Legislating into the future: soil law, AI, and digitalisation

Ruda Murray & Oliver C. Ruppel

"It is customary to offer a grain of comfort, in the form of a statement that some peculiarly human characteristic could never be imitated by a machine. I cannot offer any such comfort, for I believe that no such bounds can be set." —Alan Turing, 1951

1. Introduction

Artificial intelligence (AI) has been called "the new electricity."[1] In less than a decade, technologies once confined to science fiction (e.g., robots, algorithms, and adaptive digital companions) have become part of everyday life. In 2023 alone, the United States (US) Food and Drug Administration approved 223 AI-powered medical devices, compared to only six in 2015.[2] Autonomous vehicles are no longer experimental: Waymo now delivers more than 150,000 self-driving rides weekly in the US, while Baidu's Apollo Go robotaxis operate across multiple Chinese cities.[3] In 2024, nearly 80% of businesses worldwide reported using AI tools.[4] In December 2024, an AI system known as "The Fourth Judge" was employed to score a world championship boxing match in Riyadh, Saudi Arabia.[5] In 2025, Albania made history by appointing Diella, the world's first AI-powered virtual minister, to oversee public procurement.[6] In August 2025, Malaysia launched the world's first AI-powered bank (Ryt Bank), led by YTL Group and Sea Limited.[7] What seemed futuristic has become an integral part of how societies function, communicate, and govern.

The scale of investment underscores this shift. Between 2013 and 2024, the US attracted nearly USD 500 billion in private AI funding,[8] followed by China (USD 119 billion), the United Kingdom (UK) (USD 28 billion), and Canada and Israel (around USD 15 billion each).[9] In 2024, US institutions produced 40 major AI models, while

1 See https://www.gsb.stanford.edu/insights/andrew-ng-why-ai-new-electricity, accessed 29 September 2025.
2 Stanford University (2025: 3).
3 Ibid.
4 Ibid.
5 See www.forbes.com/sites/brianmazique/2024/12/21/oleksandr-usyk-vs-tyson-fury-2-results-winner-scorecards-reaction, accessed 27 October 2025.
6 See https://www.politico.eu/article/albania-apppoints-worlds-first-virtual-minister-edi-rama-diella/, accessed 27 October 2025.
7 See https://www.artificialintelligence-news.com/news/malaysia-launches-ryt-bank-its-first-ai-powered-bank/, accessed 30 October 2025.
8 See https://www.visualcapitalist.com/visualizing-global-ai-investment-by-country/#google_vignette, accessed 29 September 2025.
9 Ibid.

China created 15 and Europe produced just 3.[10] Global trade in goods that enable AI reached approximately USD 2.3 trillion in 2023.[11] These figures reflect not only economic ambition but also a geopolitical race to shape the digital rules of the future. This race increasingly forces countries into binary choices between US and Chinese technologies, raising profound questions of sovereignty, autonomy, and security.

AI is also entering the realm of governance, including environmental governance. It offers opportunities to improve transparency, anticipate ecological risks, and strengthen enforcement. Yet it also raises pressing questions: Who controls the data on which AI depends? How are algorithmic decisions made, and who is accountable when they cause harm? Can digital governance frameworks genuinely promote soil protection and environmental justice, or do they risk entrenching existing inequalities under the guise of innovation?

Environmental governance often struggles with fragmented national laws and policies—especially in understudied sectors where coherence is crucial but poorly theorised. Legal materials are scattered across languages, jurisdictions, and political contexts, making systematic cross-country comparison difficult. Recent advances in behavioural and cognitive-scale AI provide a glimpse of what governance assistance might look like. For instance, "Centaur," a model fine-tuned on the large-scale Psych-101 dataset (covering millions of human decisions across hundreds of experiments), can predict and simulate human behaviour in any scenario expressible in natural language.[12] Its ability to generalise across unseen tasks and align with human neural patterns suggests how similar systems could eventually help policymakers model institutional performance, anticipate stakeholder responses, and test regulatory outcomes before implementation. Such cognitive-level modelling, when applied ethically, could transform governance from a reactive to an anticipatory approach.

AI can thus help close existing governance gaps by parsing multilingual legal corpora, mapping duties and institutions, and flagging inconsistencies or omissions—providing an evaluative lens on governance frameworks within a chosen environmental domain and a baseline for evidence-based reform.

This chapter explores the convergence of soil governance, AI, and digitalisation. Soils underpin food security, biodiversity, and climate regulation, yet they remain largely invisible in legal frameworks. At the same time, digital technologies are transforming how societies collect, manage, and regulate soil data. From AI-powered soil monitoring to blockchain-enabled land tenure, these tools hold potential to reshape environmental law. They can support predictive regulation, strengthen compliance, and make governance more adaptive. But they also carry risks of data colonialism, algorithmic opacity, and digital exclusion, particularly for smallholder farmers and indigenous communities.

10 Stanford University (2025: 3).
11 WTO (2025: 21).
12 Binz et al. (2024).

Against this backdrop, this chapter asks: How should soil law be redesigned to integrate AI and digitalisation to advance sustainable soil management (SSM)—by safeguarding data sovereignty, transparency, accountability, and equity—rather than reproducing digital colonisation and environmental harm? To answer this, the chapter proceeds in four steps. First, it traces the origins of AI and big data and their evolving applications, clarifying the "moving target" for regulators. Second, it examines SSM's governance mechanisms and shows how digital tools can both strengthen and undermine them (including energy/water footprints, bias, and exclusion). Third, it analyses legal and policy approaches at national, regional, and international levels and assesses their relevance to soils. Finally, it interrogates digital colonisation, focusing on soil data sovereignty in Africa (including a South African case study), and briefly surveys broader AI developments shaping this terrain. It proposes pathways—such as data commons, method transparency and guardrails, standardised soil-health indices, and rights to audit and contestation—for inclusive, transparent, and ecocentric legal frameworks.

Ultimately, this chapter argues that soil law must evolve in tandem with digitalisation. Only by integrating soil health, digital rights, and the ethical use of AI into future legislation can societies ensure that soils, often overlooked as expendable resources, are recognised as central to planetary sustainability in the digital age.

2. Understanding AI: origins, forms, and evolving applications

AI only truly entered public debate in November 2022, when ChatGPT abruptly pushed the concept into everyday consciousness. Yet the idea of creating machines capable of independent action is far older.[13] Greek philosophers speculated about artificial life more than two millennia ago,[14] while Archytas of Tarentum reportedly built a mechanical dove around 400 BCE.[15] Leonardo da Vinci designed a humanoid automaton in 1495.[16] The fascination with self-operating machines is thus deeply rooted in human imagination.

AI's formal history as a scientific field began in 1956 with the Dartmouth Summer Research Project on Artificial Intelligence. John McCarthy and colleagues proposed that every aspect of learning and intelligence could, in principle, be described precisely enough for a machine to simulate it.[17] Since then, AI has evolved into an umbrella concept encompassing a spectrum of systems capable of performing tasks traditionally

13 Singh (2020).
14 Bedini (1964).
15 Chondros (2017).
16 Moran (2006).
17 See https://home.dartmouth.edu/about/artificial-intelligence-ai-coined-dartmouth, accessed 29 September 2025.

associated with human intelligence, including learning, reasoning, problem-solving, language use, and decision-making.

