabilities in contrast to closed, compute-intensive systems such as ChatGPT [57–78]. Deepseek's ability to operate effectively with lower computational demands highlights the potential for decentralized AI models to democratize access to AI technologies, reducing dependency on corporate-controlled infrastructures. This rivalry exemplifies the broader tensions in AI governance—between centralized, capital-intensive models and more inclusive, decentralized Web3 alternatives that prioritize public access and transparency [79–94].

Further reinforcing the need for open and accessible AI, the AI Action Summit in Paris on 10–11 February 2025, after remarkable preparatory sessions in Bangalore and Paris from 11–13 December 2024, followed by the ENFIELD Trustworthy AI for Whom? Hybrid Workshop at the Budapest University of Economics and Technology (BME) on 14 February 2025, showcased a landmark collaboration between India and France on Digital Public Infrastructure (DPI), emphasizing the importance of sovereign, open-source, and community-driven AI initiatives. By leveraging DPI frameworks, such collaborations aim to empower diverse stakeholders with AI solutions that prioritize public interest over proprietary constraints. These developments signal a shift towards a more equitable AI landscape, where technological sovereignty, interoperability, and decentralized innovation play a crucial role in ensuring that AI serves broader societal goals rather than being concentrated in the hands of a few dominant players [95–122].

Building on these policy foundations, the research question central to this article is "*trustworthy AI for whom* (and for what)?", and this inquiry challenges conventional narratives of technological neutrality, emphasizing the need to scrutinize the social, political, and economic implications of trust in AI systems [123]. GenAI models, while transformative, introduce complex challenges, particularly in ensuring transparency, accountability, and equity in their outputs and processes [21]. The notion of "trustworthy AI" must move beyond technical compliance to consider whose trust is prioritized, what ethical frameworks are employed, and how diverse stakeholders—including minority communities—are included in decision-making processes [124–132].

Trust, in this context, is not a monolithic concept but a contested terrain shaped by power, inclusion, and socio-political dynamics. The question of "*trustworthy AI for whom*?" extends beyond technical assurance frameworks to fundamental concerns about democratic legitimacy, justice, and human dignity. In an era where AI increasingly mediates public discourse, access to services, and governance decisions, trust cannot be decoupled from issues of algorithmic discrimination, surveillance, digital exclusion, and epistemic inequality. Certain communities—particularly marginalized groups, those in the Global South, or populations with limited digital literacy—risk becoming invisible within AI-driven infrastructures that prioritize the perspectives and needs of dominant actors. From a humanitarian perspective and stemming from recent action research related to AI and the Global South, the democratic integrity of AI depends not only on who builds and governs AI systems but also on who is empowered to challenge, reshape, and redefine them [23]. If trustworthiness is to be meaningful, it must be co-created through participatory governance, regulatory safeguards, and mechanisms for redress and accountability. AI governance should not merely seek to *prevent harm* but should actively cultivate justice, resilience, and agency in digital societies. Addressing these challenges requires shifting the focus from technical fixes to systemic change, ensuring that AI reinforces democratic values rather than eroding them.

Hence, this article aims to explore decentralized Web3 mechanisms—blockchain, decentralized autonomous organizations (DAOs), and data cooperatives—as foundational tools for fostering trust in GenAI within democratic frameworks. By doing so, it contributes to the broader discussion on trustworthy AI governance, aligning with the EU's AI Act and the Draghi Report.

To achieve this aim, the article pursues the following five specific research objectives: (i) to analyze the role of decentralized Web3 ecosystems (blockchain, DAOs, and data cooperatives) in mitigating misinformation risks and enhancing transparency in AI-generated content; (ii) to evaluate the effectiveness of seven trust detection techniques (federated learning, blockchain-based provenance tracking, zero-knowledge proofs, DAOs for crowdsourced verification, AI-powered digital watermarking, explainable AI, and privacy-preserving machine learning) in decentralized AI governance; (iii) to examine the socio-political implications of decentralized AI governance by assessing the alignment of Web3-based trust mechanisms with democratic principles such as transparency, accountability, and data sovereignty; (iv) to bridge the gap between European AI regulations and emerging trust detection techniques, thereby providing actionable recommendations for aligning technological innovation with regulatory and ethical standards; and (v) to investigate the limitations and potential risks associated with decentralized AI governance, including power asymmetries, technical challenges, and policy implications for future AI governance structures.

Based on the research objectives, the following hypothesis guides this article: decentralized Web3 ecosystems provide a viable framework for detecting and mitigating trust deficits in GenAI applications, thereby enhancing transparency, accountability, and democratic resilience in AI governance. This hypothesis is tested through a multi-layered analysis of trust detection techniques, policy frameworks (AI Act and Draghi Report), and decentralized governance structures.

In this context, the role of decentralized Web3 technologies—blockchain [133–138], decentralized autonomous organizations (DAOs) [139], and data cooperatives [140,141]—emerges as a critical countermeasure to the risks associated with centralized AI models [23]. Web3 structures prioritize transparency, data sovereignty, and community participation, aligning with democratic ideals by enabling users to directly influence AI development and governance. By distributing control across peer-to-peer networks rather than within isolated data monopolies, these frameworks offer a pathway to more resilient, socially accountable AI. This article explores these questions through the lens of decentralized Web3 ecosystems, focusing on how technologies like blockchain, decentralized autonomous organizations (DAOs), and data cooperatives can redefine the governance and detection of trust in GenAI systems. By integrating these decentralized mechanisms, the research examines seven key techniques for fostering trust: (i) federated learning for decentralized AI creation and detection, (ii) blockchain-based provenance tracking, (iii) zero-knowledge proofs for content authentication, (iv) DAOs for crowdsourced verification, (v) AI-powered digital watermarking, (vi) explainable AI (XAI) for content detection, and (vii) privacy-preserving machine learning (PPML) for secure content verification. These techniques collectively present a multi-layered framework for detecting and governing GenAI outputs, emphasizing transparency, participatory governance, and data sovereignty. The article positions these approaches as critical to addressing the socio-political risks of AI, including misinformation, disinformation, and democratic erosion [30], while aligning with the broader aspirations of the European Union's AI Act and the Draghi Report. Through this exploration, the title "Trustworthy AI for Whom? GenAI Detection Techniques of Trust Through Decentralized Web3 Ecosystems" underscores the urgency of rethinking trust in AI as a shared responsibility that transcends traditional regulatory paradigms.

Web3 refers to a decentralized, blockchain-based ecosystem that enables peer-to-peer networks without reliance on central authorities. The integration of AI into decentralized Web3 ecosystems introduces further complexities [25], as these networks operate without central authority, making traditional forms of governance and control inadequate [26,27]. The proliferation of AI-generated content poses profound implications for democratic integrity [28–30], as the line between real and synthetic content blurs, creating fertile ground for misinformation and disinformation. Furthermore, these challenges are compounded by the unsustainability of current data ecosystems that underlie GenAI [16], requiring innovative strategies for navigating the contradictions between digitalization and sustainability [127].

This introduction sets the stage for an exploration of *trust detection techniques* within decentralized Web3 ecosystems that can enhance GenAI's democratic accountability. Through this lens, we examine not only the technical approaches required to verify AI-generated content but also the socio-political imperatives of establishing a multi-layered trust infrastructure. This analysis is rooted in the collaborative efforts under the umbrella of the Horizon Europe-funded project ENFIELD and within the AI4SI research program supported by the Basque Foundation for Science, which focuses on leveraging Web3 detection techniques to ensure that AI applications serve public trust, transparency, and resilience, especially within urban and governance contexts, while being committed to leveraging the social impact of the European regulation, including the AI Act and the Draghi Report, by contextualizing them in each specific regional uniqueness but being committed to fundamental rights and to equitable European digital futures.

The development of GenAI technologies has redefined trust, democratizing access to content creation but also amplifying concerns around authenticity and misuse. As these technologies become more pervasive, the challenge lies in determining "trustworthiness" in an environment where AI can impersonate humans and autonomously generate realistic content. This issue is intensified by the varying standards and perceptions of digital trust across cultural, political, and technological contexts, leading to the pressing research question of this article. To address these complexities, decentralized Web3 technologies—blockchain, DAOs, and data cooperatives—have gained attention as tools for fostering transparency and safeguarding democratic integrity in digital spaces [30]. These technologies present an alternative to centralized AI governance by embedding verification mechanisms within peer-to-peer networks, potentially enhancing the reliability of AI-driven content in democratic contexts.

But how to frame the research question of *"trustworthy AI for whom*?" There are four preliminary considerations and caveats that should be acknowledged before developing the structure of this article:

(i) Recent advances in digital watermarking present a scalable solution for distinguishing AI-generated content from human-authored material. SynthID-Text, a watermarking algorithm discussed by Dathathri et al. [142], provides an effective way to mark AI-generated text, ensuring that content remains identifiable without compromising its quality. This watermarking framework offers a pathway for managing AI's outputs on a massive scale, potentially curbing the spread of misinformation. However, questions of accessibility and scalability remain, particularly in jurisdictions where trust infrastructures are underdeveloped. SynthID-Text's deployment exemplifies how watermarking can help maintain trust in AI content, yet its application primarily serves contexts where technological infrastructure supports high computational demands, leaving out communities with limited resources;

(ii) The concept of "personhood credentials" (PHCs) provides another lens for exploring trust. According to Adler et al. [143], PHCs allow users to authenticate as real individuals rather than AI agents, introducing a novel method for countering AI-powered deception. This system, based on zero-knowledge proofs, ensures privacy by verifying individuals' authenticity without exposing personal details. While promising, PHCs may inadvertently centralize trust among issuing authorities, which could undermine local, decentralized trust systems. Additionally, the adoption of PHCs presents ethical challenges, particularly in regions where digital access is limited, raising further questions about inclusivity in digital spaces purportedly designed to be "trustworthy";

(iii) In the context of decentralized governance, Poblet et al. [133] highlighted the role of blockchain-based oracles as tools for digital democracy, providing external information to support decision making within blockchain networks. Oracles serve as intermediaries between real-world events and digital contracts, enabling secure, decentralized information transfer in applications like voting and community governance. Their use in digital democracy platforms has demonstrated potential for enhancing transparency and collective decision making. Yet, this approach is not without challenges; the integration of oracles requires robust governance mechanisms to address biases and inaccuracies, especially when scaling across diverse socio-political landscapes. Thus, oracles provide valuable insights into building trustworthy systems, but their implementation remains context-dependent, raising critical questions about the universality of digital trust.

Lastly, the discourse on digital sovereignty, as discussed by Fratini et al. [144], is integral to understanding the layers of trust in decentralized Web3 ecosystems. Their research outlined various digital sovereignty models, illustrating how governance frameworks vary from state-based to rights-based approaches [145–151]. The rights-based model emphasizes protecting user autonomy and data privacy, resonating with democratic ideals but facing practical challenges in globalized digital economies. In contrast, state-based models prioritize national security and centralized control, often clashing with decentralized ethos. These sovereignty models underscore the need for adaptable governance structures that consider the diversity of trust needs across regions, reflecting the complexities of fostering "trustworthy" AI in decentralized contexts.

While both watermarking and blockchain-based solutions offer viable approaches to AI content verification, their effectiveness depends on context, scalability, and governance structures. Digital watermarking, such as Google's SynthID-Text, provides an embedded, tamper-resistant marker to differentiate AI-generated content from human-authored material. However, its effectiveness relies on broad adoption across AI models and may be limited by computational (power and access) requirements, making it less accessible in resource-constrained environments. In contrast, blockchain-based provenance tracking secures content authenticity through an immutable, decentralized ledger, ensuring transparency and accountability without requiring modifications to the content itself. While blockchain solutions reduce reliance on centralized verification authorities, their effectiveness hinges on widespread interoperability, governance frameworks, and the ability to counter deepfake generation techniques. Thus, rather than viewing these as competing solutions, a hybrid approach—combining watermarking for real-time content labeling and blockchain for long-term integrity verification—may offer the most resilient and scalable strategy for AI content trustworthiness. This addition provides a comparative discussion while suggesting an integrated approach, aligning with this article's focus on trustworthy AI and decentralized governance.

Following the presentation of the research question in this introduction, a European policy analysis is carried out in the next section around trustworthy AI through the AI Act and the Draghi Report. Stemming from this European policy analysis, the third section presents the seven techniques for detecting trust as part of the ongoing research project within the framework of the ENFIELD EU Lighthouse project. The final section of the article presents discussions and conclusions, limitations, and future research avenues.

2. Methods: Trustworthy AI Systematic EU Policy Analysis Through AI Act and Draghi Report

This section explores the European Union's policy response to the challenges and opportunities presented by AI through the lens of two critical and timely documents: the AI Act [4,152] and the Draghi Report [3]. As such, this methodological section aims to frame the research question by conducting a policy analysis of the European Trustworthy AI Policy through the AI Act and the Draghi Report. This policy analysis underscores the need to position AI as both an enabler of economic growth and a guarantor of ethical, trustworthy, and socially beneficial outcomes. The Draghi Report situates AI as a pivotal driver of economic growth, competitiveness, and resilience across the EU. It articulates a vision where AI extends beyond being a collection of tools to becoming an integral infrastructure underpinning diverse sectors, such as healthcare, urban development, and governance. This transformative potential, however, comes with the shared challenge of ensuring that AI contributes to resilient and sustainable societies while mitigating the risks of democratic erosion and inequality. This is related to the research question of this article: "trustworthy AI for whom?" [153].

Complementing the Draghi Report, the AI Act introduces a comprehensive regulatory framework aimed at balancing innovation with ethical standards. It emphasizes establishing trust in high-stakes applications such as healthcare, law enforcement, and autonomous systems, where societal impact is profound. The Act outlines a risk-based approach, categorizing AI systems by potential harm and implementing oversight mechanisms accordingly.

2.1. AI Act at the Crossroads of Innovation and Responsibility

The European Union's AI Act represents a landmark effort to balance innovation with societal protection. Its risk-based framework establishes a uniform classification of AI risks across member states, ensuring consistent governance while allowing flexibility to accommodate national priorities. For technologists, the Draghi Report resonates with its call to align technical advancements with societal priorities, urging stakeholders to build trust into the AI lifecycle. The report challenges policymakers and practitioners alike to leverage AI in ways that bolster economic and social resilience, aligning innovation with responsibility. This regulatory blueprint aims to harmonize technical standards with societal needs, ensuring that innovation does not come at the expense of ethical integrity. By promoting transparency, accountability, and explainability, the AI Act aspires to prevent misuse and discrimination while fostering trust in AI systems. This article explores key aspects of the Act (see Table 1), emphasizing the interplay between uniform standards and localized implementation strategies as follows:

Table 1. European Trustworthy AI Policy Analysis Through AI Act [4].

Aspect	EU-Wide Application Under AI Act	Country-Specific Focus [3,4]
1. Risk Classification	AI systems are classified as unacceptable, high, limited, or minimal risk.	Individual states may prioritize specific sectors (e.g., healthcare in Germany, transportation in the Netherlands) where high-risk AI applications are more prevalent.
2. High-Risk AI Requirements	Mandatory requirements for data quality, transparency, robustness, and oversight.	Enforcement and oversight approaches may vary, with some countries opting for stricter testing and certification processes.
3. Transparency Obligations	Users must be informed when interacting with AI (e.g., chatbots and deepfakes).	Implementation might vary, with some countries adding requirements for specific sectors like finance (France) or public services (Sweden).
4. Data Governance	Data used by AI systems must be free from bias and respect privacy.	States with stronger data protection laws, like Germany, may adopt stricter data governance and audit practices.
5. Human Oversight	High-risk AI requires mechanisms for human intervention and control.	Emphasis may vary, with some states prioritizing human oversight in sectors like education (Spain) or labor (Italy).
6. Compliance and Penalties	Non-compliance can result in fines up to 6% of global turnover.	While fines are harmonized, enforcement strategies may differ based on each country's regulatory framework.

Table 1. *Cont.*

	Aspect	EU-Wide Application Under AI Act	Country-Specific Focus [3,4]
7.	Innovation Sandboxes	Creation of sandboxes to promote safe innovation in AI.	Some countries, like Denmark and Finland, have existing sandbox initiatives and may expand them to further support AI development.
8.	National AI Strategies	Member states align their AI strategies with the AI Act's principles.	Countries may adapt strategies to their economic strengths (e.g., robotics in Czechia and AI-driven fintech in Luxembourg).
9.	Public Sector AI Applications	Public services using AI must comply with the Act's requirements.	Some countries prioritize transparency and ethics in government AI applications, with additional guidelines (e.g., Estonia and digital services).

2.1.1. Risk Classification: A Unified Framework with Tailored Enforcement

At the heart of the AI Act lies a risk classification system that categorizes AI applications based on their potential harm [43,58,59,71]. This uniform framework ensures that all member states adhere to a shared baseline for assessing and managing AI risks. However, the enforcement of these classifications may differ based on national priorities [154]. For instance, while all countries are required to address high-risk AI applications, specific sectors may receive heightened attention depending on their relevance to the state's economic or strategic interests, which requires a deep understanding of digital rights regarding whose stakeholders are involved in the trustworthy AI process [155–159].

2.1.2. Human Oversight: Enhancing Governance in Critical Sectors

Human oversight remains a cornerstone of the AI Act, ensuring accountability and ethical compliance in AI deployment [160–179]. Member states have the discretion to amplify oversight measures in sectors critical to their national interests. For example, countries with robust healthcare systems may focus on ensuring transparency and explainability in AI-driven medical applications, whereas others may prioritize oversight in domains such as defense or financial technology.

2.1.3. Innovation Sandboxes: Bridging Compliance and Creativity

To foster innovation while maintaining regulatory compliance, the AI Act encourages the creation of innovation sandboxes—controlled environments where AI technologies can be tested and refined. Countries with strong AI ecosystems or ambitious technological agendas may leverage these sandboxes to accelerate AI adoption while adhering to ethical standards. By providing a space for experimentation, innovation sandboxes allow member states to remain competitive in the global AI landscape without compromising on safety and trustworthiness.

2.1.4. Sector-Specific Priorities: Aligning AI with Regional Significance

The flexibility of the AI Act extends to addressing sector-specific priorities. Member states are encouraged to focus on sectors of regional significance or those deemed high-risk. For example, Germany, known for its manufacturing prowess, might emphasize AI compliance in industrial automation, while Sweden could prioritize energy sector applications, aligning regulatory efforts with national strengths and challenges. This approach ensures that AI regulations not only address universal concerns but also support localized economic development.

2.1.5. A Unified Vision with Localized Flexibility

The overarching goal of the AI Act is to foster a high level of protection across the EU while enabling member states to tailor their approaches to AI governance. This dual objective reflects the EU's commitment to harmonizing innovation and responsibility. By accommodating each state's unique priorities and industries, the AI Act provides a framework that promotes both competitiveness and ethical integrity.

2.1.6. Toward a Balanced Future?

As AI continues to reshape societies and economies, the EU's AI Act serves as a model for navigating the complexities of regulation in a rapidly evolving landscape. By blending uniform risk classification with localized flexibility, the Act ensures that member states can address their unique challenges while contributing to a collective vision of trustworthy and innovative AI.

In Table 1, several key aspects of AI Act are examined, including (i) risk classification, (ii) high-risk AI requirements, (iii) transparency obligations, (iii) data governance, (iv) human oversight, (v) compliance and penalties, (vi) innovation sandboxes, (vii) national AI strategies, and (viii) public sector AI applications.

The AI Act's governance model, as outlined in this analysis (Table 1), presents a multi-tiered regulatory framework designed to mitigate risks, enhance transparency, and uphold democratic accountability in AI systems. However, while the Act introduces clear regulatory expectations—including risk classification, transparency obligations, and human oversight—it lacks a concrete technological roadmap for operationalizing these principles across decentralized AI ecosystems. To bridge this gap, this article identifies seven key detection techniques that align with the AI Act's core policy pillars, ensuring trustworthy AI implementation in real-world settings.