2.1. Forms of AI

Britannica defines AI as "the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings."[18] The United Nations Educational, Scientific, and Cultural Organisation (UNESCO) explains that, "[b]uilt from data, hardware and connectivity, AI allows machines to mimic human intelligence such as perception, problem-solving, linguistic interaction or creativity."[19] According to the European Commission:

> Artificial intelligence (AI) refers to systems designed by humans that, given a complex goal, act in the physical or digital world by perceiving their environment, interpreting the collected structured or unstructured data, reasoning on the knowledge derived from this data and deciding the best action(s) to take (according to pre-defined parameters) to achieve the given goal. AI systems can also be designed to learn to adapt their behaviour by analysing how the environment is affected by their previous actions. As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems).[20]

At its core, AI is not a single technology but a continuum that ranges from narrow or "weak" AI (Artificial Narrow Intelligence, ANI)—systems designed for specific tasks, such as voice assistants, facial recognition, and recommendation engines, which are fast and efficient but lack a general understanding[21]—to the still-theoretical realm of Artificial General Intelligence (AGI), which would replicate human-like adaptability across many domains.[22] Within this spectrum sits generative AI, capable of creating original text, images, audio, or code by learning from large datasets (e.g., ChatGPT, DALL·E, Codex).[23] Much of modern AI is driven by Machine Learning (ML), a subset in which models learn from data and improve performance without explicit programming, encompassing branches such as deep learning, natural language processing, computer vision, and reinforcement learning.[24] Underpinning all of this is Big Data—the high-volume, high-velocity, and high-variety information streams that fuel training

18 See https://www.britannica.com/technology/artificial-intelligence, accessed 29 September 2025.
19 See https://www.unesco.org/en/artificial-intelligence, accessed 29 September 2025.
20 European Commission (2018: 7).
21 For example, Google's DeepMind, Facebook's facial recognition technology, Apple's 'Siri', Amazon's Alexa, and Tesla's and Uber's self-driving vehicles. McLean et al. (2023); Flowers (2019).
22 McLean et al. (2023).
23 Jackson et al. (2024); Zhang et al. (2025).
24 Ibrahim & Abdulazeez (2021); Bowman (2024); Chinnaiyan et al. (2024); Gaur et al. (2023).

and inference—whose analysis enables insights and decisions that would otherwise be impractical or impossible.[25]

A widely cited operational criterion for identifying AI is the Turing test, which asks whether a person, engaged in natural-language exchange with a purported AI system, cannot reliably distinguish it from a human.[26] A positive result is taken as *prima facie* evidence of intelligence. In addition to such evidentiary markers, autonomy constitutes a central attribute of AI. Autonomous systems can generate outputs that are not fully predetermined by programmers, even when they originate from human-specified objectives and constraints.[27] This capacity for non-preprogrammed responses is both intellectually and practically valuable, enabling AI systems to generate novel and unexpected solutions that humans might overlook due to habitual patterns or cognitive biases.

2.2. Applications across sectors

AI now permeates nearly every domain of human activity: in health, it assists with diagnosing diseases, personalising treatments, and supporting the regulatory review and approval of medical devices; in finance, it powers fraud detection and algorithmic trading; in agriculture, it enables crop monitoring, precision irrigation, and predictive yield modelling; in environmental stewardship, it models climate change, tracks deforestation, detects pollution, and monitors compliance; and in law and governance, it supports legal research, case prediction, and automated decision-making in areas such as parole or welfare.[28]

The potential and risks of AI are visible across diverse sectors. Google's Air View+ provides real-time air quality data in India, combining AI, sensors, and satellite imagery.[29] In the Amazon, AI detects illegal logging, while in South Africa, smart collars track rhinos and alert rangers to distress signals, bolstering anti-poaching efforts.[30]

25 Wang et al. (2021).
26 Martinez (2019: 1024).
27 Ibid.: 1026.
28 Selvakumar et al. (2025); Mishra & Mishra (2023); Gatla (2024); Johnson et al. (2021); Patil (2024); Mwangi & Njoroge (2024); Tironi & Lisboa (2023).
29 See https://www.sandtech.com/insight/ai-for-environmental-monitoring/, accessed 29 September 2025; Rautela & Goyal (2024); See https://economictimes.indiatimes.com/tech/technology/google-maps-launches-air-view-in-india-real-time-hyperlocal-air-quality-info/articleshow/115489441.cms?from=mdr, accessed 29 September 2025.
30 See https://www.sandtech.com/insight/ai-for-environmental-monitoring/; https://news.microsoft.com/source/latam/features/ai/project-guacamaya-rainforest-deforestation/?lang=en; https://news.mongabay.com/2021/08/new-artificial-intelligence-tool-helps-forecast-amazon-deforestation/, accessed 29 September 2025; Teixeira et al. (2023).

The justice system offers even more striking illustrations.[31] In Australia, the Judicial Information Research System (JIRS) assists judges in criminal sentencing by analysing vast datasets of past decisions through neural networks.[32] China has taken further steps, establishing "smart courts" in Beijing, Suzhou, and Hangzhou.[33] Litigants can file cases and attend hearings entirely online, with the average case resolved in 40 days and hearings lasting 37 minutes. Nearly all rulings (98%) are accepted without appeal, underscoring both efficiency and compliance.[34] These courts also employ Xiao Fa, an AI-powered assistant that translates complex legal rules into plain language.[35] While it was originally accessible only in courthouses, it is now integrated with Aegis, a WeChat-based platform that handles 30,000 daily queries with 85% accuracy.[36] Together, they reduce barriers to justice by making legal information widely accessible. Similar initiatives are emerging elsewhere. In Europe, the Claudette system, developed at the European University Institute, assists plaintiffs, defendants, and lawyers by assessing litigation risks and estimating the likelihood of success in court.[37]

It must be acknowledged that AI systems differ significantly in design and capability, and they are not always employed in ways consistent with their original or intended objectives. For example, in 2023, a US judge imposed sanctions on two New York lawyers after they submitted a legal brief containing fictitious case citations—all generated by the AI chatbot ChatGPT.[38] In the case of *Mata v Avianca, Inc.* (a routine personal injury case), the plaintiff's attorney, limited by a restricted legal research subscription, utilised ChatGPT to assist in drafting a response to a motion to dismiss.[39] Relying on the chatbot, the attorney submitted an affirmation citing multiple cases, including *Varghese v China Southern Airlines Co., Ltd.*, which appeared to support tolling the statute of limitations under the Montreal Convention due to Avianca's bankruptcy. However, that case, along with several others cited, was entirely fabricated by ChatGPT, complete with invented quotes and legal citations. This highlights the risks of overreliance on generative AI in legal practice, particularly when outputs are not correctly verified, and underscores the need for human oversight and accountability in the use of AI tools. Notably, the judge did not criticise the use of ChatGPT or generative AI itself: "[t]echnological advances are commonplace and there is nothing inherently improper about using a reliable artificial intelligence tool for assistance."[40]

31 See https://www.thomsonreuters.com/en-us/posts/ai-in-courts/humanizing-justice/, accessed 29 September 2025; Bell et al. (2022).
32 Tahura & Selvadurai (2022).
33 See https://www.lexisnexis.ca/en-ca/ihc/2020-02/robot-justice-chinas-use-of-internet-courts.page, accessed 29 September 2025.
34 Ibid.
35 Chen & Li (2020: 8–9).
36 Ibid.
37 Zhou (2024).
38 Lyon (2023).
39 2023 WL 4138427 (S.D.N.Y. June 22, 2023).
40 Lyon (2023: 11).

Instead, the real issue was the failure to verify its output, and its reliance as the primary research tool was described as an example of "poor and sloppy research." A similar incident occurred in 2023, in an appellate decision by the Texas Court of Appeals.[41] There is also *Park v Kim* (US),[42] where an attorney relied on fake, AI-generated legal citations in a filing; *Kruse v Karlan* (US),[43] where a litigant filed a brief with multiple fake, AI-generated legal citations; and *Kohls v Ellison* (US),[44] where lawyers used expert testimony, reports, and affidavits with fake citations and false information generated by AI in court.

In South Africa, the courts have not been as open-minded to the use of AI. In *Parker v Forsyth NO*, where the plaintiff's attorneys relied on ChatGPT for legal research, without verifying its accuracy, the court stated:

> In this age of instant gratification, this incident serves as a timely reminder to, at least, the lawyers involved in this matter that when it comes to legal research, the efficiency of modern technology still needs to be infused with a dose of good old-fashioned independent reading. Courts expect lawyers to bring a legally-independent and questioning mind to bear on, especially, novel legal matters, and certainly not to merely repeat in parrot-fashion, the unverified research of a chatbot (...) The embarrassment associated with this incident is probably sufficient punishment for the Plaintiff's attorneys.[45]

Further, in *Mavundla v MEC: Department of Co-Operative Government and Traditional Affairs KwaZulu-Natal*,[46] a traditional leadership dispute in KwaZulu-Natal, the court encountered a troubling issue with AI-generated legal content. Mavundla's legal representatives submitted a supplementary notice of appeal containing numerous case citations. However, upon review, the court discovered that several of these cited authorities could not be found in any recognised legal database. By design, ChatGPT is not intended to be a legal research tool. When tested on the Uniform Bar Exam (US), OpenAI's GPT-4 language model (released in 2023) outperformed 90% of human test takers.[47] However, it is essential to note that the free version of ChatGPT does not run on GPT-4 and, by comparison, performed significantly worse, scoring better than only 10% of human test-takers.[48] While an AI model running on GPT-4 can perform well when paired with a dedicated legal database, ChatGPT itself lacks access to platforms such as LexisNexis and Westlaw, which are essential for conducting reliable and up-to-date legal research.[49] As a language-based chatbot, ChatGPT can generate legal-

41 Ibid.: 8.
42 91 F.4th 610, 614–16 (2d Cir. 2023).
43 692 S.W.3d 43, 53 (Mo. Ct. App. 2024).
44 24-cv-3754 (LMP/DLM) (D. Minn. Jan 10, 2025).
45 (1585/20) [2023] ZAGPRD 1 (29 June 2023) paras 90-91; See https://www.derebus.org.za/what-have-the-courts-said-about-the-ethical-use-of-artificial-intelligence-in-legal-practice/, accessed 27 October 2025.
46 2025 (3) SA 534 (KZP) (8 January 2025); Petse & Phindelo (2025).
47 See https://law.stanford.edu/2023/04/19/gpt-4-passes-the-bar-exam-what-that-means-for-artificial-intelligence-tools-in-the-legal-industry/, accessed 27 October 2025.
48 Ibid.
49 See https://www.spellbook.legal/learn/chatgpt-for-lawyers, accessed 27 October 2025.

sounding arguments and even cite cases; however, these may be invented or outdated, as it relies solely on its pre-existing training data and is not connected to live legal databases.

These developments illustrate both the transformative potential and the persistent fragility of AI integration across sectors. Whether in environmental monitoring, judicial efficiency, or legal practice, the value of AI depends on responsible design, ethical deployment, and human oversight. The growing number of cases involving fabricated citations or unverified outputs serves as a cautionary reminder that technological sophistication cannot substitute for professional diligence. As AI becomes more deeply embedded in decision-making systems, the challenge is not simply to adopt it but to cultivate the institutional, ethical, and legal frameworks that ensure it advances—rather than undermines—the integrity of human judgment.

2.3. The moving target

The boundary between digitalisation and AI is fluid. As once-novel technologies become commonplace, definitions shift, making AI a "moving target" for regulators. Crucially, AI is never neutral: its outputs reflect the data and values on which it is trained. ML begins with large datasets, from which computers extract patterns and generate their own algorithms.[50] Unlike traditional programming, the model then applies these learned patterns to new data. But because humans curate training data, AI systems often reproduce the biases in that data. For example, self-driving car systems struggled to detect people of colour because the training images underrepresented them.[51] In disaster-risk management, algorithms that privilege affluent districts while overlooking marginalised ones do not deliver fairness; they entrench vulnerability and widen existing inequalities.[52]

AI's potential to reduce bias has been tested in the criminal justice system. A Tulane University study examined 50,000 Virginia convictions in which judges used AI to assess the risk of reoffending.[53] While AI recommendations reduced gender disparities in sentencing, racial gaps persisted; judges were less likely to follow AI advice when the defendant was a person of colour. This highlights AI's dual role: it can promote consistency, yet human prejudice can still distort outcomes. Furthermore, transparency remains a concern. Many judicial AI systems rely on opaque "black box" reasoning, raising questions about accountability and fairness.[54] A 'black box' refers to a

50 Thornton (2023).
51 See https://www.vox.com/future-perfect/2019/3/5/18251924/self-driving-car-racial-bias-study-autonomous-vehicle-dark-skin, accessed 29 September 2025.
52 Zhan & Liao (2024).
53 See https://news.tulane.edu/pr/ai-sentencing-cut-jail-time-low-risk-offenders-study-finds-racial-bias-persisted, accessed 29 September 2025.
54 von Eschenbach (2021).

tool that produces a score without revealing its inputs or logic, sometimes even shielded by trade-secret claims. In court settings, that opacity makes it hard for defendants to challenge errors, for judges to give reasons that can be appealed, and for oversight bodies to detect disparate impact. In other words, even if AI can improve consistency, a lack of explainability and auditability risks entrenching or hiding bias.

US case law illustrates the risks. In *State v Loomis,* a COMPAS risk score contributed to the determination of a six-year sentence, although the defendant was not given insight into the algorithm.[55] The Wisconsin Supreme Court upheld the ruling, treating COMPAS as a legitimate tool despite its opacity.[56] By contrast, in *Kansas v Walls*, the court ordered disclosure of the complete diagnostic assessment used in sentencing, recognising the need for transparency.[57] More recently, *In Re Matter of Weber* exposed the dangers of relying on generative AI: an expert who used Microsoft Copilot was unable to explain how it produced its financial calculations, thereby undermining the credibility of his testimony.[58]

Even at the supranational level, structural biases are evident. Studies of AI applied to European Court of Human Rights (ECtHR) decisions have shown that models trained on judges' summaries often reinforce reasoning aligned with the outcomes, rather than substantively engaging with the law.[59] This raises doubts about whether such systems analyse legal precedent or mimic linguistic cues.