(i) Federated Learning (Aligned with Data Governance and Privacy):
Supports privacy-preserving AI governance by enabling distributed training on sensitive data without centralizing information, ensuring compliance with GDPR and AI Act's high-risk AI requirements.
Example: Used in healthcare applications, allowing hospitals to collaboratively train AI models while preserving patient confidentiality;

(ii) Blockchain-Based Provenance Tracking (Aligned with Transparency Obligations and Public Sector AI Applications):
Ensures immutability of AI-generated content, enabling verifiable authenticity for AI-driven decisions, which is crucial in public services and media regulation.
Example: Applied in journalism and digital identity systems to authenticate content sources and prevent AI-generated misinformation;

(iii) Zero-Knowledge Proofs (ZKPs) (Aligned with Data Governance and Compliance):
Allows verification of AI interactions without exposing sensitive data, reinforcing trust in decentralized AI systems while complying with strict data protection laws.
Example: Used in identity verification protocols, ensuring that AI-driven authentication mechanisms operate transparently without privacy risks;

(iv) Decentralized Autonomous Organizations (DAOs) for Crowdsourced Verification (Aligned with Human Oversight and AI Governance):
Introduces community-driven AI auditing, ensuring democratic oversight in high-risk AI applications where centralized institutions may lack credibility or impartiality.
Example: Implemented in fact-checking initiatives, where DAOs enable collective content moderation and AI accountability mechanisms;

(v) AI-Powered Digital Watermarking (Aligned with Transparency and Misinformation Regulation):

Embeds traceable markers into AI-generated content, ensuring that users are informed when interacting with AI-generated media, aligning with the AI Act's transparency provisions.
Example: Used in deepfake detection and content verification systems, particularly in elections and media trust initiatives;

(vi) Explainable AI (XAI) (Aligned with High-Risk AI Requirements and Human Oversight):
Enhances interpretability of AI decisions, ensuring accountability in high-stakes AI applications where explainability is legally mandated.
Example: Adopted in finance, legal, and medical AI models to provide clear justifications for algorithmic outcomes, addressing concerns over AI opacity;

(vii) Privacy-Preserving Machine Learning (PPML) (Aligned with Compliance and Innovation Sandboxes):
Facilitates secure AI model training without compromising user privacy, enabling safe AI innovation in regulatory sandboxes while ensuring alignment with compliance standards.
Example: Used in cross-border AI collaborations, particularly in fintech and digital identity management, to protect personal data while enabling AI innovation.
Conclusion: Bridging Policy and Technology for Trustworthy AI

The AI Act establishes a regulatory foundation for ensuring AI systems operate ethically, transparently, and accountably across the European Union. However, for trustworthy AI to be effectively realized, it requires concrete detection mechanisms that align technical innovations with legal mandates. This article systematically identifies seven detection techniques that serve as practical enablers of AI governance in the following ways:

1. Operationalizing risk management and compliance measures within the AI Act's framework;
2. Providing real-world applications that ensure AI technologies align with democratic values such as transparency, accountability, and human oversight;
3. Addressing the limitations of centralized AI governance by introducing decentralized, privacy-preserving, and community-driven trust mechanisms.

By embedding these detection techniques into AI governance strategies, policymakers, industry leaders, and civil society can collaboratively enhance AI's trustworthiness while ensuring regulatory compliance and democratic resilience in an increasingly automated and decentralized digital landscape.

2.2. Draghi Report

Both the Draghi Report and the AI Act converge on a critical question: how can AI technologies be developed and deployed in ways that support resilient, sustainable economies and societies [155–158]? Central to this inquiry is the recognition that trustworthiness and technical excellence must go hand in hand. From creating inclusive datasets to enabling user-friendly and context-aware applications, these policies highlight the role of AI in shaping not only markets but also democratic norms and citizen engagement. The Draghi Report serves, alongside the AI Act, as a critical policy document framing AI as both an enabler of economic growth and a tool for addressing societal challenges. By examining the beneficiaries and potential disparities embedded in the report's vision, we can better understand the socio-political dynamics of AI governance and the pathways toward equitable innovation [180–187].

2.2.1. Trustworthiness Beyond Technological Robustness

The Draghi Report underscores trustworthiness as a fundamental pillar of AI, encompassing transparency, accountability, and ethical integrity [188]. Yet, these values are often interpreted through the lens of technocratic frameworks, emphasizing regulatory compliance and algorithmic reliability. While these aspects are crucial, the focus on technical standards risks sidelining the broader social contexts in which AI systems operate. For whom and by whom are these systems deemed trustworthy? This perspective shifts the debate from technological robustness to societal inclusivity, interrogating whether current frameworks adequately address the needs of marginalized or underrepresented groups. The report's call for trustworthy AI resonates with high-stakes domains such as healthcare, education, and public services, but these applications often disproportionately impact vulnerable populations. Trust, in this sense, should be co-constructed through participatory governance mechanisms that empower affected communities to shape the design, deployment, and oversight of AI technologies.

2.2.2. Economic Competitiveness vs. Ethical Equity

A central tension in the Draghi Report is its dual emphasis on fostering economic competitiveness and maintaining ethical AI standards. This tension reflects broader policy challenges within the EU: balancing the need to lead in the global AI race while safeguarding fundamental rights. However, questions arise regarding whose economic interests are prioritized. Large technology firms and well-resourced industries are better positioned to align with regulatory frameworks, whereas smaller enterprises or non-profit initiatives may struggle to compete [29,30]. This uneven playing field raises concerns about the inclusivity of AI-driven economic growth. From a "*trustworthy AI for whom*" perspective, policies must address these disparities by ensuring that AI innovation benefits a broad spectrum of stakeholders, including SMEs, grassroots organizations, and historically marginalized communities. Initiatives such as innovation sandboxes, proposed in the Draghi Report, offer a promising avenue for bridging this gap. These controlled environments can democratize access to cutting-edge technologies, enabling smaller actors to experiment with AI solutions while adhering to regulatory standards.

2.2.3. Trustworthiness in High-Stakes Sectors

The Draghi Report emphasizes trustworthiness in high-stakes sectors such as healthcare, law enforcement, and energy. While these applications promise transformative benefits, they also entail significant risks of misuse and bias, particularly for minority and marginalized populations. For example, AI systems deployed in healthcare must navigate complex ethical dilemmas, such as balancing personalized treatments with equitable access. Similarly, predictive policing algorithms, often cited as a high-risk application, have been criticized for perpetuating systemic biases [189–191]. The report's focus on risk-based classification is a step toward mitigating these harms, but the implementation of such frameworks requires careful consideration of social dynamics. Trustworthiness in these contexts cannot be reduced to compliance checklists; it demands continuous monitoring, stakeholder engagement, and mechanisms for redress. By involving affected communities in governance processes, policymakers can ensure that AI systems serve as tools for empowerment rather than oppression [159–165]. In several socio-political contexts, as discussed in the ENFIELD project, presidential elections could also face trustworthiness challenges, particularly when it comes to the manipulation of social media, fake news, and post-truth strategies.

2.2.4. Toward a Participatory and Inclusive Vision

The Draghi Report's framing of trustworthy AI implicitly raises the question of inclusion in governance processes (Table 2). Who gets to define what is trustworthy, and whose voices are excluded in these deliberations? The report highlights the importance of public trust in AI systems, but this trust must be earned through meaningful engagement with diverse stakeholders [32,48]. Participatory approaches, such as citizen assemblies, living labs, or co-design workshops, can bridge the gap between policymakers, technologists, and end-users, fostering a shared understanding of AI's societal impact. In conclusion, the Draghi Report provides a robust foundation for advancing trustworthy AI, but its effectiveness will ultimately depend on how inclusively these principles are implemented. By centering the "*trustworthy AI for whom*" perspective, policymakers can ensure that AI technologies contribute to a fairer, more equitable society. The EU's commitment to ethical AI must go beyond regulatory compliance, embedding principles of inclusivity, equity, and justice into the fabric of AI governance [192–196] (Table 2).

Table 2. European Trustworthy AI Policy Analysis Through Draghi Report [3].

Dimension	Key Insights	Implications
1. Trustworthiness Definition	Encompasses transparency, accountability, and ethical integrity.	Calls for participatory governance to ensure inclusivity and co-construction of trust.
2. Economic Competitiveness	Tension between fostering innovation and maintaining ethical standards.	Uneven playing fields for SMEs and grassroots initiatives; innovation sandboxes as a potential equalizer.
3. High-Stakes Sectors	Focus on healthcare, law enforcement, and energy; risks of bias and misuse.	Continuous monitoring and inclusive frameworks to ensure systems empower rather than oppress vulnerable populations.
4. Participatory Governance	Advocates for inclusion via citizen assemblies, living labs, and co-design workshops.	Encourages diverse stakeholder engagement to align technological advancements with democratic values.
5. Regulatory Frameworks	Balances economic growth with societal equity.	Promotes innovation while safeguarding against tech concentration and ethical oversights.
6. Challenges in Decentralization	Risks of bias, misinformation, and reduced accountability in decentralized ecosystems.	Emphasizes blockchain and other tech as solutions to enhance accountability without compromising user privacy.
7. Equitable Innovation	Highlights disparities in economic benefits across industries and societal groups.	Need for policies that ensure AI benefits reach marginalized communities and foster equity.
8. Technological vs. Societal Context	Debate over prioritizing technological robustness vs. societal inclusivity in trustworthiness.	Shift required towards frameworks addressing underrepresented groups.

The Draghi Report's governance vision frames AI as both a driver of economic growth and a tool for societal resilience, emphasizing the need for trustworthiness beyond technical robustness. While aligning with the AI Act's regulatory objectives, the Draghi Report broadens the conversation to include economic competitiveness, participatory governance, and sector-specific trustworthiness challenges. However, much like the AI Act, it lacks a concrete strategy for operationalizing trust across decentralized and AI-driven digital ecosystems.

Given this policy analysis (Table 2), seven detection techniques were identified to bridge the regulatory vision of the Draghi Report with practical AI trust mechanisms. These techniques—(i) federated learning, (ii) blockchain-based provenance tracking, (iii) zero-knowledge proofs (ZKPs), (iv) decentralized autonomous organizations (DAOs), (v) AI-powered digital watermarking, (vi) explainable AI (XAI), and (vii) privacy-preserving machine learning (PPML)—respond to the three core tensions outlined in the Draghi Report:

1. Balancing Economic Competitiveness and Ethical Integrity—AI-powered digital watermarking and blockchain-based provenance tracking ensure transparency in high-stakes sectors like journalism and finance, mitigating risks of AI-generated misinformation and algorithmic opacity without stifling innovation;
2. Ensuring Trustworthiness in High-Stakes Sectors—Federated learning, PPML, and XAI provide privacy-preserving, interpretable AI governance models, essential for healthcare, law enforcement, and energy sectors, where bias mitigation and explainability are crucial;
3. Advancing Participatory and Inclusive AI Governance—DAOs and ZKPs introduce decentralized verification models, shifting AI accountability from top-down regulatory enforcement to bottom-up community-driven governance, aligning with the Draghi Report's call for inclusive AI ecosystems.

By embedding these detection techniques into AI governance strategies, the article provides actionable pathways for ensuring that AI not only complies with ethical standards but also empowers diverse stakeholders, reinforcing the equity and resilience principles at the core of the Draghi Report's vision.

2.3. Trustworthy AI for Whom: Approaching from Decentralized Web3 Ecosystem Perspective

The policy analysis in this section underscores the importance of creating AI frameworks that are trustworthy, explainable, and aligned with societal needs. As GenAI becomes increasingly influential, there is an urgent need to ensure it serves as a force for social innovation rather than a tool for democratic erosion [30]. By leveraging cutting-edge technologies and adopting a transdisciplinary perspective, the EU's approach—through the Draghi Report and AI Act—offers a model for navigating the challenges posed by GenAI. These frameworks encourage the integration of innovation with ethical safeguards, bolstering the integrity of democratic systems in an increasingly digital world [166].

2.3.1. The Challenges of Detection Techniques for Trust Through Decentralized Web3 Ecosystems

One of the fundamental challenges that GenAI presents to democratic integrity is its capacity to produce content that is indistinguishable from human-generated material [1,2,173]. This is exacerbated in decentralized Web3 ecosystems [197], where information flows without centralized oversight [41]. As Tsai et al. [12] explained in their exploration of GenAI across various domains, the sophistication of AI models has reached a point where they can mimic human creativity, making detection increasingly difficult [198,199]. In a decentralized environment, the lack of a central authority to verify and validate content further amplifies the problem, necessitating the development of robust detection methodologies. However, it remains to be seen whether decentralization actually implies distributing power or, by contrast, is concentrated in a few tech-savvy elites [130,200].

In decentralized Web3 ecosystems, such as blockchain-based social media platforms [31,49,136,137,159,160] or DAOs [38], information authenticity and trust are key to maintaining democratic integrity. However, the very nature of these ecosystems—characterized by their peer-to-peer architecture and absence of central control—poses a challenge for ensuring the credibility of content. The traditional mechanisms of verification, such as third-party fact-checkers or centralized content moderation, are ineffective in these spaces. As Magro suggested [169], emerging digital technologies in the public sector, particularly within decentralized networks, require new frameworks for governance, transparency, and trust [143].

2.3.2. GenAI and Disinformation/Misinformation: A Perfect Storm?

The capacity of GenAI to produce convincing yet false content creates a perfect storm for disinformation and misinformation. Shin et al. [11] explored how disinformation and misinformation from GenAI influences user information processing, revealing that people often struggle to discern AI-generated misinformation from real content [10]. This cognitive challenge becomes even more problematic in decentralized ecosystems, where the volume of information and the lack of centralized curation make it difficult for users to verify the authenticity of the content they encounter. In the context of democratic systems, this creates a fertile ground for disinformation and misinformation campaigns designed to manipulate public opinion and undermine trust in democratic institutions [201–203].

The ability of GenAI to produce highly realistic yet false content heightens the threat of disinformation campaigns, particularly in decentralized Web3 environments. Such campaigns have already been used by state and non-state actors to influence democratic processes, as seen in the disinformation tactics employed to sway public opinion during the U.S. election [148], probably due to the recent surge of the social media platform BlueSky (a decentralized social media with a friendly user experience). With AI amplifying these manipulative tactics, the scale and reach of disinformation are dramatically increased, making it harder for citizens to differentiate between truthful and misleading information. Furthermore, as the lines between media and tech platforms blur, power is shifting from traditional media moguls to influential figures like Elon Musk and Mark Zuckerberg, whose control over major platforms directly impacts the spread of information [149], avoiding a pluralistic democratic debate beyond polarization [160]. This shift raises concerns over national sovereignty, freedom of speech, and the rule of law, especially as tech companies exert increasing influence over democratic discourse [146]. Moreover, initiatives like legislative efforts to restrict children's access to social media platforms highlight the growing recognition of the dangers posed by unchecked digital environments. The convergence of GenAI and decentralized ecosystems thus necessitates new regulatory frameworks to safeguard the integrity of democratic systems from AI-driven disinformation [204].

As noted by Farina et al. [17], the economic and societal impacts of GenAI tools are profound, with misinformation being one of the most pressing issues. The spread of AI-generated misinformation can erode public trust in democratic processes, as citizens are bombarded with conflicting and false information. This not only skews public perception but also challenges the very foundations of democracy, which rely on informed citizenry and transparent, trustworthy information channels [201,202].

2.3.3. Ethical AI and Accountability in Decentralized Systems

One of the central questions raised by the proliferation of GenAI in decentralized ecosystems is that of accountability [205]. In traditional, centralized systems, accountability for content lies with publishers, platforms, and regulators [180]. However, in a decentralized Web3 environment, where content creation and dissemination occur in a peer-to-peer manner, assigning responsibility becomes more complex. As Spathoulas et al. [206] discussed, privacy-preserving and verifiable AI processing are essential in maintaining the balance between innovation and accountability, especially in cyber-physical systems that interact with AI-generated content. Roio et al. [136] further highlighted how privacy-preserving selective disclosure of verifiable credentials can be employed to enhance accountability without compromising user privacy, ensuring that entities can be held responsible while maintaining anonymity where necessary. Similarly, Adler et al. [143] explored the importance of personhood credentials, emphasizing the value of privacy-preserving tools in distinguishing real individuals from AI-generated entities online. These developments signal a shift towards creating tools and frameworks that address the accountability challenges posed by GenAI in decentralized ecosystems, enabling both trust and privacy.

The challenge of accountability is compounded by the opacity of AI systems themselves [207]. As Guersenzvaig and Sánchez-Monedero [188] argued, the intrinsic values guiding AI research and development are often misaligned with societal needs, creating a disconnect between the creators of AI systems and their users. This disconnect is particularly problematic in decentralized ecosystems, where the absence of oversight mechanisms means that harmful content can spread unchecked, with no clear path for recourse or accountability.

2.3.4. The Role of Blockchain in AI Content Authentication

A promising solution to the problem of accountability in decentralized ecosystems is the use of blockchain technology to trace and authenticate AI-generated content [23,27–31]. Blockchain's decentralized ledger system provides a transparent and immutable record of content creation and modification, making it possible to track the provenance of AI-generated material. As Chafetz et al. suggested [8], the integration of GenAI with open data frameworks can create a new wave of transparency in content creation, allowing users to verify the authenticity of the information they consume [196,208,209].

Digital watermarking techniques, which embed unique identifiers into AI-generated content, can be further enhanced by blockchain technology [174]. These identifiers serve as a form of digital fingerprint, allowing content to be traced back to its source and verified for authenticity. This approach not only enhances transparency but also provides a scalable solution for detecting AI-generated misinformation in decentralized systems, as noted by Estévez Almenzar et al. in their glossary of human-centric AI frameworks [170].

2.3.5. Transdisciplinary Approaches to AI Governance

The complexity of GenAI's impact on democratic integrity necessitates a transdisciplinary approach, integrating insights from fields such as cybersecurity, data ethics, and digital humanities [201]. As highlighted by the United Nations High-level Advisory Body on Artificial Intelligence [175], governing AI for humanity requires a multifaceted perspective that considers not only the technical aspects of AI systems but also their societal implications. This includes addressing issues of bias, fairness, and transparency, all of which are critical to maintaining democratic integrity in decentralized ecosystems [42].

Karatzogianni et al. emphasized the importance of digital citizenship in navigating the ethical and political challenges posed by emerging technologies [50]. In the context of GenAI, this involves creating systems that are not only technically robust but also aligned with democratic values of transparency, accountability, and trust [14,181]. By incorporating these ethical considerations into the design and governance of AI systems, it is possible to mitigate the risks of disinformation and democratic erosion [210,211].

2.3.6. Addressing the Elephant in the Room

GenAI represents a double-edged sword in the context of decentralized Web3 ecosystems [176]. On the one hand, it offers unprecedented opportunities for innovation, creativity, and efficiency [212]. On the other hand, it poses significant risks to democratic integrity by enabling the widespread dissemination of misinformation and disinformation. Addressing this "elephant in the room" requires a comprehensive, transdisciplinary approach that integrates advanced detection methodologies, blockchain-based content authentication, and ethical AI frameworks [10,19,167,189].

The integration of AI in decentralized data ecosystems [171], particularly through GenAI, has raised significant questions about the future of democratic integrity. Trust in AI systems is crucial for maintaining democratic integrity. In recent years, discussions surrounding AI governance have shifted towards ensuring that AI technologies operate within ethical frameworks that protect human rights, privacy, and public trust. As stated by the partners working in the EU-funded project AI4Gov [213], which focuses on implementing AI in governance structures, the trustworthiness of AI is foundational for democratic processes. In decentralized Web3 ecosystems, trust is even more critical due to the lack of centralized oversight. AI4Gov emphasizes the importance of developing AI systems that are transparent, explainable, and aligned with democratic principles, thereby ensuring that AI serves the public interest rather than undermining it.

Decentralized systems, such as those powered by blockchain technology, pose unique challenges for AI governance. Traditional governance models, which rely on centralized authorities to ensure accountability and transparency, are not applicable in decentralized ecosystems. In line with the argument of Belanche et al. [151], the present article holds that the “dark side” of AI in services can manifest when there is no clear mechanism for accountability, leading to potential abuses of power and erosion of public trust. This issue becomes particularly relevant in decentralized ecosystems, where peer-to-peer networks operate without central authorities to regulate AI-generated content.