The pitfalls of overstated claims are evident in the case of DoNotPay, a startup that branded itself as "the world's first robot lawyer."[60] The US Federal Trade Commission found that it had not tested its AI to the standard of a human attorney and lacked professionals to verify its outputs.[61]

Together, these examples demonstrate that while AI can streamline processes and reduce certain inequities, it can also amplify hidden biases, undermine transparency, and pose risks when deployed without oversight. The same concerns arise in the governance of agricultural and soil data. Just as courts risk relying on opaque "black box" systems, farmers may be asked to trust AI-driven soil or crop recommendations without insight into how outputs are generated, what data they rely on, or whose interests

55 *State v Loomis* (2016) WI 68, 371 Wis. 2d 235, 881 N.W.2d 749; Freeman (2016); Gualdi & Cordella (2021). COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) is a proprietary risk-assessment tool developed by Northpointe (now Equivant) that some US courts use at bail, sentencing, and parole to estimate a person's risk of reoffending (general and violent). It draws on questionnaire answers and administrative data (e.g., age, prior arrests/convictions, employment, substance-use history) and outputs risk categories/deciles.

56 *Loomis v Wisconsin*, 881 N.W.2d 749 (Wis. 2016), cert. denied, 137 S.Ct. 2290 (2017).

57 *State of Kansas v John Keith Walls*, pp. 116, 027, The Court of Appeals of the State of Kansas (2017).

58 See https://law.justia.com/cases/new-york/other-courts/2024/2024-ny-slip-op-24258.html; https://www.freereferral.com/blog/disqualification-of-expert-witness-for-artificial-intellegence-use, accessed 29 September 2025.

59 Ibid.

60 See https://gizmodo.com/donotpay-has-to-pay-up-over-worlds-first-robot-lawyer-2000503265, accessed 29 September 2025.

61 *In re DoNotPay, Inc*., No. C-4812 (F.T.C. Jan. 14, 2025).

they ultimately serve.[62] In both domains, reliability depends not only on technical design but also on institutional safeguards, accountability, and fair distribution of benefits. Crucially, the quality and diversity of training data are critical: entire climate zones—tropical, arid, mild-continental, and polar tundra—are markedly underrepresented in AI research for agricultural soil health, despite spanning vast areas of Central and South America, Africa, Central and South Asia, and Australia.[63] Suppose AI systems are trained on narrow, imported, or incomplete datasets. In that case, they risk misclassifying soil health, overlooking local realities, and promoting one-size-fits-all recommendations ill-suited to African (and other) contexts.[64] To ensure global applicability, future work should prioritise high-quality, standardised datasets from these under-sampled regions, as well as the rigorous use of bias detection and mitigation methods in datasets and models.

In the worst case, unchecked bias becomes a system driver rather than a bug: a handful of powerful agri-tech platforms, trained on skewed data and optimised for a narrow notion of "efficiency," could standardise practice across regions, marginalising indigenous and local agronomies honed over centuries.[65] In such a stunted trajectory, long-term soil vitality is traded for short-term output: biased systems privilege input-heavy farming, driving widespread application of synthetic fertilisers and pesticides that degrade soil structure, deplete organic matter, and damage the microbial webs that underpin healthy soils—locking farmers into an input treadmill to maintain yields on exhausted land.[66] The biodiversity fallout would be severe: monocultures and intensive pesticide use depress pollinators, natural enemies, and other wildlife, weakening ecological regulation, triggering more frequent pest outbreaks and disease, and eroding the resilience of food systems.[67]

Ensuring diverse, locally relevant soil data feeds into AI systems is therefore essential, not only to improve accuracy but also to uphold equity and resilience in agricultural decision-making. That aim also requires transparency, contestability, and oversight, so that recommendations are explainable, open to challenge, and aligned with the interests of farmers and communities, rather than solely with corporate logics.

62 Gardezi et al. (2023).
63 Schweng et al. (2026: 12).
64 See https://prism.sustainability-directory.com/scenario/algorithmic-bias-in-soil-health-management-systems/, accessed 29 September 2025.
65 Ibid.
66 Ibid.
67 Ibid.

2.4. Sustainable soil management and governance

SSM addresses the multiple pressures contributing to soil degradation and seeks to ensure the long-term health and resilience of soils.[68] Because soils underpin food security, biodiversity, climate regulation, and human livelihoods, their governance is inherently crosscutting. Pressures arise from agriculture, urbanisation, infrastructure, mining, and industrial activity, while climate change intensifies risks through droughts, flooding, and water scarcity. Poverty and insecure land tenure further drive unsustainable practices, weakening resilience.[69]

SSM relies on four main mechanisms:[70] First, SSM starts with reliable data.[71] That means taking field-level measurements of soil conditions, analysing and interpreting the results, and then sharing the information in usable formats with policymakers, regulators, farmers, and the public. Good data enables evidence-based decisions and creates a common factual baseline for action. Second, land-use planning and zoning can shield fertile soils from permanent sealing by urban growth, infrastructure, or industrial projects.[72] Effective planning relies on comprehensive, up-to-date information, and AI can assist by processing large datasets and transforming raw measurements into actionable insights. Digital soil maps that layer soil status, weather patterns, current land uses, and the legal status of ownership and tenure are powerful tools for guiding sustainable planning choices.[73] Third, binding, enforceable soil quality standards set thresholds for acceptable interference and empower authorities to restrict harmful activities when those limits are exceeded.[74] Because soil degradation has many dimensions—erosion, compaction, loss of organic matter, salinisation—developing robust standards is complex and resource-intensive. New digital technologies can support this work by improving monitoring accuracy, analysing large datasets, and grounding the standards in sound evidence. Lastly, long-term soil protection depends on broad recognition of soil's value. Although awareness is improving, soils continue to receive insufficient attention in policy debates. Targeted outreach to politicians, the private sector, civil society, and young people can foster a shared commitment to stewardship.[75] Digital tools can accelerate this by delivering audience-specific materials—adapted to local languages, levels of technical knowledge, and preferred visual styles—that clearly convey the importance and vulnerability of soil.

68 Ginzky & Ruppel (2025a: 252).
69 Ginzky (2023: 535).
70 Ginzky (2022).
71 Ginzky & Ruppel (2022: 44–45).
72 Ginzky & Ruppel (2025b: 32); Ginzky & Ruppel (2025a: 252).
73 Statement of a Soil scientist during a workshop on 8 April 2025 in Stellenbosch, South Africa, "Digitalisation, AI, Sustainability and Soil Protection: Multiple Perspectives"; Ginzky & Ruppel (2025a: 253).
74 Ginzky (2021); Ginzky (2022).
75 Ginzky & Ruppel (2025b: 33).

For decades, soils have been treated as expendable, often overshadowed by air and water in environmental law. Yet soils are non-renewable on human timescales: they take centuries to form but can be degraded within years. Recognising soils as a vital, fragile resource demands governance approaches that are both comprehensive and enforceable.

Digital technologies offer significant opportunities to strengthen soil governance. While field data remains the foundation, digital tools can accelerate analysis, enhance accuracy, and make soil information more accessible to a diverse range of users. The applications of AI in soil science are diverse and impactful, falling into several key branches. The first branch focuses on monitoring and predicting soil health, utilising AI to develop predictive models based on soil properties, microbiome data, sensors, and satellite imagery.[76] This analytical power extends to the very foundation of soil fertility. A second branch focuses on analysing the soil microbiome, where AI tools build predictive models of microbial interactions and their impact on nutrient cycles.[77] Furthermore, AI provides critical insights into soil composition, with specific techniques predicting soil organic carbon levels to forecast global carbon dynamics and identify soils at higher risk of CO_2 release, thereby informing sequestration and sustainable carbon management strategies.[78]

These advanced technologies enable the real-time monitoring and management of inputs, such as fertilisers, pesticides, and irrigation systems. AI plays a crucial role in detecting soil contamination, estimating heavy metal concentrations from soil spectra, and determining nutrient levels in real time.[79] AI tools for soil moisture and water management integrate monitoring and prediction to analyse climatic parameters and provide farmers with irrigation recommendations, thereby reducing water stress and fostering more sustainable, resilient farming practices.[80] Remote sensing, when combined with AI, offers powerful applications for soil management, including detecting land-use changes and estimating soil quality from images.[81] Techniques that interpret soil colour and vegetation from drone or satellite imagery can estimate organic matter and moisture.[82]

Equally important is the dissemination of this complex information. AI can be harnessed to produce audience-tailored outputs, such as translating information into local or indigenous languages, adapting content to varying levels of technical complexity, and using visualisation tools to make data more accessible and meaningful to diverse stakeholders.[83]

76 Rosca & Stancu (2025: 17–18).
77 Ibid.
78 Ibid.
79 Ibid.
80 Nalwimba (2024); Mienye et al. (2024).
81 World Economic Forum (2024).
82 Rosca & Stancu (2025: 17–18).
83 World Economic Forum (2024); Nalwimba (2024).

2.5. Digitalisation, power asymmetries, and sustainability risks

While digital technologies offer great potential for soil governance, they also carry environmental, social, and economic risks. If left unmanaged, these risks could undermine the very sustainability goals that digitalisation aims to support.

First, regarding environmental risks, digitalisation relies on substantial amounts of energy and water.[84] Recent analyses suggest that producing a single image using a state-of-the-art generative model consumes roughly as much electricity as charging a typical smartphone once.[85] By 2027, AI's overall power demand could rival that of countries such as the Netherlands or Argentina.[86] Data centres require cooling systems, often in regions already experiencing water scarcity.[87] Recent estimates suggest that a single conversational session with a leading chatbot (roughly 20–50 prompts and replies) can indirectly consume about the equivalent of a 500 ml bottle of water through evaporative cooling, depending on location, cooling technology, and grid mix.[88] Scaled across millions of sessions, this translates into a substantial aggregate water footprint. In 2022, Google reported that its data centres withdrew roughly 25 billion litres of water and consumed nearly 20 billion litres for on-site cooling—about 77% of which was potable.[89] Typically, around 80% of water withdrawn by data centres is "consumed" (lost) through evaporation.[90] If energy is derived from fossil fuels, emissions rise and may outweigh the environmental benefits of precision agriculture or reduced fertiliser use.

Second, regarding the social risks, two challenges stand out, both of which are explored further below: The first is data privacy and misuse; soil data, when linked to farmers or geolocation, can reveal sensitive information.[91] Without clear rules on ownership, accountability, and liability, private actors may exploit data at the expense of smallholders.[92] The risks are not merely theoretical, as demonstrated by the significant cyberattack against DeepSeek, a Chinese AI startup, in early 2025, which resulted in the leak of data from over a million users.[93] This incident underscores concerns raised by security researchers about the neglect of basic cybersecurity measures on some digital platforms, highlighting a clear and present danger that extends to the agricultural

84 Harvey (2025); see https://www.theguardian.com/technology/2025/apr/10/energy-demands-from-ai-datacentres-to-quadruple-by-2030-says-report, accessed 29 September 2025.
85 Hacker (2023).
86 Ibid.
87 Barratt et al. (2025); https://www.theguardian.com/environment/2025/apr/09/big-tech-datacentres-water, accessed 29 September 2025.
88 Hacker (2023: 5).
89 Ibid.: 7.
90 Ibid.
91 Ginzky & Ruppel (2025a: 254).
92 OECD (2024a and b).
93 See https://www.darkreading.com/cyberattacks-data-breaches/deepseek-breach-opens-floodgates-dark-web, accessed 29 September 2025.

sector, where protecting proprietary farm and location data is paramount. The second is the digital divide: One-third of the world's population remains offline.[94] Digital technologies depend on a reliable power supply. Yet load-shedding and power cuts remain a daily reality in many developing countries.[95] Rural areas are particularly affected, limiting the use of digital tools precisely where they are most needed for soil and agricultural management.[96] Investments in AI and digital infrastructure are concentrated in the Global North, leaving many countries in the Global South behind.[97] An Oxford Insights assessment of 181 countries reveals that many regions in the Global South, particularly sub-Saharan Africa, parts of Central and South Asia, and certain areas of Latin America, rank lowest in preparedness to implement AI in public services.[98] The report emphasises that effective AI development relies on a supportive operating environment, including a robust technology sector, reliable data infrastructure, and a clear strategic direction focused on governance and ethical standards. Without basic infrastructure, even the most advanced digital applications cannot function effectively, leaving rural farmers and communities excluded from the benefits of innovation.[99]

Third, regarding economic risks, inclusive access is vulnerable to restrictions due to high costs and technical barriers, which could exacerbate disparities in agriculture. Investment in digitalisation and AI is disproportionately concentrated in the Global North.[100] For instance, training sophisticated AI models can cost several million dollars.[101] Canada unveiled a USD 2.4 billion package to strengthen its AI infrastructure, while China introduced a USD 47.5 billion fund to accelerate semiconductor production. France has committed USD 113 billion to advancing AI capabilities, while India has pledged USD 1.25 billion. Saudi Arabia's ambitious Project Transcendence, valued at USD 100 billion, aims to position the country as a leader in AI.[102] Most African and other developing countries cannot match these levels, leaving them dependent on technologies, platforms, and expertise imported from abroad. In Nigeria, for instance, despite its relative technical advancement, around 90% of software is imported, with local efforts confined largely to producing add-ons or extensions for mainstream products.[103] A handful of global technology companies dominate the digital sector. Their

94 See https://www.destatis.de/DE/Themen/Laender-Regionen/Internationales/Thema/wissenschaft-technologie-digitales/_inhalt.html, accessed 29 September 2025; Ginzky & Ruppel (2025a: 254-255).
95 AU (2024b: 14); Okolo et al. (2023: 38).
96 Okolo et al. (2023: 41).
97 Ruthmann-Bloem (2023).
98 See https://oxfordinsights.com/ai-readiness/ai-readiness-index/, accessed 29 September 2025.
99 Arakpogun et al. (2021). See also https://news.un.org/en/story/2023/07/1138827, accessed 29 September 2025.
100 For example: African Union Development Agency (2021:45); von Carlowitz, Züfle & Schmid (2025).
101 For further information see https://www.weforum.org/stories/2023/01/davos23-ai-divide-global-north-global-south/, accessed 29 September 2025.
102 Stanford University (2025: 4).
103 Birhane (2020: 396).