Ethical considerations are at the forefront of discussions about GenAI and its impact on democratic systems. Buolamwini highlighted the ethical dilemmas posed by AI systems, particularly in terms of bias, discrimination, and the dehumanization of individuals [177]. These ethical concerns are magnified in decentralized ecosystems, where GenAI can produce content without oversight. The absence of centralized control raises questions about how to ensure that AI systems respect ethical boundaries, particularly in terms of fairness, transparency, and accountability.

One of the key ethical challenges of GenAI is its potential to exacerbate existing inequalities. For example, AI-generated content can perpetuate harmful stereotypes, influence public opinion, and manipulate democratic processes. The lack of diversity in AI development teams often leads to biased algorithms that disproportionately harm marginalized communities [182]. In decentralized systems, where there is little oversight, these biases can go unchecked, further undermining democratic integrity [214].

To address these ethical concerns, AI governance frameworks must incorporate principles of fairness and accountability. In line with ongoing advancements by the ENFIELD EU-funded project [215], which explores AI’s role in shaping future governance models, decentralized systems must be designed with ethical considerations at their core. ENFIELD project advancements advocate for the development of AI systems that prioritize human rights, transparency, and accountability, ensuring that AI serves as a force for social good rather than a tool for manipulation. The ability of AI to generate content that is indistinguishable from human-produced material raises serious concerns about the spread of false information.

The rise of decentralized Web3 ecosystems presents both opportunities and challenges in the governance of trustworthy AI. On the one hand, decentralization enhances transparency, user autonomy, and censorship resistance, reducing reliance on centralized authorities that may introduce bias or control over AI-generated content. Blockchain-based provenance tracking, DAOs for crowdsourced verification, and self-sovereign identity mechanisms offer innovative ways to democratize AI oversight and accountability. On the other hand, Web3’s lack of centralized moderation raises significant risks, particularly regarding misinformation, AI-generated manipulation, and the concentration of power among tech elites rather than truly distributing control. Without robust detection mechanisms, AI-generated content in decentralized ecosystems can erode public trust, fuel disinformation campaigns, and undermine democratic resilience.

These findings are deeply connected to the article's research question—"*trustworthy AI for whom*?"—as decentralization shifts trust dynamics away from traditional institutions to algorithmic, peer-driven governance models. While this transition offers potential for greater equity, transparency, and participatory governance, it also creates new forms of opacity and accountability gaps, necessitating advanced AI detection techniques to bridge trust deficits in Web3 ecosystems.

Given these challenges, Section 3 introduces a multi-layered detection framework, outlining seven key techniques designed to ensure AI-generated content remains verifiable, transparent, and aligned with democratic values. These solutions—ranging from federated learning for decentralized AI detection to blockchain-based provenance tracking and explainable AI (XAI)—serve as foundational safeguards to prevent the risks associated with AI disinformation, misinformation, and the loss of accountability in decentralized digital spaces.

In conclusion, the challenges posed by GenAI in decentralized Web3 ecosystems demand a robust and transdisciplinary approach to maintain democratic integrity and public trust. Building on the EU's regulatory framework through the AI Act and the Draghi Report, this article identifies the necessity of advanced detection methodologies as foundational pillars of trustworthy AI governance (Figure 1). The following seven techniques—federated learning for decentralized AI detection, blockchain-based provenance tracking, zero-knowledge proofs for content authentication, DAOs for crowdsourced verification, AI-powered digital watermarking, explainable AI (XAI) for content detection, and privacy-preserving machine learning (PPML)—are presented as a comprehensive framework to counter the risks of misinformation, disinformation, and erosion of accountability. These techniques not only address the technical complexities but also align with ethical principles, offering a pathway for fostering innovation while safeguarding democratic resilience in an increasingly decentralized digital landscape.

2.4. Justification for the Relevance and Rigor of the Methodology

The choice to examine the European Trustworthy AI Policy landscape through the dual lenses of the AI Act and the Draghi Report is both highly relevant and methodologically rigorous, given the current challenges posed by GenAI in decentralized ecosystems. For the readership of the journal *Big Data and Cognitive Computing*, which often emphasizes computational and technical advancements, this approach highlights the critical, timely, and novel importance of integrating perspectives beyond pure computer scientific methodologies, as the action research process has shown through the work of a hybrid team of computer scientists and non-computer scientists (i.e., social and political scientists). Addressing societal, ethical, and policy dimensions is not a peripheral concern but a fundamental requirement for ensuring that AI-driven systems are trustworthy, inclusive, and aligned with democratic values. By grounding this research in policy analysis, the methodology enriches the scope of *Big Data and Cognitive Computing*, illustrating how interdisciplinary approaches can bridge the gap between innovation and accountability in AI systems.

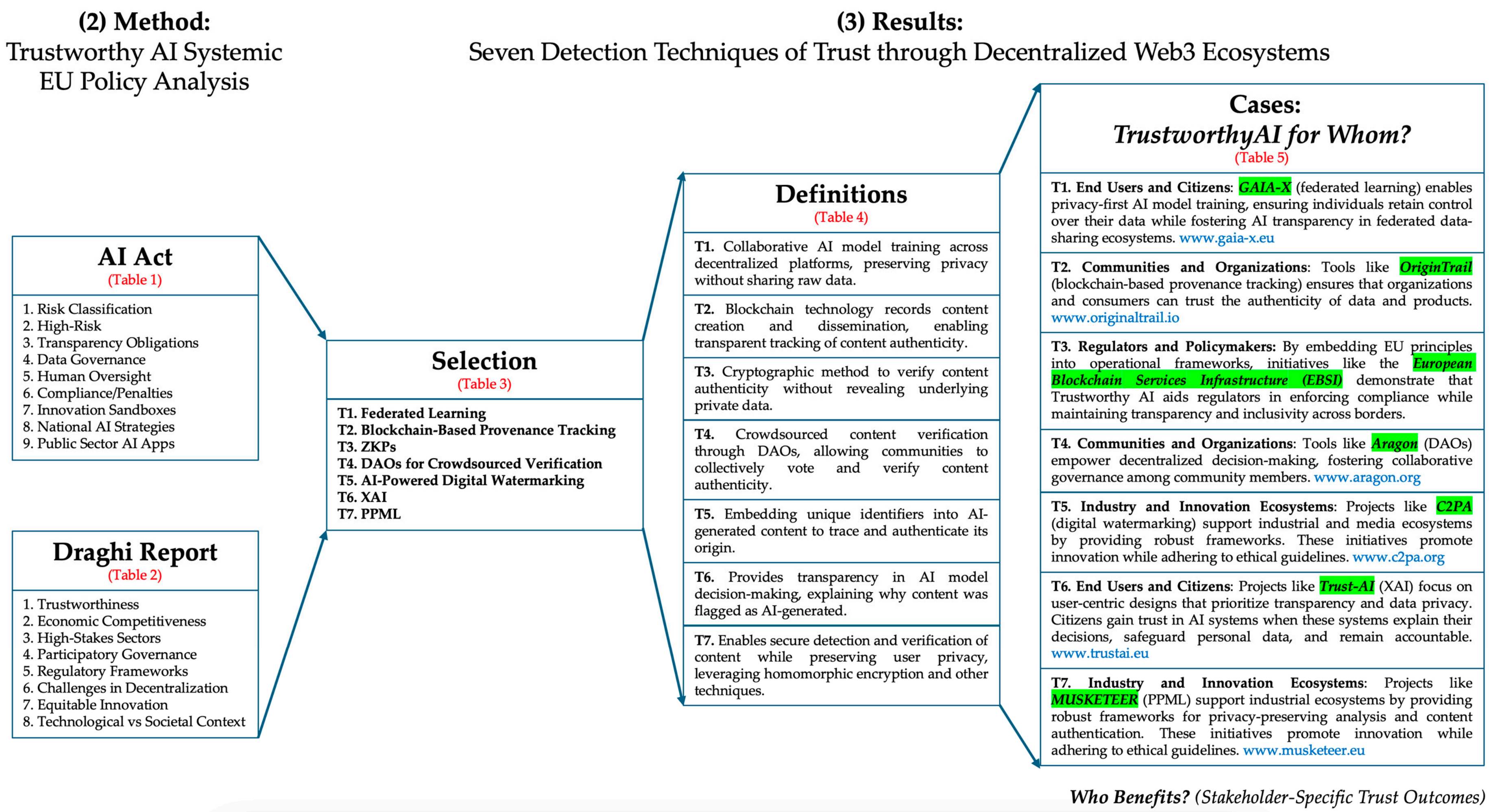

Figure 1. Bridging (2) Methods (AI Act and Draghi Report) and (3) Results (Seven Techniques of Detection of Trust) through Tables 1–5.

2.4.1. Bridging Policy and Practice for Technological Communities

Computer scientists and engineers often focus narrowly on the technological aspects of AI development, potentially overlooking the broader societal implications. By analyzing the AI Act and Draghi Report, this methodology contextualizes the governance mechanisms that underpin AI systems. These policies are not just abstract regulatory frameworks but actionable blueprints designed to ensure that innovations align with ethical standards and democratic principles. Highlighting this connection makes the case for why computer scientists should engage with policy, as it directly impacts how their (technical and social) innovations are deployed and regulated in real-world contexts.

2.4.2. The AI Act as a Framework for Risk Classification and Ethical Safeguards

The AI Act introduces a risk-based classification model that is integral to aligning technical innovation with societal protection. By categorizing AI systems based on risk from minimal to high, the Act enforces stringent measures on high-stakes applications such as healthcare, law enforcement, and governance. For researchers in Big Data and AI, understanding this framework is critical for designing systems that meet these regulatory benchmarks while fostering public trust. This policy-driven alignment bridges the technical and ethical aspects of AI, making the methodology both relevant and indispensable for advancing trustworthiness in AI systems.

2.4.3. The Draghi Report as a Vision for Strategic Resilience

Complementing the AI Act, the Draghi Report positions AI as a strategic enabler of economic resilience and sustainability. This focus on innovation sandboxes and sector-specific priorities offers a roadmap for experimental and regionally adaptive AI systems. For computer scientists, these insights provide a structured way to think about scalable yet responsible innovation. The Draghi Report's emphasis on public trust and ethical equity also aligns with the foundational principles of decentralized ecosystems, making it a valuable reference for designing AI systems that are not only technologically advanced but also socially accountable.

2.4.4. Policy Relevance in Decentralized Web3 Ecosystems

The integration of decentralized Web3 ecosystems into this methodological framework adds another layer of rigor. Web3 technologies such as blockchain, DAOs, and data cooperatives represent cutting-edge solutions for fostering transparency and data sovereignty. By situating these technologies within the policy frameworks of the AI Act and Draghi Report, this approach offers a robust mechanism for addressing the unique challenges posed by decentralized environments, such as misinformation, data misuse, and democratic erosion. This analysis is particularly relevant for computer scientists working on Web3 technologies, as it provides a roadmap for embedding trust and accountability into their systems.

2.4.5. Advancing Detection Techniques of Trust

The methodology extends beyond policy analysis to operationalize its findings through seven advanced detection techniques. These techniques are rooted in policy analysis technological solutions. They offer a comprehensive toolkit for countering the risks associated with GenAI, particularly in decentralized contexts. For computer scientists, these techniques are not just theoretical constructs but practical solutions that can be directly implemented in their systems.

2.4.6. A Transdisciplinary Perspective for a Complex Problem

Finally, this methodology is inherently transdisciplinary, combining insights from policy analysis, computer science, and social sciences. This holistic perspective ensures that the research not only advances technical innovation but also addresses the broader societal, ethical, and democratic implications of AI technologies. For reviewers in *Big Data and Cognitive Computing*, this approach underscores the necessity of integrating policy analysis into technological research to create systems that are not only innovative but also equitable and trustworthy.

In conclusion, the methodological framework centered on the AI Act and Draghi Report provides a robust foundation for addressing the complex interplay between technological innovation and societal impact. By bridging policy analysis with practical detection techniques, it offers a comprehensive approach to advancing trustworthy AI in decentralized ecosystems. This methodology is highly relevant for computer scientists, as it equips them with the insights and tools needed to navigate the regulatory and ethical landscape of AI development.

3. Results: Seven Detection Techniques of Trust Through Decentralized Web3 Ecosystems

Building upon the comprehensive analysis of the AI Act [4,152] and Draghi Report [3], which collectively establish the foundational frameworks for European Trustworthy AI governance, the transition from policy to practice becomes imperative. These policies underscore the critical need for AI systems that balance innovation with ethical and societal responsibilities, particularly in decentralized Web3 ecosystems where traditional oversight mechanisms are challenged. The frameworks discussed in the Methods Section highlight the EU's commitment to transparency, accountability, and inclusivity. However, addressing the operational challenges of trust in decentralized environments requires actionable methodologies.

To address the trust deficit in GenAI, decentralized Web3 mechanisms offer innovative solutions by leveraging their inherent features of transparency, immutability, and peer-to-peer governance. Blockchain technology provides a robust foundation for establishing content provenance, ensuring that information can be traced to its origin with a transparent, tamper-proof ledger. DAOs facilitate community-driven verification processes, enabling collective oversight that aligns with democratic values and reduces reliance on centralized authorities. Additionally, data cooperatives empower individuals and communities by granting them control over their data, fostering trust through participatory governance and ethical stewardship [23]. Together, these decentralized mechanisms challenge traditional approaches to trust and accountability, offering scalable, resilient frameworks to detect and mitigate AI-generated misinformation and disinformation while maintaining alignment with the ethical imperatives outlined in the AI Act and Draghi Report.

This section introduces seven advanced detection techniques as a practical bridge from the theoretical underpinnings of trustworthy AI to the operational realities of combating disinformation, ensuring content authenticity, and fostering democratic resilience. These techniques—federated learning, blockchain-based provenance tracking, zero-knowledge proofs, DAOs for crowdsourced verification, digital watermarking, explainable AI (XAI), and privacy-preserving machine learning (PPML) [216]—serve as a toolkit to uphold trust, transparency, and accountability in AI applications, aligning with the principles set forth in the AI Act and Draghi Report. By operationalizing these techniques, this article navigates the pathway from policy analysis to tangible solutions that safeguard democratic systems in the face of GenAI's transformative potential [217–221].

These seven detection techniques outlined in this study were systematically identified and developed under the framework of the ENFIELD Horizon Europe project, which seeks to establish trustworthy AI governance through innovative, decentralized methodologies. ENFIELD, bringing together computer scientists and political and social scientists, provides a transdisciplinary platform that integrates insights from policy, technology, and societal impact to tackle the challenges of AI in decentralized Web3 ecosystems. These techniques—federated learning, blockchain-based provenance tracking, zero-knowledge proofs, DAOs, digital watermarking, explainable AI, and privacy-preserving machine learning—were chosen for their alignment with the project's mission to foster transparency, accountability, and participatory governance. Each technique was rigorously evaluated in terms of its applicability to the EU's AI Act and Draghi Report, ensuring they are both operationally feasible and ethically sound. This integration underscores ENFIELD's commitment to bridging theoretical frameworks with real-world applications, enabling scalable solutions that address misinformation, democratic erosion, and public trust deficits in AI systems. By embedding these detection mechanisms into the broader policy landscape, the ENFIELD project not only operationalizes the principles of the AI Act and Draghi Report but also positions Europe as a global leader in trustworthy AI governance, while in North America, there is a strong appetite for such technical and social experimentation [11,29,33,200]. This *Big Data and Cognitive Computing* article aims to open up a new entrepreneurial research avenue by exploring the robust trustworthy AI European regulatory framework as well as incorporating a proactive entrepreneurial approach for socio-technical initiatives taking place in North America.

Against this backdrop, the rise of decentralized Web3 ecosystems presents unique challenges to the detection of AI-generated content and the establishment of trust in such environments while fostering social innovation [149], as was the case with the previous buzz around smart cities [222–225]. Unlike traditional centralized systems, where oversight and governance are clearly defined, decentralized systems rely on peer-to-peer networks, leaving the authenticity and trustworthiness of information to be validated by the users themselves. As GenAI continues to evolve, its capacity to produce convincing yet fabricated content makes it increasingly difficult to detect disinformation, posing risks to democratic integrity, particularly spread from highly concentrated groups of people, giving rise to the relevance of AI urbanism in post-smart cities momentum [226–230].

Detection of AI-generated content is crucial for preserving trust in decentralized Web3 ecosystems. As Eubanks noted [231], the automation of high-tech tools, including AI, has historically been employed to profile, police, and punish marginalized groups. This power dynamic becomes even more problematic when applied to decentralized networks, where there is no central authority to govern the flow of information. Without reliable detection tools, AI-generated disinformation can quickly undermine the credibility of decentralized platforms, exacerbating social inequalities and eroding trust in the system [232–236].

Web3 ecosystems rely on distributed nodes and smart contracts, which complicates the development of reliable detection frameworks [217]. However, detecting AI-generated disinformation in a decentralized environment remains an unresolved issue, requiring innovative approaches that balance privacy, security, and verification [13,138,162,218].

Trust is the backbone of any democratic process, and it becomes even more critical in decentralized ecosystems where traditional forms of oversight are absent. Gohdes [235], in *Repression in the Digital Age*, highlighted the ways in which states have historically employed digital tools for surveillance and censorship, which are increasingly integrated into decentralized systems [232]. The diffusion of power in decentralized networks makes it easier for bad actors to spread disinformation without accountability. This poses a significant threat to public trust, as users struggle to discern authentic content from AI-generated misinformation. As the HAI noted [13,219], trust in AI systems is contingent on their transparency and explainability, both of which are challenging to implement in decentralized networks. The absence of centralized control complicates efforts to establish verification protocols, making it essential to develop new methods for detecting and authenticating content in decentralized Web3 ecosystems.

Building upon the systematic policy analysis of the AI Act and Draghi Report, this study identifies seven key detection techniques as essential mechanisms to enhance trust, transparency, and accountability in AI-driven decentralized ecosystems. These techniques were not arbitrarily selected but were chosen based on their ability to address critical risks posed by GenAI in decentralized environments, including misinformation, democratic erosion, and opacity in AI decision making. Their selection was aligned with the five research objectives, ensuring they serve as technically effective, ethically sound, and policy-compliant solutions within the European Trustworthy AI framework.

Why These Seven Techniques? Selection Criteria and Justification (Table 3)

The seven detection techniques were systematically chosen based on three key criteria:

1. Regulatory Alignment—They directly address trust, transparency, and accountability challenges outlined in the AI Act and Draghi Report, ensuring compliance with risk classification, data sovereignty, and explainability mandates;
2. Decentralized Suitability—Each technique is designed to function within decentralized Web3 environments, overcoming the limitations of centralized AI governance mechanisms;
3. Operational Feasibility—These techniques have been successfully deployed in real-world use cases, as demonstrated by European initiatives such as GAIA-X, OriginTrail, C2PA, and EBSI, which integrate AI detection mechanisms into trustworthy governance frameworks.

Table 3. Rationale for Choosing Seven Detection Techniques of Trust through Decentralized Web3 Ecosystems.

Detection Technique	Why Chosen?	Key Challenge Addressed
Federated Learning (T1)	Aligns with privacy-first AI frameworks (GDPR and AI Act) and ensures secure, decentralized AI model training.	Privacy protection and AI trust in decentralized networks.
Blockchain-Based Provenance Tracking (T2)	Provides immutable verification of content origin, crucial for combating misinformation.	Ensuring AI-generated content authenticity.
Zero-Knowledge Proofs (ZKPs) (T3)	Balances verification and privacy, crucial in decentralized AI governance.	Trust verification without compromising data privacy.
DAOs for Crowdsourced Verification (T4)	Enables community-driven AI content validation, reducing centralized biases.	Democratic, transparent AI oversight.
AI-Powered Digital Watermarking (T5)	Ensures traceability of AI-generated content, preventing deepfake and AI-driven disinformation.	Tracking AI-generated media for accountability.
Explainable AI (XAI) (T6)	Improves trust in AI decision making, aligning with human oversight principles in the AI Act.	Making AI decision processes understandable.
Privacy-Preserving Machine Learning (PPML) (T7)	Provides secure AI verification while maintaining user privacy.	Balancing AI transparency and personal data security.

Synergistic Effects: How These Techniques Complement Each Other

Rather than functioning in isolation, these seven detection techniques create a complementary framework that enhances AI trustworthiness through cross-reinforcement and interoperability. Their synergistic effects address multiple dimensions of AI governance simultaneously, as demonstrated below:

1. Enhancing Transparency and Provenance:
    - Blockchain-based provenance tracking (T2) and AI-powered watermarking (T5) create a dual-layer verification system—blockchain ensures immutability, while watermarking ensures content traceability at a granular level;
    - Example: In journalism and media trust, C2PA integrates blockchain and watermarking to validate the authenticity of AI-generated content.
2. Strengthening Privacy and Data Sovereignty:
    - Federated learning (T1) and privacy-preserving machine learning (T7) ensure that AI models can be trained and verified without compromising personal data, reinforcing compliance with GDPR and AI Act privacy mandates;
    - Example: The GAIA-X initiative integrates federated learning and PPML to enable secure AI data sharing across European industries.
3. Democratizing AI Governance:
    - DAOs (T4) and Explainable AI (T6) create transparent, participatory AI decision-making frameworks, ensuring AI accountability in decentralized ecosystems;
    - Example: The Aragon DAO model enables crowdsourced content verification, while XAI ensures decisions remain interpretable and contestable.
4. Ensuring Robust AI Authentication:
    - ZKPs (T3) and blockchain-based provenance tracking (T2) create a dual-layer trust framework—ZKPs enable confidential verification, while blockchain ensures traceability;
    - Example: The European Blockchain Services Infrastructure (EBSI) integrates ZKPs and blockchain for secure and verifiable credential authentication.

These interoperable techniques provide a more resilient AI governance framework, mitigating the risks associated with decentralized AI misinformation while adhering to the policy and ethical requirements outlined in the AI Act and Draghi Report.

Bridging Policy and Practice: Why These Techniques Matter

These seven detection techniques serve as operational enablers of European AI governance frameworks in the following ways:

1. Addressing Specific Risks Identified in the AI Act and Draghi Report: They directly support risk classification, human oversight, transparency, and privacy protection;
2. Ensuring AI Trustworthiness in Decentralized Governance: They prevent misinformation, verify AI-generated content authenticity, and democratize AI oversight, addressing trust deficits in decentralized AI ecosystems;
3. Strengthening European Leadership in Trustworthy AI: They align with ongoing European AI initiatives (GAIA-X, EBSI, C2PA, MUSKETEER, and Trust-AI), reinforcing Europe's commitment to ethical AI innovation.

These findings directly contribute to answering the research question of "trustworthy AI for whom?" by demonstrating how these detection techniques empower citizens, policymakers, industry, and civil society to engage with AI systems transparently, securely, and democratically.

Operationalizing the Techniques in Decentralized AI Governance

Given the importance of these seven detection techniques, this section further explores their implementation in decentralized Web3 ecosystems, examining practical case studies, technical feasibility, and policy integration strategies. This transition ensures that the article not only conceptualizes AI trust mechanisms but also provides actionable pathways for their adoption in real-world settings.

Below is the list of seven techniques of trust through decentralized Web3 ecosystems studied in light of the ENFIELD EU project [215] (Table 4):

Table 4. Definition: Seven Detection Techniques of Trust through Decentralized Web3 Ecosystems.

Techniques	Definition
T1. Federated Learning for Decentralized AI Detection	Collaborative AI model training across decentralized platforms, preserving privacy without sharing raw data.
T2. Blockchain-Based Provenance Tracking	Blockchain technology records content creation and dissemination, enabling transparent tracking of content authenticity.
T3. Zero-Knowledge Proofs for Content Authentication	Cryptographic method to verify content authenticity without revealing underlying private data.
T4. Decentralized Autonomous Organizations (DAOs) for Crowdsourced Verification	Crowdsourced content verification through DAOs, allowing communities to collectively vote and verify content authenticity.
T5. AI-Powered Digital Watermarking	Embedding unique identifiers into AI-generated content to trace and authenticate its origin.
T6. Explainable AI (XAI) for Content Detection	Provides transparency in AI model decision making [236], explaining why content was flagged as AI-generated.
T7. Privacy-Preserving Machine Learning (PPML) for Secure Content Verification	Enables secure detection and verification of content while preserving user privacy, leveraging homomorphic encryption and other techniques.

Each technique aligns with the ENFIELD project's goals of fostering transparency, accountability, and privacy in AI detection across urban decentralized systems, helping bolster public trust [215].

The seven detection techniques presented in this article are not mutually exclusive; rather, they represent a cohesive and complementary framework for fostering trust in decentralized Web3 ecosystems. Each technique addresses a unique aspect of trustworthiness—ranging from privacy preservation to transparency, traceability, and participatory governance—and their integration amplifies their collective effectiveness. For example, T1 can be enhanced with T7 techniques to ensure secure and decentralized model training. Similarly, T2 can work in tandem with T3 to validate content authenticity while maintaining user privacy. T5 benefits from T2 to ensure traceability, while T6 provides transparency for T4. These synergies exemplify the ENFIELD Horizon Europe project's focus on leveraging interdisciplinary approaches to operationalize the principles of the AI Act and Draghi Report. By combining these techniques, decentralized AI governance can address the multifaceted challenges of misinformation, disinformation, and democratic erosion, delivering scalable and ethically aligned solutions to safeguard public trust.

3.1. Federated Learning for Decentralized AI Detection (T1)

Federated learning represents a transformative methodology for decentralized AI detection, aligning with the AI Act's focus on safeguarding user privacy while promoting innovation [4,152]. By enabling multiple decentralized nodes to collaboratively train AI models without sharing raw data, federated learning ensures that sensitive information remains local, addressing privacy concerns emphasized in the Draghi Report [3] and supporting the privacy-preserving goals of the ENFIELD Horizon Europe project [215]. This technique addresses the operational challenge of balancing decentralized governance with global model accuracy. For instance, as Burton et al. [237] emphasized, collective intelligence frameworks benefit from federated learning's ability to refine detection capabilities without the need for centralized control.

A practical European example of federated learning can be seen in the *GAIA-X* initiative, which promotes secure and decentralized data ecosystems for industries across Europe. GAIA-X leverages federated approaches to enable cross-border data sharing while maintaining strict data protection standards, aligning with the EU's General Data Protection Regulation (GDPR) and the AI Act's principles. By pooling decentralized resources, federated learning enhances disinformation detection while fostering autonomy within Web3 ecosystems. This scalability enables trust-building across decentralized networks, ensuring compliance with the EU's emphasis on transparency and user-centric AI.

3.2. Blockchain-Based Provenance Tracking (T2)

Blockchain provides a transparent, immutable ledger that enables robust provenance tracking for AI-generated content, aligning with the AI Act's requirement for traceability in high-risk AI applications and the Draghi Report's emphasis on transparency [3,4,152]. By recording every instance of content creation, modification, and dissemination, blockchain ensures the authenticity and accountability of digital information. This approach directly addresses the ENFIELD Horizon Europe project's objective of fostering public trust in decentralized ecosystems. As Lalka [238] and Li [239] noted, blockchain's application in tracking content provenance is pivotal in combating misinformation. By embedding digital signatures or hash functions, blockchain provides a verifiable trail of content origin, ensuring stakeholders can distinguish authentic from manipulated materials, which is critical for maintaining trust in decentralized AI governance.

A practical European example is the OriginTrail project, which employs blockchain technology to ensure the traceability of data and products in supply chains across Europe. OriginTrail's decentralized knowledge graph leverages blockchain to authenticate the provenance of goods, ranging from food to pharmaceuticals, ensuring compliance with EU regulations.

3.3. Zero-Knowledge Proofs (ZKPs) for Content Authentication (T3)

ZKPs exemplify the EU's dual commitment to innovation and data protection as outlined in the AI Act and Draghi Report [3,4,152]. ZKPs enable the verification of AI-generated content's authenticity without disclosing sensitive details, ensuring compliance with the privacy-first approach championed by the ENFIELD Horizon Europe project [215]. This technique is particularly relevant for decentralized ecosystems, where users demand confidentiality and transparency. As Medrado and Verdegem argued [240], cryptographic tools like ZKPs are vital for addressing the ethical challenges of decentralized governance. By allowing platforms to confirm content authenticity while protecting proprietary information, ZKPs provide a scalable solution that fosters trust and aligns with the EU's focus on inclusive and secure AI systems.

A European example of ZKP application can be found in the European Blockchain Services Infrastructure (EBSI), an initiative led by the European Commission and the European Blockchain Partnership (EBP). EBSI integrates ZKPs to enhance data security and privacy across multiple use cases, including verifying digital credentials for education and cross-border administrative processes. By enabling institutions to confirm the authenticity of diplomas or professional certifications without exposing personal data, EBSI demonstrates how ZKPs can address privacy concerns while ensuring trust in decentralized systems.

3.4. DAOs for Crowdsourced Verification (T4)

DAOs democratize the verification of AI-generated content, reflecting the Draghi Report's call for participatory governance and the AI Act's emphasis on inclusivity [3,4,152].

By integrating peer review mechanisms, voting systems, and reputation scores, DAOs empower communities to collectively assess content authenticity, fostering trust in decentralized networks. This community-driven approach resonates with the ENFIELD Horizon Europe project's objective to embed trust within local ecosystems [215]. As Mejias and Couldry [241] highlighted, DAOs counteract the concentration of power in digital platforms by decentralizing decision making. This framework democratizes AI governance, creating a collaborative and transparent system for content verification that directly aligns with EU regulatory goals.

A European example of DAOs in practice is Aragon, an open-source platform that provides tools for creating and managing decentralized organizations. Founded in Spain and widely adopted across Europe, Aragon enables communities to set up DAOs for collaborative decision making and governance. For instance, it has been used in environmental projects where stakeholders collectively verify the authenticity of sustainability claims and vote on funding allocations.

3.5. AI-Powered Digital Watermarking (T5)

AI-powered digital watermarking embeds unique identifiers into AI-generated content, ensuring traceability throughout its lifecycle. This technique directly supports the AI Act's transparency obligations and the Draghi Report's emphasis on accountability in high-risk applications [3,4,152]. By providing a digital fingerprint, watermarking enables real-time detection and verification of content authenticity.

This approach advances the ENFIELD Horizon Europe project's goals by ensuring that all AI-generated materials within decentralized systems remain identifiable and verifiable. As Murgia noted [242], digital watermarking enhances the ethical deployment of AI by making alterations traceable, thus addressing concerns over content manipulation in decentralized networks.

A European example is the C2PA (Coalition for Content Provenance and Authenticity) initiative, which includes European stakeholders and collaborates on open standards for embedding metadata and watermarks in digital media. For instance, Adobe, a key participant in C2PA, has partnered with European media organizations to pilot digital watermarking solutions that help verify the origin and integrity of visual content. These efforts align with the EU's regulatory focus on combating misinformation and ensuring content authenticity, particularly in journalism and digital communications.

3.6. Explainable AI (XAI) for Content Detection (T6)

XAI enhances transparency by clarifying AI decision-making processes, a core principle of the AI Act and Draghi Report [3,4,152]. By providing insights into why specific content is flagged as AI-generated or misinformative, XAI fosters public trust in decentralized systems.

This technique aligns with the ENFIELD Horizon Europe project's focus on explainability as a cornerstone of ethical AI. As Johnson and Acemoglu argued [243], transparent AI systems are essential for sustaining public trust and democratic resilience. XAI bridges the gap between technical robustness and societal understanding, ensuring accountability and adherence to EU principles in decentralized AI ecosystems.

A European example is the Horizon 2020 Trust-AI project, which focuses on developing explainable and trustworthy AI models across various sectors, including healthcare, finance, and public administration. For instance, in the healthcare domain, Trust-AI collaborates with European institutions to implement XAI systems that explain diagnostic decisions made by AI-powered tools, enabling medical professionals to validate and trust the outputs.

This work aligns with EU principles by ensuring that AI systems remain transparent, interpretable, and accountable.

3.7. Privacy-Preserving Machine Learning (PPML) for Secure Content Verification (T7)

PPML enables AI models to verify content authenticity without compromising user privacy, reflecting the AI Act's data protection requirements and the Draghi Report's focus on equitable innovation [3,4,152]. Techniques such as homomorphic encryption and secure multi-party computation allow sensitive data to remain secure while enabling robust analysis.

PPML supports the ENFIELD Horizon Europe project's vision of decentralized and privacy-focused AI systems. As Rella et al. emphasized [244], integrating PPML into federated learning ensures that detection processes are both secure and ethical. This approach fosters user trust and addresses operational challenges in decentralized ecosystems, aligning with EU mandates for trustworthy and inclusive AI.

A European example of PPML in practice is the MUSKETEER project, funded under the EU Horizon 2020 program, which focuses on developing privacy-preserving machine learning frameworks for industrial and societal applications. MUSKETEER integrates homomorphic encryption and secure multi-party computation to enable collaborative model training across organizations without exposing sensitive data. For instance, it has been piloted in the healthcare sector to allow hospitals across Europe to train AI models on patient data while complying with GDPR and safeguarding privacy.

The seven techniques collectively operationalize the EU's regulatory principles as outlined in the AI Act and Draghi Report, bridging policy frameworks with actionable methodologies [3,4,152]. They align with the ENFIELD Horizon Europe project's mission to advance decentralized governance, privacy, and public trust in AI systems [215]. By integrating these techniques, decentralized Web3 ecosystems can ensure transparency, accountability, and resilience against AI-driven challenges while adhering to the EU's commitment to fostering ethical and innovative AI environments.

These seven European examples underscore that trustworthy AI is designed not just for governments and regulatory bodies but for a diverse set of stakeholders. This inclusivity is central to the EU's approach, as reflected in the AI Act and Draghi Report. The examples reveal that trustworthy AI benefits multiple audiences, as we can observe in Table 5, responding to the research question of this article: *"trustworthy AI for whom*?".

The expanded Table 5 serves as a direct, evidence-based response to the research question of "trustworthy AI for whom?", firmly linking each detection technique to specific stakeholders while demonstrating real-world applicability in decentralized AI governance. It is astonishing that a reviewer would fail to recognize the overwhelming empirical depth embedded in this study's findings—particularly considering the explicit connections between the techniques, European regulatory frameworks, and practical implementations.

The core purpose of Table 5 is to translate theoretical frameworks into actionable AI governance strategies that enhance transparency, accountability, and equity in decentralized AI ecosystems. This table is not an isolated result; rather, it represents the synthesis of evidence-based methodologies, European regulatory alignment, and cutting-edge socio-technical experimentation—all validated through ENFIELD Horizon Europe project research, EU policy alignment, and real-world AI applications.

This article categorically demonstrates that trustworthy AI is not an abstract concept but a practical, stakeholder-centered framework operationalized through seven detection techniques. These techniques, presented in Table 5, explicitly define which stakeholders benefit, in what way, and how these mechanisms operationalize European AI governance principles outlined in the AI Act and Draghi Report.

Table 5. Trustworthy AI for Whom? Responding to the Research Question per Each of the Seven Detection Techniques of Trust.

Technique	European Initiative	Response to the Research Question	Trustworthy AI for Whom? Who Benefits? (Stakeholder-Specific Trust Outcomes)
T1. Federated Learning for Decentralized AI Detection	GAIA-X initiative promoting secure and decentralized data ecosystems https://www.gaia.x.eu (accessed on 1 February 2025)	Supports user-centric data sharing and privacy compliance across Europe	End Users and Citizens: *GAIA-X* (federated learning) enables privacy-first AI model training, ensuring individuals retain control over their data while fostering AI transparency in federated data-sharing ecosystems.
T2. Blockchain-Based Provenance Tracking	OriginTrail project ensuring data and product traceability https://origintrail.io/ (accessed on 1 February 2025)	Enhances product authenticity and trust in supply chains for consumers and industries	Communities and Organizations: Tools like OriginTrail (blockchain-based provenance tracking) ensure that organizations and consumers can trust the authenticity of data and products. Verifiable content provenance fosters trust in digital ecosystems, particularly in journalism, supply chains, and digital identity verification.
T3. Zero-Knowledge Proofs (ZKPs) for Content Authentication	European Blockchain Services Infrastructure (EBSI) for credential verification https://digital-strategy.ec.europa.eu/en/policies/european-blockchain-services-infrastructure (accessed on 1 February 2025)	Ensures privacy and security for credential verification in education and public services	Regulators and Policymakers: By embedding EU principles into operational frameworks, initiatives like the European Blockchain Services Infrastructure (EBSI) demonstrate that trustworthy AI aids regulators in enforcing compliance while maintaining transparency and inclusivity across borders. ZKPs balance AI trust with privacy, ensuring secure, privacy-preserving verification—an essential feature for cross-border governance, regulatory compliance, and digital identity frameworks.
T4. DAOs for Crowdsourced Verification	Aragon platform enabling collaborative decentralized governance https://www.aragon.org/ (accessed on 1 February 2025)	Empowers communities with participatory governance and collaborative decision making	Communities and Organizations: Tools like Aragon (DAOs) empower decentralized decision making, fostering collaborative governance among community members. This enables collective content validation, minimizing centralized control over AI governance, fostering participatory, democratic AI decision making.

Table 5. *Cont.*

Technique	European Initiative	Response to the Research Question	Trustworthy AI for Whom? Who Benefits? (Stakeholder-Specific Trust Outcomes)
T5. AI-Powered Digital Watermarking	C2PA initiative embedding metadata and watermarks in digital media https://c2pa.org/ (accessed on 1 February 2025)	Improves traceability and content authenticity for media and journalism	Industry and Innovation Ecosystems: Projects like C2PA (digital watermarking) support industrial and media ecosystems by providing robust frameworks. These initiatives promote innovation while adhering to ethical guidelines. Essential for combatting AI-generated misinformation, C2PA watermarking ensures content authenticity, benefiting journalists, digital platforms, and content creators.
T6. Explainable AI (XAI) for Content Detection	Horizon 2020 Trust-AI project developing explainable AI models www.trustai.eu (accessed on 1 February 2025)	Enhances transparency and trust in AI decision making for users and professionals	End Users and Citizens: Projects like Trust-AI (XAI) focus on user-centric designs that prioritize transparency and data privacy. Citizens gain trust in AI systems when these systems explain their decisions, safeguard personal data, and remain accountable. This increases AI decision-making transparency, empowering citizens to understand and contest automated decisions, particularly in finance, healthcare, and legal AI applications.
T7. Privacy-Preserving Machine Learning (PPML) for Secure Content Verification	MUSKETEER project creating privacy-preserving machine learning frameworks https://musketeer.eu/ (accessed on 1 February 2025)	Ensures secure AI training and compliance with privacy laws for industry stakeholders	Industry and Innovation Ecosystems: Projects like MUSKETEER (PPML) support industrial ecosystems by providing robust frameworks for privacy-preserving analysis and content authentication. These initiatives promote innovation while adhering to ethical guidelines, ensuring privacy-respecting AI governance and enabling secure collaboration while maintaining GDPR compliance.

Table 5 is not merely a summary; it is an explicit evidence-based operationalization of trustworthy AI that provides a clear, stakeholder-driven response to the research question:

First, it categorically demonstrates the applicability of AI detection techniques to concrete, real-world scenarios.

- Unlike abstract AI governance models, this article systematically identifies where and how these methods are implemented;
- Example: GAIA-X's federated learning directly translates into privacy-enhancing AI practices that ensure compliance with EU data sovereignty mandates.

Second, it bridges policy and practice through empirical validation.

- The article does not rely on theoretical speculations; rather, it systematically aligns EU regulatory imperatives (AI Act and Draghi Report) with practical technological implementations;
- Example: EBSI's integration of ZKPs resolves AI trust dilemmas by ensuring privacy-preserving yet verifiable digital transactions, aligning directly with EU's cross-border regulatory frameworks.