control over platforms, algorithms, and services risks creating monopolies and undermining fair competition. Robust national and international competition rules are needed to prevent dependency on a few powerful actors.[104] Furthermore, many countries in the Global South face shortages of skilled personnel to design, adapt, and govern digital technologies. Many African AI experts work abroad, contributing to a talent drain that weakens local capacity and expertise. Farmers and end-users may also lack the literacy and training necessary to benefit from digital services.[105] These services include mobile phones and the internet, as well as newer tools such as big-data analytics, blockchain, drones, satellite imagery, AI/machine learning, and remote sensing—used both on farms (e.g., drones for spraying) and as support services (e.g., blockchain traceability or mobile weather alerts).[106]

There is a clear need to address market power concentrations through effective regulatory frameworks. Given that many leading technology companies operate in highly globalised markets, international regulation is crucial to ensure accountability and equitable access.[107] Achieving agreement on shared international standards, however, is likely to become increasingly challenging in the current geopolitical climate. At the same time, the accumulation of market power within domestic economies also calls for strong national oversight to curb monopolistic practices and safeguard fair competition.[108] These risks and challenges vary depending on the specific digital tools and applications involved. For instance, it will be necessary to examine whether the deployment of AI in fertiliser use is so energy-intensive that it negates the environmental benefits of reduced fertiliser application, and whether access to such technologies risks exacerbating existing economic inequalities among farmers.[109]

Taken together, these environmental, social, and economic risks highlight that digitalisation is not a neutral process. Its outcomes depend on context, regulation, and capacity. Without proactive governance, digital tools intended to strengthen soil management may unintentionally deepen existing inequalities and environmental pressures. The challenge, therefore, is not whether to embrace digitalisation, but how to design rules and institutions that ensure its benefits reach farmers and ecosystems alike.

These risks point to a broader structural challenge: digitalisation, environmental degradation, and socio-economic inequality cannot be governed in isolation. As the German Advisory Council on Global Change (WBGU) emphasises, future-oriented policymaking requires an integrated understanding of security—one that places the protection of natural life-support systems at its core.[110] Climate change, biodiversity

104 OECD (2024a: 33).
105 Okolo et al. (2023: 40).
106 Abdulai et al. (2023).
107 Ginzky & Ruppel (2025a: 255).
108 Ibid.
109 Ibid.
110 WBGU (2026: 1).

loss, pollution, land degradation, and desertification are no longer peripheral environmental concerns but are among the most significant long-term risks to societal stability, economic systems, and democratic resilience. From this perspective, soil governance must be understood as a foundational element of integrated security policy. The WBGU highlights that sustainable agricultural systems, soil conservation, and climate-resilient land management are essential not only for environmental protection but for ensuring food security, social cohesion, and geopolitical stability.[111] At the same time, the rapid expansion of AI and digital infrastructures introduces new vulnerabilities, including dependencies on external technologies, risks to information integrity, and widening global inequalities in digital capacity. A future-oriented legal response must therefore move beyond fragmented regulatory approaches and instead embed soil governance, digital governance, and socio-ecological resilience within a multidimensional security architecture. This includes integrating environmental risks into early-warning systems, strengthening international cooperation, reducing technological dependencies, and ensuring that digital innovation aligns with long-term sustainability goals.[112] Without such integration, efforts to regulate AI and digitalisation risk reinforcing, rather than mitigating, the structural vulnerabilities they seek to address.

2.6. Governing AI: law, power, and accountability

AI has been described as "summoning the demon."[113] While hyperbolic, the remark reflects widespread concern that without proper regulation, AI may produce harms that are irreversible or uncontrollable. Clear governance frameworks are, therefore, essential to maximise benefits while minimising risks. The evidence shows a landscape already skewed toward large-scale, industrial farming. The "bias" in datasets and models is not a technical hiccup—it mirrors entrenched social inequities and power imbalances. Left unchecked, it will grow worse, driving ecological decline, widening injustice, and further concentrating control in corporate hands.[114]

Yet the persistence of these risks cannot be explained solely by regulatory delays or oversight failures; it reflects deeper structural constraints within the global political economy of artificial intelligence. A growing body of scholarship suggests that the current impasse in international AI governance persists because major powers prioritise strategic and economic advantage over cooperation, private actors retain disproportionate control over data and technological infrastructure, and international

111 Ibid.: 5.
112 Ibid.: 4.
113 See https://www.cnet.com/science/elon-musk-we-are-summoning-the-demon-with-artificial-intelligence/, accessed 29 September 2025.
114 See https://prism.sustainability-directory.com/scenario/algorithmic-bias-in-soil-health-management-systems/, accessed 29 September 2025.

institutions lack both enforcement capacity and technical expertise. In such a context, global coordination remains limited, fragmented, and largely non-binding. Meaningful governance progress may therefore only become politically feasible when the costs of regulatory inaction become too significant to ignore. Historical experience demonstrates that durable governance regimes are rarely the product of foresight alone, but are instead catalysed by crisis, moments in which systemic failure collapses political resistance and creates narrow windows for institutional innovation. This suggests that the challenge for AI governance is not only to develop normative frameworks in advance, but to ensure that legal, technical, and institutional mechanisms are sufficiently developed to be rapidly operationalised when such windows emerge.[115]

Globally, legislative attention to AI is increasing rapidly. Between 2016 and 2024, the AI Index tracked bills and statutes mentioning "artificial intelligence" across 114 countries; of these, 39 countries adopted at least one AI-related law, resulting in a cumulative total of 204 AI-related enactments.[116] Over 70 countries have now developed and implemented national strategies or policies focused on AI, with the majority of these initiatives concentrated in high-income and upper-middle-income countries.[117] This compares with just 16% of lower-middle-income economies and only 8% of low-income economies.[118] References to AI in legislative proceedings rose by over 20% between 2023 and 2024 alone.[119] In the Global South, where public awareness of algorithmic bias, privacy, and accountability remains limited, strong governance is crucial. By 2025, 36 of Africa's 55 countries had adopted data protection laws, of which 31 guard against automated decision-making.[120] Only 26 had functioning data protection authorities, of which only fifteen established an expert body on AI.[121] However, no African country had yet enacted dedicated AI legislation, and only eight had adopted AI policy frameworks or strategies (twelve).[122] This patchwork highlights the unevenness of AI readiness across the continent, creating a

115 Wilkinson et al. (2026).
116 Stanford University (2025: 337).
117 WTO (2025: 69–70).
118 Ibid.
119 Stanford University (2025).
120 Makulilo (2024: 43); See https://www.trust.org/toolkit/part-2-emerging-ai-governance-in-africa/domestic-ai-governance/, accessed 29 September 2025.
121 To stay up to date, see https://iapp.org/resources/article/global-ai-legislation-tracker/, https://www.trust.org/toolkit/part-2-emerging-ai-governance-in-africa/domestic-ai-governance/, accessed 29 September 2025; Andere & Kathure (2024).
122 See https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-african-union, https://www.lawyershub.org/news/post/artificial-intelligence-and-parliaments-in-africa, https://www.dentons.com/en/insights/articles/2024/june/13/ai-regulation-and-policy-in-africa, https://www.trust.org/toolkit/part-2-emerging-ai-governance-in-africa/domestic-ai-governance/, accessed 29 September 2025; Davis et al. (2022).