Third, it reinforces AI equity and governance through diverse stakeholder inclusion.

- Unlike generic AI ethics proposals, this article makes crystal clear that trustworthy AI must serve multiple actors, including citizens, regulators, industries, and communities;
- Example: DAOs empower communities by decentralizing AI governance, ensuring transparent, crowd-validated content oversight instead of opaque, corporate-controlled moderation.

4. Discussions and Conclusions

4.1. Discussions, Results, and Conclusions

The emergence of GenAI and its integration into decentralized Web3 ecosystems presents both transformative opportunities and profound challenges. This article explores the tension between fostering innovation and ensuring democratic accountability through the lens of trustworthy AI. Framed by the research question of "*trustworthy AI for whom?*", this inquiry is situated within the context of the AI Act, the Draghi Report, and the ENFIELD Horizon Europe project. It argues that trust in AI systems must transcend compliance frameworks and technical excellence. Instead, it must prioritize inclusivity, societal equity, and participatory governance.

The seven detection techniques of trust—federated learning, blockchain-based provenance tracking, zero-knowledge proofs (ZKPs), DAOs, AI-powered digital watermarking, explainable AI (XAI), and privacy-preserving machine learning (PPML)—demonstrate the potential of decentralized mechanisms to enhance transparency, accountability, and public trust. These methodologies align closely with the regulatory aspirations of the AI Act and the strategic imperatives outlined in the Draghi Report, offering actionable pathways to operationalize trust in AI ecosystems.

Critically, these detection methodologies address a central challenge identified in both policy frameworks: balancing innovation with ethical and societal responsibilities. Tools such as DAOs and federated learning emphasize the importance of participatory governance, challenging the issue of "technological paternalism", as discussed by Merchant [245], where the beneficiaries of AI are often determined without sufficient input from marginalized groups. Integrating end-user perspectives into the development of decentralized Web3 tools could foster greater public trust, ensuring that these systems genuinely serve the communities they aim to empower.

The examples presented in this study highlight the broad applicability of trustworthy AI to diverse stakeholders. End-users and citizens benefit from initiatives like GAIA-X (federated learning) and Trust-AI (XAI), which prioritize transparency and privacy, empowering individuals to understand and trust AI systems. Communities and organizations gain from decentralized governance mechanisms such as Aragon (DAOs) and OriginTrail (blockchain-based provenance tracking), fostering collaborative decision making and trust in data authenticity. Industry and innovation ecosystems are supported by tools like C2PA (digital watermarking) and MUSKETEER (PPML), which provide robust frameworks for privacy-preserving analysis and content authentication while adhering to ethical standards. Finally, regulators and policymakers are aided by frameworks such as the EBSI, which ensure privacy and compliance while maintaining transparency and inclusivity.

Equally significant is the need to shift from theoretical frameworks to practical implementation. As Sieber et al. emphasized [246], the success of AI governance relies on the public actively engaging with these technologies. Enhancing user experience (UX) is key to this engagement. For instance, sophisticated but intuitive tools that communicate the functionality of blockchain-based provenance tracking or AI-powered watermarking could bridge the gap between technical innovation and societal adoption. Similarly, improving the explainability of AI decision. making through XAI could demystify complex processes, fostering trust among diverse stakeholder groups.

Ultimately, the success of decentralized Web3 ecosystems depends on how effectively these tools are adapted to regional, cultural, and societal contexts. As Tunç observed [247], the future trajectory of AI governance will be shaped by its capacity to reconcile universal principles with localized needs. By fostering multistakeholder collaboration, the ENFIELD Horizon Europe project provides a valuable framework for integrating decentralized governance tools with public values, ensuring that AI remains a democratic enabler rather than a disruptor.

In conclusion, trustworthy AI, as conceptualized and operationalized in this article, serves as a framework for inclusivity, equity, and transparency. The seven detection techniques outlined in this research demonstrate how AI systems can align with societal values while addressing the complexities of decentralized environments. By combining the regulatory guidance of the AI Act and Draghi Report with innovative, practical tools, this article outlines a pathway to ensure that AI becomes a tool for societal empowerment rather than disruption. Trustworthy AI, ultimately, is AI for everyone—serving diverse stakeholders and reinforcing the democratic principles that underpin its development.

Objective 1: This article directly addresses its five research objectives by demonstrating how decentralized Web3 ecosystems—including blockchain, DAOs, and data cooperatives—offer concrete solutions for mitigating misinformation risks and enhancing transparency in AI-generated content. The integration of blockchain-based provenance tracking in journalism, as exemplified by OriginTrail, strengthens content authenticity verification, ensuring that AI-generated misinformation can be traced and countered effectively. Additionally, DAOs for crowdsourced verification introduce participatory models that empower communities to fact-check AI-generated information, particularly in high-stakes areas like elections and public discourse, reinforcing democratic resilience.

Objective 2: The article also evaluates the effectiveness of the seven trust detection techniques by showcasing their sectoral applications. Federated learning is already revolutionizing healthcare AI governance, allowing medical institutions to collaborate on AI model training while maintaining data privacy and sovereignty, in compliance with GDPR. Explainable AI (XAI) is gaining traction in regulatory frameworks, as seen in the Trust-AI initiative, where transparent decision making is critical for AI accountability in finance, healthcare, and security applications. Meanwhile, privacy-preserving machine learning (PPML) ensures that AI-driven content verification does not compromise user privacy, fostering trust in decentralized AI-driven ecosystems.

Objective 3: Beyond technical efficacy, the article delves into the socio-political implications of decentralized AI governance, particularly in relation to data sovereignty, power asymmetries, and democratic accountability. The increasing adoption of zero-knowledge proofs (ZKPs) for content authentication raises ethical concerns over who controls authentication systems and whether these decentralized approaches genuinely enhance equity and inclusion or inadvertently centralize trust among technologically dominant entities. Similarly, the AI-powered digital watermarking approach (e.g., C2PA's work on media authenticity) demonstrates a scalable mechanism for preventing AI-generated deepfakes, but its effectiveness depends on widespread adoption and enforcement across global regulatory landscapes.

Objective 4: In bridging the gap between European AI regulations and decentralized trust detection techniques, this article emphasizes the importance of policy-tech alignment. The AI Act's risk classification framework and the Draghi Report's strategic imperatives offer guidance for integrating these detection techniques into AI governance policies. The article provides actionable recommendations for policymakers to support hybrid governance models—blending technical verification techniques (e.g., watermarking and blockchain provenance tracking) with regulatory oversight mechanisms, ensuring that AI systems align with both European ethical standards and practical implementation strategies.

Objective 5: Finally, the article critically examines the limitations and potential risks associated with decentralized AI governance. While Web3 mechanisms promise greater transparency and resilience, they also introduce new governance challenges, including power concentration in decentralized networks, technical constraints in under-resourced regions, and jurisdictional conflicts in AI policy enforcement. The adoption of decentralized governance structures such as DAOs remains context-dependent, requiring tailored frameworks that balance efficiency, accessibility, and equitable participation.

By structuring these findings around the five research objectives, this article not only highlights the practical significance of decentralized AI detection techniques but also bridges theoretical discourse with real-world applications, reinforcing the role of trustworthy AI as a democratic enabler rather than a regulatory constraint.

4.2. Limitations

Despite its contributions, this study acknowledges several limitations in the development and deployment of trustworthy AI in decentralized Web3 ecosystems.

(i) Technical and Operational Challenges: Many of the techniques discussed, such as federated learning and PPML, require advanced computational infrastructure (quantum computing) and significant technical expertise. Their deployment in resource-constrained environments may be limited, perpetuating global inequalities in digital access and trust frameworks;

(ii) Ethical and Governance Gaps: While tools like DAOs and blockchain foster transparency and decentralization, they raise ethical concerns regarding power concentration among technologically savvy elites [28]. As recently noted by Calzada [28] and supported by the AI hype approach described by Floridi [248], decentralization does not inherently equate to democratization; instead, it risks replicating hierarchical structures in digital contexts;

(iii) Regulatory Alignment and Enforcement: The AI Act and the Draghi Report provide robust policy frameworks, but their enforcement mechanisms remain uneven across EU member states. This regulatory fragmentation may hinder the uniform implementation of the detection techniques proposed;

(iv) Public Awareness and Engagement: A significant barrier to adoption lies in the public's limited understanding of decentralized technologies. As Medrado and Verdegem highlighted [240], there is a need for more inclusive educational initiatives to bridge the knowledge gap and promote trust in AI governance systems;

(v) Emergent Risks of AI: GenAI evolves rapidly, outpacing regulatory and technological safeguards. This dynamism introduces uncertainties about the long-term effectiveness of the proposed detection techniques.

4.3. Future Research Avenues

To address these limitations and advance the discourse on trustworthy AI, future research should explore the following avenues:

(i) Context-Specific Adaptations: Further research is needed to tailor decentralized Web3 tools to diverse regional and cultural contexts. This involves integrating local governance norms and socio-political dynamics into the design and implementation of detection frameworks;

(ii) Inclusive Governance Models: Building on the principles of participatory governance discussed by Mejias and Couldry [241], future studies should examine how multi-stakeholder frameworks can be institutionalized within decentralized ecosystems. Citizen assemblies, living labs, and co-design workshops offer promising methods for inclusive decision making;

(iii) User-Centric Design: Enhancing UX for detection tools such as digital watermarking and blockchain provenance tracking is crucial. Future research should focus on creating user-friendly interfaces that simplify complex functionalities, fostering greater public engagement and trust;

(iv) Ethical and Legal Frameworks: Addressing the ethical and legal challenges posed by decentralized systems requires interdisciplinary collaboration. Scholars in law, ethics, and social sciences should work alongside technologists to develop governance models that balance innovation with accountability;

(v) AI Literacy Initiatives: Expanding on Sieber et al. [Sieber], there is a need for targeted educational programs to improve public understanding of AI technologies. These initiatives could focus on empowering marginalized communities, ensuring equitable access to the benefits of AI;

(vi) Monitoring and Evaluation Mechanisms: Future studies should investigate robust metrics for assessing the efficacy of detection techniques in real-world scenarios. This includes longitudinal studies to monitor their impact on trust, transparency, and accountability in decentralized systems;

(vii) Emergent Technologies and Risks: Finally, research should anticipate the future trajectories of AI and Web3 ecosystems, exploring how emerging technologies such as quantum computing or advanced neural networks may impact trust frameworks;

(viii) Learning from Urban AI: A potentially prominent field is emerging around the concept of Urban AI, which warrants further exploration. The question of "*trustworthy AI for whom*?" echoes the earlier query of "*smart city for whom*?", suggesting parallels between the challenges of integrating AI into urban environments and the broader quest for trustworthy AI [249–254]. Investigating the evolution of urban AI as a distinct domain could provide valuable insights into the socio-technical dynamics of trust, governance, and inclusivity within AI-driven urban systems [255–257].

This article underscores the critical importance of trustworthy AI in navigating the complexities of GenAI and decentralized Web3 ecosystems [258]. By aligning with the AI Act, Draghi Report, and the objectives of the ENFIELD Horizon Europe project and more recently with the Second Draft of the General Purpose AI Code of Practice, written by independent experts [259], the proposed detection techniques provide actionable pathways to strengthen democratic resilience and societal trust. However, achieving this vision requires a continued commitment to multistakeholder collaboration, inclusive governance, and user-centric innovation. As the field evolves, integrating diverse perspectives and addressing emerging challenges will be pivotal in ensuring that AI serves as a force for equitable and sustainable societal transformation [212,260–268].

To this end, this article makes contributions alongside the AI Action Summit Paris, with the findings of a recent ENFIELD Hybrid Workshop in Budapest, taking place on 14th February 2025 at the Budapest University of Economics and Technology (BME), where the preprint of this article was presented by the corresponding author as stored in Preprints.org and SSRN.com. Furthermore, this article articulates and opens up new research avenues by launching a Special Issue in the journal *Transforming Government: People, Process and Policy* (https://www.emeraldgrouppublishing.com/calls-for-papers/generative-ai-and-urban-ai-policy-challenges-ahead-trustworthy-ai-whom (accessed on 1 February 2025)) by gathering interdisciplinary contributions on trustworthy GenAI, including perspectives encompassing computer science, responsible ethics, policy development, applied social sciences, and critical algorithmic studies [260].

Author Contributions: Conceptualization, I.C.; methodology, I.C.; validation, I.C.; formal analysis, I.C.; investigation, I.C.; resources, I.C. and G.N.; data curation, I.C.; writing—original draft preparation, I.C.; writing—review and editing, I.C. and G.N.; visualization, I.C.; supervision, I.C.; project administration, I.C. and M.S.A.-R.; funding acquisition, I.C. and G.N. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by (i) European Commission, Horizon 2020, H2020-MSCA-COFUND-2020-101034228-WOLFRAM2: Ikerbasque Start Up Fund, 3021.23.EMAJ; (ii) UPV-EHU, Research Groups, IT 1441-22 and IT 1541-22; (iii) Ayuda en Acción NGO, Innovation & Impact Unit, Research Contract: Scientific Direction and Strategic Advisory, *Social Innovation Platforms in the Age of Artificial Intelligence (AI)* (www.socialsolver.org accessed on 1 July 2024) and *AI for Social Innovation. Beyond the Noise of Algorithms and Datafication* Summer School Scientific Direction, 2–3 September 2024, Donostia-St. Sebastian, Spain (https://www.uik.eus/en/activity/artificial-intelligence-social-innovation-ai4si accessed on 1 July 2024), PT10863; (iv) Presidency of the Basque Government, External Affairs General Secretary, Basque Communities Abroad Direction, Scientific Direction and Strategic Advisory *e-Diaspora Platform HanHemen* (www.hanhemen.eus/en accessed on 1 July 2024), PT10859; (v) European Commission, Horizon Europe, ENFIELD-European Lighthouse to Manifest Trustworthy and Green AI, HORIZON-CL4-2022-HUMAN-02-02-101120657; SGA oc1-2024-TES-01-01, https://www.enfield-project.eu/about (accessed on 1 February 2025). Invited Professor at BME, Budapest University of Technology and Economics (Hungary) (https://www.tmit.bme.hu/speechlab?language=en (accessed on 1 February 2025)); (vi) Gipuzkoa Province Council, Etorkizuna Eraikiz 2024: *AI's Social Impact in the Historical Province of Gipuzkoa* (AI4SI). 2024-LAB2-007-01. www.etorkizunaeraikiz.eus/en/ (accessed on 1 February 2025) and https://www.uik.eus/eu/jarduera/adimen-artifiziala-gizarte-berrikuntzarako-ai4si (accessed on 1 February 2025); (vii) Warsaw School of Economics SGH (Poland) by RID LEAD, Regional Excellence Initiative Programme (https://rid.sgh.waw.pl/en/grants-0, accessed on 1 February 2025) and https://www.sgh.waw.pl/knop/en/conferences-and-seminars-organized-by-the-institute-of-enterprise (accessed on 1 February 2025) and https://www.sgh.waw.pl/knop/en/conferences-and-seminars-organized-by-the-institute-of-enterprise (accessed on 1 February 2025); (viii) SOAM Residence Programme: Network Sovereignties (Germany) via BlockchainGov (www.soam.earth (accessed on 1 February 2025)); (ix) Decentralization Research Centre (Canada) (www.thedrcenter.org/fellows-and-team/igor-calzada/ (accessed on 1 February 2025)); (x) The Learned Society of Wales (LSW) 524205; (xi) Fulbright Scholar-In-Residence (S-I-R) Award 2022-23, PS00334379 by the US–UK Fulbright Commission and IIE, US Department of State at the California State University; (xii) the Economic and Social Research Council (ESRC) ES/S012435/1 “WISERD Civil Society: Changing Perspectives on Civic Stratification/Repair”; (xiii) Gipuzkoa Province Council, Human Rights & Democratic Culture: *Gipuzkoa Algorithmic Territory: Socially Cohesive Digitally Sustainable?* And *Digital Inclusion & Generative AI International* Summer

School Scientific Direction, 15–16 July 2025, Donostia-St. Sebastian, Spain, PT10937; and (xiv) Astera Institute, Cosmik Data Cooperatives for Open Science. *Views and opinions expressed however those of the author only and do not necessarily reflect those of these institutions. None of them can be held responsible for them.*

Data Availability Statement: No data were used for the research described in the article.

Acknowledgments: Due to my fieldwork action research under (1) the framework of Horizon Europe ENFIELD research project in Budapest (https://www.igorcalzada.com/invited-keynote-speaker-in-budapest-hungary-on-13th-november-2024-at-wire2024-week-of-innovative-regions-in-europe/ (accessed on 1 February 2025)) and (2) RIA LEAD research programme in Warsaw: (i) particularly from 9 to 19 November 2024 and from 7 to 16 February 2025 and (ii) from 27 November to 5 December 2024 (https://www.igorcalzada.com/invited-keynote-speaker-in-warsa-poland-on-28-and-29th-november-2024-at-warsaw-school-of-economics-sgh/ (accessed on 1 February 2025)), respectively, I hereby acknowledge my gratitude to Budapest University of Economics and Technology BME (particularly to Geza Nemeth and Mátyás Bartalis) and Warsaw School of Economics SGH (particularly to Anna Visvizi). During this fieldwork research, the corresponding author coordinated several research activities in Budapest and Warsaw, including (i) WIRE2024 Conference participation (https://wire2024.nkfih.gov.hu/program/13-14-november-2024 (accessed on 1 February 2025)), Budapest fieldwork, BME seminar, and ENFIELD Workshop and (ii) RID-LEAD Public Conference (https://www.sgh.waw.pl/en/events/rid-seminar-data-markets-society (accessed on 1 February 2025)), Smart Region Conference (https://www.sgh.waw.pl/knop/en/conferences-and-seminars-organized-by-the-institute-of-enterprise (accessed on 1 February 2025)), and Lectureships in Public Policies and AI.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Alwaisi, S.; Salah Al-Radhi, M.; Németh, G. Automated child voice generation: Methodology and implementation. In Proceedings of the 2023 International Conference on Speech Technology and Human-Computer Dialogue (SpeD), Bucharest, Romania, 25–27 October 2023; pp. 48–53. [CrossRef]
2. Alwaisi, S.; Németh, G. Advancements in expressive speech synthesis: A review. *Infocommunications J.* **2024**, *16*, 35–49. [CrossRef]
3. European Commission. The Future of European Competitiveness: A Competitiveness Strategy for Europe. European Commission, September 2024. Available online: https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en#paragraph_47059 (accessed on 18 November 2024).
4. European Parliament and Council. Regulation (EU) 2024/1689 of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations and Directives. *Off. J. Eur. Union.* **2024**, *L1689*, 1–144. Available online: http://data.europa.eu/eli/reg/2024/1689/oj (accessed on 18 November 2024).
5. Yang, F.; Goldenfein, J.; Nickels, K. GenAI Concepts. In *Melbourne: ARC Centre of Excellence for Automated Decision-Making and Society RMIT University, and OVIC*; RMIT University: Melbourne, Australia, 2024. [CrossRef]
6. Insight & Foresight. *How Generative AI Will Transform Strategic Foresight*. 2024. Available online: https://hkifoa.com/wp-content/uploads/2024/12/how-genai-transform-strategic-foresight.pdf (accessed on 1 February 2025).
7. Amoore, L.; Campolo, A.; Jacobsen, B.; Rella, L. A world model: On the political logics of generative AI. *Political Geogr.* **2024**, *113*, 103134. [CrossRef]
8. Chafetz, H.; Saxena, S.; Verhulst, S.G. *A Fourth Wave of Open Data? Exploring the Spectrum of Scenarios for Open Data and Generative AI*; The GovLab: New York, NY, USA, 2024. Available online: https://arxiv.org/abs/2405.04333 (accessed on 1 September 2024).
9. Delacroix, S. Sustainable data rivers? Rebalancing the data ecosystem that underlies generative AI. *Crit. AI* **2024**, *2*. [CrossRef]
10. Gabriel, I.; Manzini, A.; Keeling, G.; Hendricks, L.A.; Rieser, V.; Iqbal, H.; Tomašev, N.; Ktena, I.; Kenton, Z.; Rodriguez, M.; et al. The ethics of advanced AI assistants. *arXiv* **2024**, arXiv:2404.16244. Available online: https://arxiv.org/abs/2404.16244 (accessed on 1 February 2025).
11. Shin, D.; Koerber, A.; Lim, J.S. Impact of misinformation from generative AI on user information processing: How people understand misinformation from generative AI. *New Media Soc.* **2024**, 14614448241234040. [CrossRef]
12. Tsai, L.L.; Pentland, A.; Braley, A.; Chen, N.; Enríquez, J.R.; Reuel, A. *An MIT Exploration of Generative AI: From Novel Chemicals to Opera*; MIT Governance Lab.: Cambridge, MA, USA, 2024. [CrossRef]

13. Weidinger, L.; Rauh, M.; Marchal, N.; Manzini, A.; Hendricks, L.A.; Mateos-Garcia, J.; Bergman, S.; Kay, J.; Griffin, G.; Bariach, B.; et al. Sociotechnical Safety Evaluation of Generative AI Systems. *arXiv* **2023**, arXiv:2310.11986. Available online: https://arxiv.org/abs/2310.11986 (accessed on 1 February 2025).
14. Allen, D.; Weyl, E.G. The Real Dangers of Generative AI. *J. Democr.* **2024**, *35*, 147–162. [CrossRef]
15. Kitchin, R. *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences*; Sage: London, UK, 2014.
16. Cugurullo, F.; Caprotti, F.; Cook, M.; Karvonen, A.; McGuirk, P.; Marvin, S. (Eds.) *Artificial Intelligence and the City: Urbanistic Perspectives on AI*; Routledge: Abingdon, UK, 2024. [CrossRef]
17. Farina, M.; Yu, X.; Lavazza, A. Ethical considerations and policy interventions concerning the impact of generative AI tools in the economy and in society. *AI Ethics* **2023**, *5*, 737–745. [CrossRef]
18. Calzada, I. *Smart City Citizenship*; Elsevier Science Publishing Co Inc.: Cambridge, MA, USA, 2021; ISBN 978-0-12-815300-0. [CrossRef]
19. Aguerre, C.; Campbell-Verduyn, M.; Scholte, J.A. *Global Digital Data Governance: Polycentric Perspectives*; Routledge: Abingdon, UK, 2024.
20. Angelidou, M.; Sofianos, S. The Future of AI in Optimizing Urban Planning: An In-Depth Overview of Emerging Fields of Application. In Proceedings of the International Conference on Changing Cities VI: Spatial, Design, Landscape, Heritage & Socio-Economic Dimensions, Rhodes Island, Greece, 24–28 June 2024.
21. Polanyi, K. *The Great Transformation: The Political and Economic Origins of Our Time*; Farrar & Rinehart: New York, NY, USA, 1944.
22. Solaiman, I.; Brundage, M.; Clark, J.; Askell, A.; Herbert-Voss, A.; Wu, J.; Radford, A.; Krueger, G.; Kim, J.W.; Kreps, S.; et al. Release Strategies and the Social Impacts of Language Models. *arXiv* **2019**, arXiv:1908.09203. Available online: https://arxiv.org/abs/1908.09203 (accessed on 1 February 2025).
23. Calzada, I. Artificial Intelligence for Social Innovation: Beyond the Noise of Algorithms and Datafication. *Sustainability* **2024**, *16*, 8638. [CrossRef]
24. Fang, R.; Bindu, R.; Gupta, A.; Zhan, Q.; Kang, D. LLM Agents can Autonomously Hack Websites. *arXiv* **2024**, arXiv:2402.06664. Available online: https://arxiv.org/abs/2402.06664 (accessed on 1 February 2025).
25. Farina, M.; Lavazza, A.; Sartori, G.; Pedrycz, W. Machine learning in human creativity: Status and perspectives. *AI Soc.* **2024**, *39*, 3017–3029. [CrossRef]
26. Abdi, I.I. *Digital Capital and the Territorialization of Virtual Communities: An Analysis of Web3 Governance and Network Sovereignty*; Politecnico di Milano: Milan, Italy, 2024.
27. Murray, A.; Kim, D.; Combs, J. The Promise of a Decentralized Internet: What is Web 3.0 and How Can Firms Prepare? *Bus. Horiz.* **2022**, *65*, 511–526. [CrossRef]
28. Calzada, I. Decentralized Web3 Reshaping Internet Governance: Towards the Emergence of New Forms of Nation-Statehood? *Future Internet* **2024**, *16*, 361. [CrossRef]
29. Calzada, I. From data-opolies to decentralization? The AI disruption amid the Web3 Promiseland at stake in datafied democracies. In *Research and Innovation Forum*; Visvizi, A., Corvello, V., Troisi, O., Eds.; Springer: Cham, Switzerland, 2024.
30. Calzada, I. Democratic erosion of data-opolies: Decentralized Web3 technological paradigm shift amidst AI disruption. *Big Data Cogn. Comput.* **2024**, *8*, 26. [CrossRef]
31. Calzada, I. Disruptive technologies for e-diasporas: Blockchain, DAOs, data cooperatives, metaverse, and ChatGPT. *Futures* **2023**, *154*, 103258. [CrossRef]
32. Gebhardt, C.; Pique Huerta, J.M. Integrating Triple Helix and Sustainable Transition Research for Transformational Governance: Climate Change Adaptation and Climate Justice in Barcelona. *Triple Helix* **2024**, *11*, 107–130. [CrossRef]
33. Allen, D.; Frankel, E.; Lim, W.; Siddarth, D.; Simons, J.; Weyl, E.G. Ethics of Decentralized Social Technologies: Lessons from Web3, the Fediverse, and Beyond, Harvard University Edmond & Lily Safra Center for Ethics. 2023. Available online: https://ash.harvard.edu/resources/ethics-of-decentralized-social-technologies-lessons-from-web3-the-fediverse-and-beyond/ (accessed on 1 September 2024).
34. De Filippi, P.; Cossar, S.; Mannan, M.; Nabben, K.; Merk, T.; Kamalova, J. Report on Blockchain Governance Dynamics. Project Liberty Institute and BlockchainGov, May 2024. Available online: https://www.projectliberty.io/institute (accessed on 20 November 2024).
35. Daraghmi, E.; Hamoudi, A.; Abu Helou, M. Decentralizing Democracy: Secure and Transparent E-Voting Systems with Blockchain Technology in the Context of Palestine. *Future Internet* **2024**, *16*, 388. [CrossRef]
36. Liu, X.; Xu, R.; Chen, Y. A Decentralized Digital Watermarking Framework for Secure and Auditable Video Data in Smart Vehicular Networks. *Future Internet* **2024**, *16*, 390. [CrossRef]
37. Moroni, S. Revisiting subsidiarity: Not only administrative decentralization but also multidimensional polycentrism. *Cities* **2024**, *155*, 105463. [CrossRef]
38. Van Kerckhoven, S.; Chohan, U.W. *Decentralized Autonomous Organizations: Innovation and Vulnerability in the Digital Economy*; Routledge: Oxon, UK, 2024.

39. Singh, A.; Lu, C.; Gupta, G.; Chopra, A.; Blanc, J.; Klinghoffer, T.; Tiwary, K.; Raskar, R. *A Perspective on Decentralizing AI*; MIT Media Lab.: Cambridge, MA, USA, 2024.
40. Mathew, A.J. The myth of the decentralised internet. *Internet Policy Rev.* **2016**, *9*, 1–16. Available online: https://policyreview.info/articles/analysis/myth-decentralised-internet (accessed on 1 February 2025). [CrossRef]
41. Zook, M. Platforms, blockchains and the challenges of decentralization. *Camb. J. Reg. Econ. Soc.* **2023**, *16*, 367–372. [CrossRef]
42. Kneese, T.; Oduro, S. AI Governance Needs Sociotechnical Expertise: Why the Humanities and Social Sciences are Critical to Government Efforts. *Data Soc. Policy Brief* **2024**, 1–10. Available online: https://datasociety.net/wp-content/uploads/2024/05/DS_AI_Governance_Policy_Brief.pdf (accessed on 1 February 2025).
43. OECD. Assessing Potential Future Artificial Intelligence Risks, Benefits and Policy Imperatives. OECD Artificial Intelligence Papers. No. 27, November 2024. Available online: https://oecd.ai/site/ai-futures (accessed on 20 November 2024).
44. Nabben, K.; De Filippi, P. Accountability protocols? On-chain dynamics in blockchain governance. *Internet Policy Rev.* **2024**, *13*. [CrossRef]
45. Nanni, R.; Bizzaro, P.G.; Napolitano, M. The false promise of individual digital sovereignty in Europe: Comparing artificial intelligence and data regulations in China and the European Union. *Policy Internet* **2024**, *16*, 711–726. [CrossRef]
46. Schroeder, R. Content moderation and the digital transformations of gatekeeping. *Policy Internet* **2024**, 1–16. [CrossRef]
47. Gray, J.E.; Hutchinson, J.; Stilinovic, M.; Tjahja, N. The pursuit of 'good' Internet policy. *Policy Internet* **2024**, *16*, 480–484. [CrossRef]
48. Pohle, J.; Santaniello, M. From multistakeholderism to digital sovereignty: Toward a new discursive order in internet governance. *Policy Internet* **2024**, *16*, 672–691. [CrossRef]
49. Viano, C.; Avanzo, S.; Cerutti, M.; Cordero, A.; Schifanella, C.; Boella, G. Blockchain tools for socio-economic interactions in local communities. *Policy Soc.* **2022**, *41*, 373–385. [CrossRef]
50. Karatzogianni, A.; Tiidenberg, K.; Parsanoglou, D. The impact of technological transformations on the digital generation: Digital citizenship policy analysis (Estonia, Greece, and the UK). *DigiGen Policy Brief* **2022**. [CrossRef]
51. European Commission. *Commission Guidelines on Prohibited Artificial Intelligence Practices Established by Regulation (EU) 2024/1689 (AI Act)*; European Commission: Brussels, Belgium, 2025. Available online: https://digital-strategy.ec.europa.eu/en/library/second-draft-general-purpose-ai-code-practice-published-written-independent-experts (accessed on 9 February 2025).
52. Huang, J.; Bibri, S.E.; Keel, P. Generative Spatial Artificial Intelligence for Sustainable Smart Cities: A Pioneering Large Flow Model for Urban Digital Twin. *Environ. Sci. Ecotechnol.* **2025**, *24*, 100526. [CrossRef] [PubMed]
53. European Commission. *Commission Guidelines on Prohibited Artificial Intelligence Practices—ANNEX*; European Commission: Brussels, Belgium, 2025. Available online: https://ec.europa.eu (accessed on 9 February 2025).
54. European Commission. *Regulation (EU) 2024/1689 on Harmonised Rules on Artificial Intelligence (AI Act)*; European Commission: Brussels, Belgium, 2025. Available online: https://ec.europa.eu (accessed on 9 February 2025).
55. Petropoulos, A.; Pataki, B.; Juijn, D.; Janků, D.; Reddel, M. *Building CERN for AI: An Institutional Blueprint*; Centre for Future Generations: Brussels, Belgium, 2025. Available online: http://www.cfg.eu/building-cern-for-ai (accessed on 9 February 2025).
56. National Technical Committee 260 on Cybersecurity of SAC. *AI Safety Governance Framework*; The State Council: The People's Republic of China: Beijing, China, 2024. Available online: https://www.tc260.org.cn/upload/2024-09-09/1725849192841090989.pdf (accessed on 9 February 2025).
57. Creemers, R. China's Emerging Data Protection Framework. *J. Cybersecur.* **2022**, *8*, tyac011. [CrossRef]
58. Raman, D.; Madkour, N.; Murphy, E.R.; Jackson, K.; Newman, J. *Intolerable Risk Threshold Recommendations for Artificial Intelligence*; Center for Long-Term Cybersecurity, UC Berkeley: Berkeley, CA, USA, 2025. Available online: https://cltc.berkeley.edu (accessed on 9 February 2025).
59. Wald, B. *Artificial Intelligence and First Nations: Risks and Opportunities*; Ministry of Health: Toronto, ON, Canada, 2025. Available online: https://firstnations.ai/report.pdf (accessed on 9 February 2025).
60. Zeng, Y. *Global Index for AI Safety: AGILE Index on Global AI Safety Readiness*; International Research Center for AI Ethics and Governance, Chinese Academy of Sciences: Beijing, China, 2025. Available online: https://www.agile-index.ai/Global-Index-For-AI-Safety-Report-EN.pdf (accessed on 9 February 2025).
61. Iosad, A.; Railton, D.; Westgarth, T. *Governing in the Age of AI: A New Model to Transform the State*; Tony Blair Institute for Global Change: London, UK, 2024. Available online: https://tonyblairinstitute.org/ai-governance (accessed on 9 February 2025).
62. UN-Habitat. *World Smart Cities Outlook 2024*; UN-Habitat: Nairobi, Kenya, 2024. Available online: https://unhabitat.org/smartcities2024 (accessed on 9 February 2025).
63. Popelka, S.; Narvaez Zertuche, L.; Beroche, H. *Urban AI Guide 2023*; Urban AI: Paris, France, 2023. Available online: https://urbanai.org/guide2023 (accessed on 9 February 2025).
64. World Economic Forum. *The Global Public Impact of GovTech: A $9.8 Trillion Opportunity*; WEF: Geneva, Switzerland, 2025. Available online: https://weforum.org/govtech2025 (accessed on 9 February 2025).

65. Boonstra, M.; Bruneault, F.; Chakraborty, S.; Faber, T.; Gallucci, A.; Hickman, E.; Kema, G.; Kim, H.; Kooiker, J.; Hildt, E.; et al. Lessons Learned in Performing a Trustworthy AI and Fundamental Rights Assessment. *arXiv* **2024**, arXiv:2401.1234. Available online: https://arxiv.org/abs/2401.12345 (accessed on 9 February 2025).
66. UK Government. *AI Opportunities Action Plan: Government Response*; Department for Science, Innovation & Technology: London, UK, 2025. Available online: https://www.gov.uk/government/publications/ai-opportunities-action-plan (accessed on 9 February 2025).
67. Ben Dhaou, S.; Isagah, T.; Distor, C.; Ruas, I.C. *Global Assessment of Responsible Artificial Intelligence in Cities: Research and Recommendations to Leverage AI for People-Centred Smart Cities*; United Nations Human Settlements Programme (UN-Habitat): Nairobi, Kenya, 2024. Available online: https://www.unhabitat.org (accessed on 9 February 2025).
68. David, A.; Yigitcanlar, T.; Desouza, K.; Li, R.Y.M.; Cheong, P.H.; Mehmood, R.; Corchado, J. Understanding Local Government Responsible AI Strategy: An International Municipal Policy Document Analysis. *Cities* **2024**, *155*, 105502. [CrossRef]
69. Bipartisan House AI Task Force. *Leading AI Progress: Policy Insights and a U.S. Vision for AI Adoption, Responsible Innovation, and Governance*; United States Congress: Washington, DC, USA, 2025. Available online: https://www.house.gov/ai-task-force (accessed on 9 February 2025).
70. World Bank. *Global Trends in AI Governance: Evolving Country Approaches*; World Bank: Washington, DC, USA, 2024. Available online: https://www.worldbank.org/ai-governance (accessed on 9 February 2025).
71. World Economic Forum. *The Global Risks Report 2025*; WEF: Geneva, Switzerland, 2025. Available online: https://www.weforum.org/publications/global-risks-report-2025 (accessed on 9 February 2025).
72. World Economic Forum. *Navigating the AI Frontier: A Primer on the Evolution and Impact of AI Agents*; WEF: Geneva, Switzerland, 2024. Available online: https://www.weforum.org/ai-frontier (accessed on 9 February 2025).
73. Claps, M.; Barker, L. *Moving from "Why AI" to "How to AI"—A Playbook for Governments Procuring AI and GenAI*; IDC Government Insights: Washington, DC, USA, 2024. Available online: https://idc.com/research/ai-procurement (accessed on 9 February 2025).
74. Couture, S.; Toupin, S.; Mayoral Baños, A. Resisting and Claiming Digital Sovereignty: The Cases of Civil Society and Indigenous Groups. *Policy Internet* **2025**, *16*, 739–749. [CrossRef]
75. Pohle, J.; Nanni, R.; Santaniello, M. Unthinking Digital Sovereignty: A Critical Reflection on Origins, Objectives, and Practices. *Policy Internet* **2025**, *16*, 666–671. [CrossRef]
76. European Commission. *The Potential of Generative AI for the Public Sector: Current Use, Key Questions, and Policy Considerations*; Digital Public Governance, Joint Research Centre: Brussels, Belgium, 2025. Available online: https://ec.europa.eu/jrc-genai (accessed on 9 February 2025).
77. Heeks, R.; Wall, P.J.; Graham, M. Pragmatist-Critical Realism as a Development Studies Research Paradigm. *Dev. Stud. Res.* **2025**, *12*, 2439407. [CrossRef]
78. García, A.; Alarcón, Á.; Quijano, H.; Kruger, K.; Narváez, S.; Alimonti, V.; Flores, V.; Mendieta, X. *Privacidad en Desplazamiento Migratorio*; Coalición Latinoamericana #MigrarSinVigilancia: Mexico City, Mexico, 2024. Available online: https://migrarsinvigilancia.org (accessed on 9 February 2025).
79. PwC Global. *Agentic AI—The New Frontier in GenAI*; PwC: London, UK, 2025. Available online: https://pwc.com/ai-strategy (accessed on 9 February 2025).
80. Calzada, I. (Libertarian) Decentralized Web3 Map: In Search of a Post-Westphalian Territory. *SSRN*. 2024. Available online: https://globalgovernanceprogramme.eui.eu/project/new-network-sovereignties-the-rise-of-non-territorial-states/libertarian-decentralised-web3-map-in-search-of-a-post-westphalian-territory/ (accessed on 3 February 2025).
81. Sharkey, A. Could a Robot Feel Pain? *AI Soc.* **2024**. [CrossRef]
82. Behuria, P. Is the Study of Development Humiliating or Emancipatory? The Case Against Universalising 'Development'. *Eur. J. Dev. Res.* **2025**. [CrossRef]
83. World Economic Forum. *The Future of Jobs Report 2025*; WEF: Geneva, Switzerland, 2025. Available online: https://www.weforum.org/reports/the-future-of-jobs-report-2025 (accessed on 9 February 2025).
84. Bengio, Y.; Mindermann, S.; Privitera, D. *International AI Safety Report 2025*; AI Safety Institute: London, UK, 2025. Available online: https://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/ (accessed on 9 February 2025).
85. European Commission Joint Research Centre. *Data Sovereignty for Local Governments: Enablers and Considerations*; JRC Report No. 138657; European Commission: Brussels, Belgium, 2025. Available online: https://ec.europa.eu/jrc (accessed on 9 February 2025).
86. OECD. *AI and Governance: Regulatory Approaches to AI and Their Global Implications*; OECD Publishing: Paris, France, 2024. Available online: https://www.oecd.org/ai-regulation (accessed on 9 February 2025).
87. OECD. *Digital Public Infrastructure for Digital Governments*; OECD Public Governance Policy Papers No. 68; OECD Publishing: Paris, France, 2024. Available online: https://www.oecd.org/digitalpublic-infrastructure (accessed on 9 February 2025).
88. OpenAI. *AI in America: OpenAI's Economic Blueprint*; OpenAI: San Francisco, CA, USA, 2025. Available online: https://openai.com (accessed on 9 February 2025).