vacuum that allows external actors to dominate Africa's digital landscape with minimal accountability.[123]

The challenges associated with digitalisation in the context of soil governance are not merely technical but reveal a deeper structural problem within contemporary legal systems. The rapid pace of technological development, particularly in fields such as AI, the Internet of Things, and data-driven agriculture, has outstripped the capacity of existing regulatory frameworks to respond effectively.[124] As a result, regulatory systems are frequently reactive, fragmented, and ill-equipped to anticipate or manage emerging risks. This temporal mismatch creates a persistent governance gap, where technologies are widely deployed before their implications are fully understood, leaving both ecosystems and communities vulnerable. This challenge is compounded by significant information asymmetries between regulators, industry actors, and affected communities. Policymakers often lack access to the technical knowledge, data, and predictive capacity necessary to make informed decisions, while private actors—particularly large technology firms—retain disproportionate control over both technological development and the data that underpins it.[125] In the context of soil governance, this asymmetry is especially pronounced, as soil data is increasingly captured, processed, and commercialised through digital platforms that are often external to the jurisdictions in which the data originates. This dynamic risks reinforcing existing inequalities and contributing to new forms of digital dependency and extraction.

At the same time, the transboundary nature of digital technologies further complicates governance efforts. Data flows, algorithmic systems, and digital infrastructures operate across national borders, challenging traditional concepts of jurisdiction, accountability, and regulatory authority.[126] Actions undertaken in one jurisdiction may have far-reaching environmental, economic, and social consequences in another, while fragmented regulatory approaches create inconsistencies, gaps, and opportunities for regulatory arbitrage. In such a context, purely national or sectoral approaches to regulation are insufficient. These dynamics are exacerbated by institutional fragmentation. Digital technologies frequently fall within overlapping or unclear regulatory mandates, resulting in a diffusion of responsibility across multiple agencies.[127] In some cases, this leads to duplication and inefficiency; in others, critical risks fall through the cracks altogether. Soil governance, already characterised by fragmented legal and institutional frameworks, is particularly vulnerable to these dynamics. The integration of digital technologies into soil management, therefore, risks entrenching, rather than resolving, existing governance deficiencies.

123 Salami (2024).
124 OECD (2025b: 87).
125 Ibid.: 90.
126 Ibid.: 91–92.
127 Ibid.: 97 & 111–112.

Traditional regulatory approaches are poorly suited to these conditions. Law has historically operated through relatively static, "set-and-forget" models, whereby rules are designed, enacted, and only periodically reviewed.[128] However, such approaches are incompatible with the dynamic and rapidly evolving nature of digital technologies. By the time regulatory interventions are implemented, the technologies in question may already have evolved, rendering existing rules obsolete or ineffective. This highlights the need for a fundamental shift in regulatory design and governance philosophy. In response, there is growing recognition of the need for more adaptive, anticipatory, and integrated forms of governance. Anticipatory governance approaches—incorporating tools such as horizon scanning, strategic foresight, and early-stage stakeholder engagement—offer a means of identifying emerging risks and opportunities before they become entrenched.[129] Such approaches emphasise iterative policy cycles, continuous learning, and the integration of diverse forms of knowledge, including scientific, technical, and local expertise.

For soil governance, this shift is particularly significant. It requires moving beyond fragmented, sector-specific regulation towards a more holistic framework that integrates environmental protection, digital governance, and socio-economic considerations. This includes recognising soil not only as a resource to be managed but also as a critical component of broader socio-ecological systems that underpin food security, climate resilience, and human well-being. It also necessitates addressing questions of data ownership, technological sovereignty, and equitable access to digital tools and infrastructures. Governing soil in the digital age demands more than incremental reform. It requires a reconfiguration of legal and institutional frameworks to address the interconnected challenges of technological innovation, environmental degradation, and global inequality. Without such a shift, efforts to harness digital technologies for sustainable soil management risk reproducing the very power imbalances and governance failures they seek to overcome.

2.6.1. The 2024 OECD Study

The Organisation for Economic Co-operation and Development (OECD) conducted a comprehensive study between 2023 and 2024 on the risks, benefits, and policy implications of AI.[130] Its Expert Group on AI Futures, comprising around 70 specialists from various regions and disciplines, published its findings in December 2024.[131]

The report identified ten priority policy actions, including:[132]

128 Ibid.: 91.
129 Ibid.: 92–93.
130 OECD (2024a).
131 See https://oecd.ai/en/site/ai-futures, accessed 29 September 2025.
132 Ginzky & Ruppel (2025a: 256–259).

Establishing more explicit liability rules for AI-related harms. Because new digital technologies, including AI, carry inherent risks of harm, transparent and enforceable liability regimes are indispensable. Such frameworks must reflect the distinctive features of AI systems—especially their complexity, autonomy, and opacity—and clarify how accountability is allocated. This involves defining the legal standards of causation and establishing rules for assigning the burden of proof in cases of harm. Without this clarification, it will be challenging to guarantee justice for affected parties, safeguard rights, and promote responsible innovation.

Defining "red lines" to prohibit AI uses that violate fundamental rights. Clear red lines may be necessary where AI applications infringe on fundamental rights, such as human rights or privacy. In such cases, outright prohibitions should apply. Beyond individual rights, the prospect of severe adverse impacts on broader public goods, such as democratic integrity or climate stability, can also justify adopting strict regulatory measures, including bans on specific applications.

Requiring disclosure of key information about AI systems. Disclosure of the information underlying AI applications is essential, particularly to enable consumers to make informed choices and to counterbalance the power asymmetry between AI developers, users, and those affected by the technology. As the number and influence of AI applications continue to grow, ensuring such transparency becomes ever more critical.

Implementing risk management procedures across the AI lifecycle. Certain types and categories of new digital technologies may pose significant risks to the public good during both their development and deployment. To address these concerns, robust risk assessment and management mechanisms must be designed and agreed upon. Such assessments should be conducted before market entry and then continuously monitored and revised throughout the technology's deployment.

Preventing excessive concentration of market power. The concentration of market power poses a significant challenge to ensuring equitable access to new digital technologies and maintaining transparency regarding the conditions under which they are developed and deployed. Such concentration risks slowing technological progress, hindering economic growth, and creating structural imbalances between developers and users on the one hand, and consumers on the other. To mitigate these risks, appropriate international regulation, particularly competition rules, is essential to safeguard fair access, stimulate innovation, and prevent the adverse effects of excessive market concentration.

Investing in AI safety, transparency, and interpretability research. The safety of AI systems is paramount and must be understood in multiple dimensions. First, AI must be aligned with human values and respect human rights. Second, high-risk AI applications require rigorous assessment and management, supported by appropriate safeguards. Third, systems must demonstrate robustness, i.e., safety, reliability, and resilience to deviations from their intended purpose. Together, these principles underpin

the trustworthy and responsible deployment of AI. In parallel, technological development must prioritise explainability, interpretability, and transparency to reduce bias and other systemic deficiencies.

Expanding education and retraining to address labour disruptions. Capacity building is essential to ensure the availability of skilled human resources for the development and deployment of AI and other digital technologies. This requires investment in both higher education and continuous on-the-job training. Importantly, capacity-building initiatives must also consider the specific perspectives, priorities, and needs of the Global South, where resource constraints and developmental challenges demand tailored approaches.