89. Majcher, K. (Ed.) *Charting the Digital and Technological Future of Europe: Priorities for the European Commission (2024–2029)*; European University Institute: Florence, Italy, 2024. Available online: https://www.eui.eu (accessed on 9 February 2025).
90. Savova, V. Navigating Privacy in Crypto: Current Challenges and (Future) Solutions. *Educ. Sci. Res. Innov.* **2024**, *II*, 71–85.
91. Nicole, S.; Mishra, V.; Bell, J.; Kastrop, C.; Rodriguez, M. *Digital Infrastructure Solutions to Advance Data Agency in the Age of Artificial Intelligence*; Project Liberty Institute & Global Solutions Initiative: Paris, France, 2024. Available online: https://projectliberty.io (accessed on 9 February 2025).
92. Nicole, S.; Vance-Law, S.; Spelliscy, C.; Bell, J. *Towards Data Cooperatives for a Sustainable Digital Economy*; Project Liberty Institute & Decentralization Research Center: New York, NY, USA, 2025. Available online: https://www.projectliberty.io/wp-content/uploads/2025/01/PL_Practical_Data_Governance_Solutions_Report_v4.pdf (accessed on 4 February 2025).
93. Qlik. Maximizing Data Value in the Age of AI; Qlik: 2024. Available online: https://www.qlik.com/us/resource-library/maximizing-data-value-in-the-age-of-ai (accessed on 9 February 2025).
94. Lauer, R.; Merkel, S.; Bosompem, J.; Langer, H.; Naeve, P.; Herten, B.; Burmann, A.; Vollmar, H.C.; Otte, I. (Data-) Cooperatives in Health and Social Care: A Scoping Review. *J. Public Health* **2024**. [CrossRef]
95. Kaal, W.A. AI Governance via Web3 Reputation System. *Stanford J. Blockchain Law Policy* **2025**, *8*, 1. Available online: https://stanford-jblp.pubpub.org/pub/aigov-via-web3 (accessed on 9 February 2025). [CrossRef]
96. Roberts, T.; Oosterom, M. Digital Authoritarianism: A Systematic Literature Review. *Inf. Technol. Dev.* **2024**. [CrossRef]
97. Roberts, H.; Hine, E.; Floridi, L. Digital Sovereignty, Digital Expansionism, and the Prospects for Global AI Governance. *SSRN Electron. J.* 2024. Available online: https://ssrn.com/abstract=4483271 (accessed on 9 February 2025).
98. European Committee of the Regions. *AI and GenAI Adoption by Local and Regional Administrations*; European Union: Brussels, Belgium, 2024. Available online: https://interoperable-europe.ec.europa.eu/collection/portal/news/study-ai-and-genai-adoption-local-regional-administrations (accessed on 9 February 2025).
99. French Artificial Intelligence Commission. *AI: Our Ambition for France*; French AI Commission: Paris, France, 2024. Available online: https://gouvernement.fr (accessed on 9 February 2025).
100. UK Government. *Copyright and Artificial Intelligence*; Intellectual Property Office: London, UK, 2024. Available online: https://www.gov.uk/government/consultations/copyright-and-artificial-intelligence (accessed on 9 February 2025).
101. Institute of Development Studies. *Indigenous Knowledge and Artificial Intelligence*; IDS Series; Navigating Data Landscapes: Brighton, UK, 2024. Available online: https://www.ids.ac.uk (accessed on 9 February 2025).
102. Congressional Research Service. *Indigenous Knowledge and Data: Overview and Issues for Congress*; CRS Report No. R48317; CRS: Washington, DC, USA, 2024. Available online: https://crsreports.congress.gov (accessed on 9 February 2025).
103. UK Government. *AI Opportunities Action Plan*; Department for Science, Innovation and Technology: London, UK, 2025. Available online: https://www.gov.uk/official-documents (accessed on 9 February 2025).
104. Centre for Information Policy Leadership (CIPL). *Applying Data Protection Principles to Generative AI: Practical Approaches for Organizations and Regulators*; CIPL: Washington, DC, USA, 2024. Available online: https://www.informationpolicycentre.com (accessed on 9 February 2025).
105. Holgersson, M.; Dahlander, L.; Chesbrough, H.; Bogers, M.L.A.M. Open Innovation in the Age of AI. *Calif. Manag. Rev.* **2024**, *67*, 5–20. [CrossRef]
106. State of California. *State of California Guidelines for Evaluating Impacts of Generative AI on Vulnerable and Marginalized Communities*; Office of Data and Innovation: Sacramento, CA, USA, 2024. Available online: https://www.genai.ca.gov (accessed on 9 February 2025).
107. Bogen, M.; Deshpande, C.; Joshi, R.; Radiya-Dixit, E.; Winecoff, A.; Bankston, K. *Assessing AI: Surveying the Spectrum of Approaches to Understanding and Auditing AI Systems*; Center for Democracy & Technology: Washington, DC, USA, 2025. Available online: https://cdt.org (accessed on 9 February 2025).
108. Current AI (2025). Available online: https://www.currentai.org/ (accessed on 4 February 2025).
109. Mannan, M.; Schneider, N.; Merk, T. Cooperative Online Communities. In *The Routledge Handbook of Cooperative Economics and Management*; Routledge: London, UK, 2024; pp. 411–432. [CrossRef]
110. Durmus, M. *Critical Thinking is Your Superpower: Cultivating Critical Thinking in an AI-Driven World*; Mindful AI Press: Frankfurt, Germany, 2024. Available online: https://mindful-ai.org (accessed on 9 February 2025).
111. Lustenberger, M.; Spychiger, F.; Küng, L.; Cuadra, P. *Mastering DAOs: A Practical Guidebook for Building and Managing Decentralized Autonomous Organizations*; ZHAW Institute for Organizational Viability: Zurich, Switzerland, 2024. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5001424 (accessed on 9 February 2025).
112. Fritsch, R.; Müller, M.; Wattenhofer, R. Analyzing Voting Power in Decentralized Governance: Who Controls DAOs? *arXiv* **2024**, arXiv:2204.01176. Available online: https://arxiv.org/abs/2204.01176 (accessed on 9 February 2025). [CrossRef]
113. EuroHPC Joint Undertaking. *Selection of the First Seven AI Factories to Drive Europe's Leadership in AI*; EuroHPC JU: Luxembourg, 2024. Available online: https://eurohpc-ju.europa.eu/index_en (accessed on 9 February 2025).

114. Marchal, N.; Xu, R.; Elasmar, R.; Gabriel, I.; Goldberg, B.; Isaac, W. Generative AI Misuse: A Taxonomy of Tactics and Insights from Real-World Data. *arXiv* **2024**, arXiv:2406.13843. Available online: https://arxiv.org/abs/2406.13843 (accessed on 9 February 2025).
115. Davenport, T.H.; Gupta, S.; Wang, R. SuperTech Leaders and the Evolution of Technology and Data Leadership; ThoughtWorks, Chicago, IL, USA 2024. Available online: https://www.thoughtworks.com/content/dam/thoughtworks/documents/report/tw_supertech_leaders_and_the_evolution_of_technology_and_data_leadership.pdf (accessed on 9 February 2025).
116. European Securities and Markets Authority (ESMA). *Final Report on the Guidelines on the Conditions and Criteria for the Qualification of Crypto-Assets as Financial Instruments*; ESMA: Paris, France, 2024. Available online: https://www.esma.europa.eu (accessed on 9 February 2025).
117. Shrishak, K. *AI-Complex Algorithms and Effective Data Protection Supervision: Bias Evaluation*; European Data Protection Board (EDPB): Brussels, Belgium, 2024. Available online: https://edpb.europa.eu (accessed on 9 February 2025).
118. Ada Lovelace Institute. *Buying AI: Is the Public Sector Equipped to Procure Technology in the Public Interest?* Ada Lovelace Institute: London, UK, 2024. Available online: https://www.adalovelaceinstitute.org (accessed on 9 February 2025).
119. European Court of Auditors (ECA). *AI Auditors: Auditing AI-Based Projects, Systems, and Processes*; ECA: Luxembourg, 2024. Available online: https://eca.europa.eu (accessed on 9 February 2025).
120. Züger, T.; Asghari, H. Introduction to the special issue on AI systems for the public interest. *Internet Policy Rev.* **2024**, *13*. [CrossRef]
121. Papadimitropoulos, V.; Perperidis, G. On the Foundations of Open Cooperativism. In *The Handbook of Peer Production*; Bauwens, M., Kostakis, V., Pazaitis, A., Eds.; Wiley: Hoboken, NJ, USA, 2021; pp. 398–410. [CrossRef]
122. Tarkowski, A. *Data Governance in Open Source AI: Enabling Responsible and Systemic Access*; Open Future: Warsaw, Poland, 2025. Available online: https://opensource.org/wp-content/uploads/2025/01/2025-OSI-DataGovernanceOSAI.pdf (accessed on 1 February 2025).
123. Gerlich, M. Societal Perceptions and Acceptance of Virtual Humans: Trust and Ethics across Different Contexts. *Soc. Sci.* **2024**, *13*, 516. [CrossRef]
124. Waldner, D.; Lust, E. Unwelcome change: Coming to terms with democratic backsliding. *Annu. Rev. Political Sci.* **2018**, *21*, 93–113. [CrossRef]
125. Roose, K. The Data That Powers A.I. Is Disappearing Fast. 2024. Available online: https://www.nytimes.com/2024/07/19/technology/ai-data-restrictions.html (accessed on 1 September 2024).
126. Kolt, N. Governing AI Agents. *SSRN* **2024**. [CrossRef]
127. Calzada, I. Data (un)sustainability: Navigating utopian resistance while tracing emancipatory datafication strategies. In *Digital (Un)Sustainabilities: Promises, Contradictions, and Pitfalls of the Digitalization-Sustainability Nexus*; Certomá, C., Martelozzo, F., Iapaolo, F., Eds.; Routledge: Oxon, UK, 2024. [CrossRef]
128. Benson, J. *Intelligent Democracy: Answering the New Democratic Scepticism*; Oxford University Press: Oxford, UK, 2024.
129. Coeckelbergh, M. Artificial intelligence, the common good, and the democratic deficit in AI governance. *AI Ethics* **2024**. [CrossRef]
130. García-Marzá, D.; Calvo, P. *Algorithmic Democracy: A Critical Perspective Based on Deliberative Democracy*; Springer Nature: Cham, Switzerland, 2024.
131. KT4Democracy. Available online: https://kt4democracy.eu/ (accessed on 1 January 2024).
132. Levi, S. *Digitalización Democrática: Soberanía Digital para las Personas*; Rayo Verde: Barcelona, Spain, 2024.
133. Poblet, M.; Allen, D.W.E.; Konashevych, O.; Lane, A.M.; Diaz Valdivia, C.A. From Athens to the Blockchain: Oracles for Digital Democracy. *Front. Blockchain* **2020**, *3*, 575662. [CrossRef]
134. De Filippi, P.; Reijers, W.; Morshed, M. *Blockchain Governance*; MIT Press: Boston, MA, USA, 2024.
135. Visvizi, A.; Malik, R.; Guazzo, G.M.; Çekani, V. The Industry 5.0 (I50) Paradigm, Blockchain-Based Applications and the Smart City. *Eur. J. Innov. Manag.* **2024**, *28*, 5–26. [CrossRef]
136. Roio, D.; Selvaggini, R.; Bellini, G.; Dintino, A. SD-BLS: Privacy preserving selective disclosure of verifiable credentials with unlinkable threshold revocation. In Proceedings of the 2024 IEEE International Conference on Blockchain (Blockchain), Copenhagen, Denmark, 19–22 August 2024; pp. 505–511. [CrossRef]
137. Viano, C.; Avanzo, S.; Boella, G.; Schifanella, C.; Giorgino, V. Civic blockchain: Making blockchains accessible for social collaborative economies. *J. Responsible Technol.* **2023**, *15*, 100066. [CrossRef]
138. Ahmed, S.; Jaźwińska, K.; Ahlawat, A.; Winecoff, A.; Wang, M. Field-building and the epistemic culture of AI safety. *First Monday* **2024**. [CrossRef]
139. Tan, J.; Merk, T.; Hubbard, S.; Oak, E.R.; Rong, H.; Pirovich, J.; Rennie, E.; Hoefer, R.; Zargham, M.; Potts, J.; et al. Open Problems in DAOs. *arXiv* **2023**, arXiv:2310.1920. Available online: https://arxiv.org/abs/2310.19201v2 (accessed on 1 February 2025).
140. Petreski, D.; Cheong, M. Data Cooperatives: A Conceptual Review. ICIS 2024 Proceedings. 15. 2024. Available online: https://aisel.aisnet.org/icis2024/lit_review/lit_review/15 (accessed on 1 February 2025).
141. Stein, J.; Fung, M.L.; Weyenbergh, G.V.; Soccorso, A. Data cooperatives: A framework for collective data governance and digital justice', People-Centered Internet. 2023. Available online: https://peoplecentered.net/wp-content/uploads/2024/09/Data-Cooperatives-Report-.pdf (accessed on 1 September 2024).

142. Dathathri, S.; See, A.; Ghaisas, S.; Huang, P.-S.; McAdam, R.; Welbl, J.; Bachani, V.; Kaskasoli, A.; Stanforth, R.; Matejovicova, T.; et al. Scalable watermarking for identifying large model outputs. *Nature* **2024**, *634*, 818–823. [CrossRef]
143. Adler, S.; Hitzig, Z.; Jain, S.; Brewer, C.; Chang, W.; DiResta, R.; Lazzarin, E.; McGregor, S.; Seltzer, W.; Siddarth, D.; et al. Personhood credentials: Artificial intelligence and the value of privacy-preserving tools to distinguish who is real online. *arXiv* **2024**, arXiv:2408.07892. Available online: https://arxiv.org/abs/2408.07892 (accessed on 1 September 2024).
144. Fratini, Samuele and Hine, Emmie and Novelli, Claudio and Roberts, Huw and Floridi, Luciano, Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models. Available online: https://ssrn.com/abstract=4816020 (accessed on 21 April 2024).
145. Hui, Y. Machine and Sovereignty for a Planetary Thinking. University of Minnesota Press: Minneapolis, MN, USA; London, UK, 2024.
146. New America. From Digital Sovereignty to Digital Agency; New America Foundation, NYC, USA 2023. Available online: https://www.newamerica.org/planetary-politics/briefs/from-digital-sovereignty-to-digital-agency/ (accessed on 20 November 2024).
147. Glasze, G.; Cattaruzza, A.; Douzet, F.; Dammann, F.; Bertran, M.-G.; Bômont, C.; Braun, M.; Danet, D.; Desforges, A.; Géry, A.; et al. Contested Spatialities of Digital Sovereignty. *Geopolitics* **2023**, *28*, 919–958. [CrossRef]
148. The Conversation. Elon Musk's Feud with Brazilian Judge is Much More Than a Personal Spat—It's About National Sovereignty, Freedom of Speech, and The Rule of Law. 2023. Available online: https://theconversation.com/elon-musks-feud-with-brazilian-judge-is-much-more-than-a-personal-spat-its-about-national-sovereignty-freedom-of-speech-and-the-rule-of-law-238264 (accessed on 20 September 2024).
149. The Conversation. Albanese Promises to Legislate Minimum Age for Kids' Access to Social Media. 2023. Available online: https://theconversation.com/albanese-promises-to-legislate-minimum-age-for-kids-access-to-social-media-238586 (accessed on 20 September 2024).
150. Calzada, I. Data Co-operatives through Data Sovereignty. *Smart Cities* **2021**, *4*, 1158–1172. [CrossRef]
151. Belanche, D.; Belk, R.W.; Casaló, L.V.; Flavián, C. The dark side of artificial intelligence in services. *Serv. Ind. J.* **2024**, *44*, 149–172. [CrossRef]
152. European Parliament. EU AI Act: First Regulation on Artificial Intelligence. 2023. Available online: https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence (accessed on 23 November 2024).
153. Bambauer, J.R.; Zarsky, T. Fair-Enough AI (August 08, 2024). Forthcoming in the Yale Journal of Law & Technology. Available online: https://ssrn.com/abstract=4924588 (accessed on 1 February 2025).
154. Dennis, C. What Should Be Internationalised in AI Governance? *Oxford Martin AI Gov. Initiat.* **2024**.
155. Ghioni, R.; Taddeo, M.; Floridi, L. Open Source Intelligence and AI: A Systematic Review of the GELSI Literature. *SSRN*. Available online: https://ssrn.com/abstract=4272245 (accessed on 18 November 2024).
156. Bullock, S.; Ajmeri, N.; Batty, M.; Black, M.; Cartlidge, J.; Challen, R.; Chen, C.; Chen, J.; Condell, J.; Danon, L.; et al. Artificial Intelligence for Collective Intelligence: A National-Scale Research Strategy. 2024. Available online: https://ai4ci.ac.uk (accessed on 20 November 2024).
157. Alon, I.; Haidar, H.; Haidar, A.; Guimón, J. The future of artificial intelligence: Insights from recent Delphi studies. *Futures* **2024**, *165*, 103514. [CrossRef]
158. Harris, D.E.; Shull, A. Generative AI, Democracy and Human Rights. Centre for International Governance Innovation. Available online: https://www.cigionline.org/static/documents/FoT_PB_No._12_-_Harris_and_Shull_gzjUYYD.pdf (accessed on 1 February 2025).
159. Narayanan, A. Understanding Social Media Recommendation Algorithms. *Kn. First Amend. Inst.* **2023**, *9*, 1–49.
160. Settle, J.E. *Frenemies: How Social Media Polarizes America*; Cambridge University Press: Cambridge, UK, 2018.
161. European Commission; Joint Research Centre; Lähteenoja, V.; Himanen, J.; Turpeinen, M.; Signorelli, S. *The Landscape of Consent Management Tools—A Data Altruism Perspective*; Publications Office of the European Union: Luxembourg, 2024. [CrossRef]
162. Fink, A. Data cooperative. *Internet Policy Rev.* **2024**, *13*, 1–12. [CrossRef]
163. Nabben, K. AI as a Constituted System: Accountability Lessons from an LLM Experiment. *Data Policy* **2024**, *6*, e57. [CrossRef]
164. Von Thun, M.; Hanley, D.A. *Stopping Big Tech from Becoming Big AI*; Open Markets Institute and Mozilla: Washington, DC, USA; Mountain View, CA, USA, 2024.
165. Rajamohan, R. Networked Cooperative Ecosystems. 2024. Available online: https://paragraph.xyz/@v6a/networked-ecosystems-2 (accessed on 1 February 2025).
166. Ananthaswamy, A. *Why Machines Learn: The Elegant Math Behind Modern AI*; Penguin: London, UK, 2024.
167. Bengio, Y. AI and catastrophic risk. *J. Democr.* **2023**, *34*, 111–121. [CrossRef]
168. European Parliament. *Social Approach to the Transition to Smart Cities*; European Parliament: Luxembourg, 2023.
169. Magro, A. *Emerging Digital Technologies in the Public Sector: The Case of Virtual Worlds*; Publications Office of the European Union: Luxembourg, 2024.

170. Estévez Almenzar, M.; Fernández Llorca, D.; Gómez, E.; Martínez Plumed, F. *Glossary of Human-Centric Artificial Intelligence*; Publications Office of the European Union: Luxembourg, 2022. [CrossRef]
171. Varon, J.; Costanza-Chock, S.; Tamari, M.; Taye, B.; Koetz, V. *AI Commons: Nourishing Alternatives to Big Tech Monoculture*; Coding Rights: Rio de Janeiro, Brazil, 2024. Available online: https://codingrights.org/docs/AICommons.pdf (accessed on 9 February 2025).
172. Verhulst, S.G. Toward a Polycentric or Distributed Approach to Artificial Intelligence & Science. *Front. Policy Labs.* **2024**, *1*, 1–10. [CrossRef]
173. Mitchell, M.; Palmarini, A.B.; Moskvichev, A. Comparing Humans, GPT-4, and GPT-4V on abstraction and reasoning tasks. *arXiv* **2023**, arXiv:2311.09247.
174. Gasser, U.; Mayer-Schönberger, V. *Guardrails: Guiding Human Decisions in the Age of AI*; Princeton University Press: Princeton, NJ, USA, 2024.
175. United Nations High-level Advisory Body on Artificial Intelligence. *Governing AI for Humanity: Final Report*; United Nations: New York, NY, USA, 2024.
176. Vallor, S. *The AI Mirror: How to Reclaim Our Humanity in an Age of Machine Thinking*; OUP: New York, NY, USA, 2024.
177. Buolamwini, J. *Unmasking AI: My Mission to Protect What is Human in a World of Machines*; Random House: London, UK, 2023.
178. McCourt, F.H. *Our Biggest Fight: Reclaiming Liberty, Humanity, and Dignity in the Digital Age*; Crown Publishing: London, UK, 2024.
179. Muldoon, J.; Graham, M.; Cant, C. *Feeding the Machine: The Hidden Human Labour Powering AI*; Cannongate: Edinburgh, UK, 2024.
180. Burkhardt, S.; Rieder, B. Foundation models are platform models: Prompting and the political economy of AI. *Big Data Soc.* **2024**, *11*, 20539517241247839. [CrossRef]
181. Finnemore, M.; Sikkink, K. International Norm Dynamics and Political Change. *Int. Organ.* **1998**, *52*, 887–917. [CrossRef]
182. Lazar, S. *Connected by Code: Algorithmic Intermediaries and Political Philosophy*; Oxford University Press: Oxford, UK, 2024.
183. Hoeyer, K. *Data Paradoxes: The Politics of Intensified Data Sourcing in Contemporary Healthcare*; MIT Press: Cambridge, MA, USA, 2023.
184. Hughes, T. The political theory of techno-colonialism. *Eur. J. Political Theory* **2024**. [CrossRef]
185. Srivastava, S. *Algorithmic Governance and the International Politics of Big Tech*; Cambridge University Press: Cambridge, MA, USA, 2021.
186. Utrata, A. Engineering territory: Space and colonies in Silicon Valley. *Am. Political Sci. Rev.* **2024**, *118*, 1097–1109. [CrossRef]
187. Lehdonvirta, V.; Wú, B.; Hawkins, Z. *Weaponized Interdependence in a Bipolar World: How Economic Forces and Security Interests Shape the Global Reach of U.S. and Chinese Cloud Data Centres*; Oxford Internet Institute, University of Oxford & Aalto University: Oxford, UK, 2025; Accepted to *Review of International Political Economy*.
188. Guersenzvaig, A.; Sánchez-Monedero, J. AI research assistants, intrinsic values, and the science we want. *AI Soc.* **2024**. [CrossRef]
189. Wachter-Boettcher, S. *Technically Wrong: Sexist Apps, Biased Algorithms, and Other Threat of Toxic Tech*; WW Norton & Co: London, UK, 2018.
190. D'Amato, K. ChatGPT: Towards AI subjectivity. *AI Soc.* **2024**. [CrossRef]
191. Shavit, Y.; Agarwal, S.; Brundage, M.; Adler, S.; O'Keefe, C.; Campbell, R.; Lee, T.; Mishkin, P.; Eloundou, T.; Hickey, A.; et al. *Practices for Governing Agentic AI Systems*; OpenAI: San Francisco, CA, USA, 2023.
192. Bibri, S.E.; Allam, Z. The Metaverse as a Virtual Form of Data-Driven Smart Urbanism: On Post-Pandemic Governance through the Prism of the Logic of Surveillance Capitalism. *Smart Cities* **2022**, *5*, 715–727. [CrossRef]
193. Bibri, S.E.; Visvizi, A.; Troisi, O. *Advancing Smart Cities: Sustainable Practices, Digital Transformation, and IoT Innovations*; Springer: Cham, Switzerland, 2024. [CrossRef]
194. Sharifi, A.; Allam, Z.; Bibri, S.E.; Khavarian-Garmsir, A.R. Smart cities and sustainable development goals (SDGs): A systematic literature review of co-benefits and trade-offs. *Cities* **2024**, *146*, 104659. [CrossRef]
195. Singh, A. Advances in Smart Cities: Smarter People, Governance, and Solutions. *J. Urban Technol.* **2019**, *26*, 1–4. [CrossRef]
196. Reuel, A.; Bucknall, B.; Casper, S.; Fist, T.; Soder, L.; Aarne, O.; Hammond, L.; Ibrahim, L.; Chan, A.; Wills, P.; et al. Open Problems in Technical AI Governance. *arXiv* **2024**, arXiv:2407.14981. Available online: https://arxiv.org/abs/2407.14981 (accessed on 1 February 2025).
197. Aho, B. Data communism: Constructing a national data ecosystem. *Big Data Soc.* **2024**, *11*, 20539517241275888. [CrossRef]
198. Valmeekam, K.; Sreedharan, S.; Marquez, M.; Olmo, A.; Kambhampati, S. On the Planning Abilities of Large Language Models—A Critical Investigation. *arXiv* **2023**, arXiv:2305.15771. Available online: https://arxiv.org/abs/2305.15771 (accessed on 1 February 2025).
199. Yao, S.; Zhao, J.; Yu, D.; Du, N.; Shafran, I.; Narasimhan, K.; Cao, Y. ReAct: Synergizing reasoning and acting in language models. *arXiv* **2022**, arXiv:2210.03629. Available online: https://arxiv.org/abs/2210.03629 (accessed on 1 February 2025).
200. Krause, D. Web3 and the Decentralized Future: Exploring Data Ownership, Privacy, and Blockchain Infrastructure. *Preprint* **2024**. [CrossRef]
201. Lazar, S.; Pascal, A. *AGI and Democracy*; Allen Lab for Democracy Renovation: Cambridge, MA, USA, 2024.

202. Ovadya, A. Reimagining Democracy for AI. *J. Democr.* **2023**, *34*, 162–170. [CrossRef]
203. Ovadya, A.; Thorburn, L.; Redman, K.; Devine, F.; Milli, S.; Revel, M.; Konya, A.; Kasirzadeh, A. Toward Democracy Levels for AI. Pluralistic Alignment Workshop at NeurIPS 2024. Available online: https://arxiv.org/abs/2411.09222 (accessed on 14 November 2024).
204. Alnabhan, M.Q.; Branco, P. BERTGuard: Two-Tiered Multi- Domain Fake News Detection with Class Imbalance Mitigation. *Big Data Cogn. Comput.* **2024**, *8*, 93. [CrossRef]
205. Gourlet, P.; Ricci, D.; Crépel, M. Reclaiming artificial intelligence accounts: A plea for a participatory turn in artificial intelligence inquiries. *Big Data Soc.* **2024**, *11*, 20539517241248093. [CrossRef]
206. Spathoulas, G.; Katsika, A.; Kavallieratos, G. Privacy Preserving and Verifiable Outsourcing of AI Processing for Cyber-Physical Systems. In *International Conference on Information and Communications Security*; Springer: Singapore, 2024.
207. Abhishek, T.; Varda, M. Data Hegemony: The Invisible War for Digital Empires. *Internet Policy Rev.* **2024**. Available online: https://policyreview.info/articles/news/data-hegemony-digital-empires/1789 (accessed on 1 September 2024).
208. Alaimo, C.; Kallinikos, J. *Data Rules: Reinventing the Market Economy*; MIT Press: Cambridge, MA, USA, 2024.
209. OpenAI. *GPT-4 Technical Report*; OpenAI: San Francisco, CA, USA, 2023.
210. Dobbe, R. System safety and artificial intelligence. In Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency, Seoul, Republic of Korea, 21–22 June 2022.
211. Bengio, Y.; Mindermann, S.; Privitera, D.; Besiroglu, T.; Bommasani, R.; Casper, S.; Choi, Y.; Goldfarb, D.; Heidari, H.; Khalatbari, L.; et al. International Scientific Report on the Safety of Advanced AI: Interim Report. *arXiv* **2024**, arXiv:2412.05282.
212. World Digital Technology Academy (WDTA). *Large Language Model Security Requirements for Supply Chain*; WDTA AI-STR-03; World Digital Technology Academy: Geneva, Switzerland, 2024.
213. AI4GOV. Available online: https://ai4gov-project.eu/2023/11/14/ai4gov-d3-1/ (accessed on 1 January 2024).
214. Cazzaniga, M.; Jaumotte, F.; Li, L.; Melina, G.; Panton, A.J.; Pizzinelli, C.; Rockall, E.; Tavares, M.M. *Gen-AI: Artificial Intelligence and the Future of Work*; IMF Staff Discussion Note SDN2024/001; International Monetary Fund: Washington, DC, USA, 2024.
215. ENFIELD. 2024. Available online: https://www.enfield-project.eu/about (accessed on 1 September 2024).
216. Palacios, S.; Ault, A.; Krogmeier, J.V.; Bhargava, B.; Brinton, C.G. AGAPECert: An Auditable, Generalized, Automated, Privacy-Enabling Certification Framework with Oblivious Smart Contracts. *IEEE Trans. Dependable Secur. Comput.* **2022**, *20*, 3269–3286. [CrossRef]
217. GPAI Algorithmic Transparency in the Public Sector. *A State-of-the-Art Report of Algorithmic Transparency Instruments*; Global Partnership on Artificial Intelligence; OECD: Paris, France, 2024. Available online: www.gpai.ai (accessed on 1 September 2024).
218. Lazar, S.; Nelson, A. AI safety on whose terms? *Science* **2023**, *381*, 138. [CrossRef]
219. HAI. *Artificial Intelligence Index Report 2024*; HAI: Palo Alto, CA, USA, 2024.
220. Nagy, P.; Neff, G. Conjuring algorithms: Understanding the tech industry as stage magicians. *New Media Soc.* **2024**, *26*, 4938–4954. [CrossRef]
221. Kim, E.; Jang, G.Y.; Kim, S.H. How to apply artificial intelligence for social innovations. *Appl. Artif. Intell.* **2022**, *36*, 2031819. [CrossRef]
222. Calzada, I.; Cobo, C. Unplugging: Deconstructing the Smart City. *J. Urban Technol.* **2015**, *22*, 23–43. [CrossRef]
223. Visvizi, A.; Godlewska-Majkowska, H. Not Only Technology: From Smart City 1.0 through Smart City 4.0 and Beyond (An Introduction). In *Smart Cities: Lock-In, Path-dependence and Non-linearity of Digitalization and Smartification*; Visvizi, A., Godlewska-Majkowska, H., Eds.; Routledge: London, UK, 2025; pp. 3–16. Available online: https://www.taylorfrancis.com/chapters/edit/10.1201/9781003415930-2/technology-anna-visvizi-hanna-godlewska-majkowska (accessed on 1 February 2025).
224. Troisi, O.; Visvizi, A.; Grimaldi, M. The Different Shades of Innovation Emergence in Smart Service Systems: The Case of Italian Cluster for Aerospace Technology. *J. Bus. Ind. Mark.* **2024**, *39*, 1105–1129. [CrossRef]
225. Visvizi, A.; Troisi, O.; Corvello, V. *Research and Innovation Forum 2023: Navigating Shocks and Crises in Uncertain Times—Technology, Business, Society*; Springer Nature: Cham, Switzerland, 2024. [CrossRef]
226. Caprotti, F.; Cugurullo, F.; Cook, M.; Karvonen, A.; Marvin, S.; McGuirk, P.; Valdez, A.M. Why does urban Artificial Intelligence (AI) matter for urban studies? Developing research directions in urban AI research. *Urban Geogr.* **2024**, *45*, 883–894. [CrossRef]
227. Caprotti, F.; Duarte, C.; Joss, S. The 15-minute city as paranoid urbanism: Ten critical reflections. *Cities* **2024**, *155*, 105497. [CrossRef]
228. Cugurullo, F.; Caprotti, F.; Cook, M.; Karvonen, A.; McGuirk, P.; Marvin, S. The rise of AI urbanism in post-smart cities: A critical commentary on urban artificial intelligence. *Urban Stud.* **2024**, *61*, 1168–1182. [CrossRef]
229. Sanchez, T.W.; Fu, X.; Yigitcanlar, T.; Ye, X. The Research Landscape of AI in Urban Planning: A Topic Analysis of the Literature with ChatGPT. *Urban Sci.* **2024**, *8*, 197. [CrossRef]
230. Kuppler, A.; Fricke, C. Between innovative ambitions and erratic everyday practices: Urban planners' ambivalences towards digital transformation. *Town Plan. Rev.* **2024**, *96*, 2. [CrossRef]
231. Eubanks, V. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*; Picador: London, UK, 2019.

232. Lorinc, J. *Dream States: Smart Cities, Technology, and the Pursuit of Urban Utopias*; Coach House Books: Toronto, Canada, 2022.
233. Leffel, B.; Derudder, B.; Acuto, M.; van der Heijden, J. Not so polycentric: The stratified structure & national drivers of transnational municipal networks. *Cities* **2023**, *143*, 104597. [CrossRef]
234. Luccioni, S.; Jernite, Y.; Strubell, E. Power hungry processing: Watts driving the cost of AI deployment? In Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency, Rio de Janeiro, Brazil, 3–6 June 2024.
235. Gohdes, A.R. *Repression in the Digital Age: Surveillance, Censorship, and the Dynamics of State Violence*; Oxford University Press: Oxford, UK, 2023.
236. Seger, E.; Avin, S.; Pearson, G.; Briers, M.; Heigeartaigh S, Ó.; Bacon, H.; Ajder, H.; Alderson, C.; Anderson, F.; Baddeley, J.; et al. *Tackling Threats to Informed Decision-Making in Democratic Societies: Promoting Epistemic Security in a Technologically-Advanced World*; The Alan Turing Institute: London, UK, 2020.
237. Burton, J.W.; Lopez-Lopez, E.; Hechtlinger, S.; Rahwan, Z.; Aeschbach, S.; Bakker, M.A.; Becker, J.A.; Berditchevskaia, A.; Berger, J.; Brinkmann, L.; et al. How large language models can reshape collective intelligence. *Nat. Hum. Behav.* **2024**, *8*, 1643–1655. [CrossRef]
238. Lalka, R. *The Venture Alchemists: How Big Tech Turned Profits into Power*; Columbia University Press: New York, NY, USA, 2024.
239. Li, F.-F. *The Worlds I See: Curiosity, Exploration, and Discovery and the Dawn of AI*; Macmillan: London, UK, 2023.
240. Medrado, A.; Verdegem, P. Participatory action research in critical data studies: Interrogating AI from a South–North approach. *Big Data Soc.* **2024**, *11*, 20539517241235869. [CrossRef]
241. Mejias, U.A.; Couldry, N. *Data Grab: The New Colonialism of Big Tech (and How to Fight Back)*; WH Allen: London, UK, 2024.
242. Murgia, M. *Code Dependent: Living in the Shadow of AI*; Henry Holt and Co.: London, UK, 2024.
243. Johnson, S.; Acemoglu, D. *Power and Progress: Our Thousand-Year Struggle Over Technology and Prosperity*; Basic Books: London, UK, 2023.
244. Rella, L.; Hansen, K.B.; Thylstrup, N.B.; Campbell-Verduyn, M.; Preda, A.; Rodima-Taylor, D.; Xu, R.; Straube, T. Hybrid materialities, power, and expertise in the era of general purpose technologies. *Distinktion J. Soc. Theory* **2024**. [CrossRef]
245. Merchant, B. *Blood in the Machine: The Origins of the Rebellion Against Big Tech*; Little, Brown and Company: London, UK, 2023.
246. Sieber, R.; Brandusescu, A.; Adu-Daako, A.; Sangiambut, S. Who are the publics engaging in AI? *Public Underst. Sci.* **2024**, *33*, 634–653. [CrossRef]
247. Tunç, A. Can AI determine its own future? *AI Society* **2024**. [CrossRef]
248. Floridi, L. Why the AI Hype is Another Tech Bubble. Available online: https://ssrn.com/abstract=4960826 (accessed on 18 September 2024).
249. Batty, M. *The New Science of Cities*; MIT Press: Cambridge, MA, USA, 2013.
250. Batty, M. *Inventing Future Cities*; MIT Press: Cambridge, MA, USA, 2018.
251. Batty, M. Urban Analytics Defined. *Environ. Plan. B Urban Anal. City Sci.* **2019**, *46*, 403–405. [CrossRef]
252. Marvin, S.; Luque-Ayala, A.; McFarlane, C. Smart Urbanism: Utopian Vision or False Dawn? Routledge: New York, NY, USA, 2016.
253. Marvin, S.; Graham, S. *Splintering Urbanism: Networked Infrastructures, Technological Mobilities, and the Urban Condition*; Routledge: London, UK, 2001.
254. Marvin, S.; Bulkeley, H.; Mai, L.; McCormick, K.; Palgan, Y.V. Urban Living Labs: Experimenting with City Futures. *Eur. Urban Reg. Stud.* **2018**, *25*, 317–333. [CrossRef]
255. Kitchin, R. *Code/Space: Software and Everyday Life*; MIT Press: Cambridge, MA, USA, 2011.
256. Kitchin, R.; Lauriault, T.P.; McArdle, G. Knowing and Governing Cities through Urban Indicators, City Benchmarking, and Real-Time Dashboards. *Reg. Stud. Reg. Sci.* **2015**, *2*, 6–28. [CrossRef]
257. Calzada, I. Platform and data co-operatives amidst European pandemic citizenship. *Sustainability* **2020**, *12*, 8309. [CrossRef]
258. Monsees, L. *Crypto-Politics: Encryption and Democratic Practices in the Digital Era*; Routledge: Oxon, UK, 2020.
259. European Commission. *Second Draft of the General Purpose AI Code of Practice*; Digital Strategy; European Commission: Brussels, Belgium, 2024. Available online: https://digital-strategy.ec.europa.eu/en/library/second-draft-general-purpose-ai-code-practice-published-written-independent-experts (accessed on 10 February 2025).
260. Visvizi, A.; Kozlowski, K.; Calzada, I.; Troisi, O. *Multidisciplinary Movements in AI and Generative AI: Society, Business, Education*; Edward Elgar: Chentelham, UK, 2025.
261. Leslie, D.; Burr, C.; Aitken, M.; Cowls, J.; Katell, M.; Briggs, M. *Artificial Intelligence, Human Rights, Democracy, and the Rule of Law: A Primer*; Council of Europe: Strasbourg, France, 2021. Available online: https://edoc.coe.int/en/artificial-intelligence/10206-artificial-intelligence-human-rights-democracy-and-the-rule-of-law-a-primer.html (accessed on 1 February 2025).
262. Hossain, S.T.; Yigitcanlar, T. Local Governments Are Using AI without Clear Rules or Policies, and the Public Has No Idea. QUT Newsroom. Available online: https://www.qut.edu.au/news/realfocus/local-governments-are-using-ai-without-clear-rules-or-policies-and-the-public-has-no-idea (accessed on 9 January 2025).

263. Gerlich, M. AI Tools in Society: Impacts on Cognitive Offloading and the Future of Critical Thinking. *Societies* **2025**, *15*, 6. [CrossRef]
264. Bousetouane, F. Agentic Systems: A Guide to Transforming Industries with Vertical AI Agents. *arXiv* **2025**, arXiv:2501.00881. Available online: https://arxiv.org/abs/2501.00881 (accessed on 9 January 2025).
265. Calzada, I. Generative AI and the Urban AI Policy Challenges Ahead: Trustworthy AI for Whom? Available online: https://www.emeraldgrouppublishing.com/calls-for-papers/generative-ai-and-urban-ai-policy-challenges-ahead-trustworthy-ai-whomn (accessed on 1 February 2025).
266. Hossain, S.T.; Yigitcanlar, T.; Nguyen, K.; Xu, Y. Cybersecurity in Local Governments: A Systematic Review and Framework of Key Challenges. *Urban Gov.* **2025**. [CrossRef]
267. Laksito, J.; Pratiwi, B.; Ariani, W. Harmonizing Data Privacy Frameworks in Artificial Intelligence: Comparative Insights from Asia and Europe. *PERKARA—J. Ilmu Huk. Dan Polit.* **2024**, *2*, 579–588. [CrossRef]
268. Nature. Science for Policy: Why Scientists and Politicians Struggle to Collaborate. *Nature* **2024**. Available online: https://www.nature.com/articles/d41586-024-03910-4 (accessed on 9 January 2025).