Ensuring broad stakeholder participation to strengthen trust and democracy. Stakeholder involvement in all decision-making processes is vital. Such participation is not only instrumental in refining, developing, and improving AI applications but also serves as a trust-building exercise. By ensuring inclusiveness and transparency, stakeholder engagement can strengthen confidence in both democratic processes and the rule of law, thereby reinforcing the legitimacy of AI governance.

Mitigating wider forms of power concentration (technological, economic, political). This dimension closely relates to mitigating competitive dynamics but places greater emphasis on broader forms of power concentration. It highlights how excessive concentrations of power—whether economic, technological, or political—can pose significant risks to public goods and therefore require careful regulatory oversight.

Taking targeted actions to secure specific societal benefits of AI. This dimension underscores the need for governance frameworks that actively secure the realisation of anticipated benefits, rather than merely facilitating them indirectly or passively. Currently, most governance approaches tend to enable potential benefits only incidentally, without ensuring that these are fully realised or fairly distributed. To close this gap, more direct, outcome-oriented measures are required—frameworks that not only support innovation but also guarantee that its benefits are effectively delivered and equitably shared.

While comprehensive, the report underemphasised three dimensions critical for the Global South: persistent deficits in power supply, infrastructure, and digital literacy; risks of deepening the global digital divide; and environmental trade-offs, such as the energy and water footprint of AI. Therefore, while the OECD framework offers a valuable foundation, its Global North bias limits its applicability in contexts where soils, agriculture, and basic infrastructure remain existential concerns.

2.6.2. Legislation at the national level

At the national level, regulating digital technologies in the context of soil governance reveals both the breadth of relevant laws and the gaps between them. Soil management

is inherently cross-sectoral: effective regulation depends not on a single statute but on a patchwork of provisions across multiple domains. Most countries lack dedicated soil laws. Instead, general environmental statutes and sector-specific provisions shape soil governance. Relevant areas include agricultural law (fertilisers, pesticides, land use); urban and regional planning; industrial and mining regulation; water management; and nature conservation. This fragmentation is often criticised, but it is unavoidable given the soils' cross-cutting role. It does, however, complicate the integration of digital tools into soil governance.

The African Union's (AU) Continental Artificial Intelligence Strategy identifies a wide range of existing laws as relevant for AI and digital governance, including:[133] intellectual property law; electronic communications and transactions law; whistleblowing and disclosure law; access to information law; personal data protection law; cybersecurity law; consumer protection law; antitrust and competition law; and laws promoting inclusion and empowerment of marginalised groups. Together, these frameworks form the legal foundation for regulating digital innovation, protecting rights, and ensuring that new technologies support equitable outcomes.

Despite this, digitalisation is rarely addressed in soil-related legal frameworks. The *International Yearbook of Soil Law and Policy* has not explicitly covered the interface between digital technologies and soil governance in any of its six volumes, nor have the recent *Soil Security* special issues.[134] Likewise, the AU's AI Strategy omits explicit references to environmental protection or climate law.

This separation reflects a broader trend: debates on digitalisation are often siloed from debates on environmental sustainability, even though they are increasingly interdependent. Bridging this gap is critical if soil governance is to keep pace with technological change.

2.6.2.1. Examples at the regional and national level

Technological change advances at a pace that often outstrips the law. Legal frameworks, typically designed to manage stable and measurable risks, struggle to keep pace with innovations that rapidly transition from "cutting-edge" to commonplace. This constant cycle of adjustment forces regulators to address not only technical risks but also deeper ethical and societal questions of fairness, dignity, and non-discrimination. Yet these values are interpreted differently across societies, making harmonisation difficult and producing fragmented regulatory approaches.[135]

133 AU (2024b: 32).

134 See https://www.umweltbundesamt.de/en/topics/international-yearbook-of-soil-law-policy, accessed 29 September 2025. For the two special issues: https://www.sciencedirect.com/special-issue/10VQ9HFPD6Z; and https://www.sciencedirect.com/special-issue/1006G3251R7.

135 WTO (2024).

Countries in the Global North, with stronger infrastructure, investment, and expertise, are better positioned to shape the trajectory of AI. At the same time, many in the Global South remain constrained by persistent deficits. By 2015, over 100 AI-related policies had already been implemented across all high-income economies.[136] Upper-middle-income economies reached this milestone in 2018, while lower-middle-income and low-income economies have yet to achieve this level of policy development.[137] Without deliberate safeguards, the digital revolution could entrench dependency rather than promote inclusion. At the same time, AI offers opportunities for leapfrogging traditional barriers to development. With appropriate governance, digital tools can support sustainable agriculture, strengthen climate adaptation, and promote more inclusive soil management. For many developing economies, the central challenge is not whether to engage with AI, but how to do so without replicating past patterns of reliance on external models.

The AU has increasingly shifted its institutional focus to AI governance. This trajectory began with the 2019 Sharm el-Sheikh Declaration, adopted by AU Ministers responsible for Communication and Information Technologies under the Specialised Technical Committee on that subject.[138] The Declaration reaffirmed earlier AU digital initiatives, including the Policy and Regulatory Initiative for Digital Africa (PRIDA), as well as existing cybersecurity and data protection frameworks, setting out an ambitious vision for an inclusive digital society and economy. It called on Member States to accelerate the implementation of the Digital Transformation Strategy for Africa (2020–2030), ratify the Malabo Convention, promote digitalisation across sectors such as postal services and financial systems, and establish national Internet Governance Forums. Institutionally, the Declaration mandated the AU Commission to mobilise resources to implement the digital strategy and established a working group on AI to develop a unified continental position. It also proposed an Africa-wide framework for capacity building and the establishment of an AI think tank aligned with Agenda 2063 and the UN Sustainable Development Goals (SDGs). Building on these foundations, the Continental Artificial Intelligence Strategy for Africa, adopted by the AU Executive Council in 2024, seeks to guide national AI strategies, governance frameworks, and capacity-building efforts.[139] Complementary efforts by the African Commission on Human and Peoples' Rights, notably Resolution 473 (2021), underscore the need to ensure that AI, robotics, and emerging technologies are developed and deployed in ways consistent with African values and human rights.[140] The Malabo Convention on Cybersecurity and Personal Data Protection, adopted in 2014 and entering into force

136 WTO (2025: 70).
137 Ibid.
138 ALT Advisory (2022: 6).
139 See https://fpf.org/blog/global/the-african-unions-continental-ai-strategy-data-protection-and-governance-laws-set-to-play-a-key-role-in-ai-regulation/, accessed 27 October 2025.
140 See https://presscouncil.org.za/2025/05/14/african-commission-study-charts-path-for-ethical-ai-in-africa/, accessed 27 October 2025.

in 2023, remains the AU's key binding instrument, setting comprehensive standards for e-commerce, data protection, and cybersecurity. Yet only sixteen states have ratified it so far, underscoring ongoing implementation challenges.

National efforts signal early steps toward regional convergence. South Africa released its National Policy Framework on AI in 2025, setting ethical guardrails for responsible use, mandating transparency in algorithmic decisions, and prioritising public safety—seeking to spur innovation while protecting rights.[141] Nigeria's National AI Strategy (2023) aims to drive growth in agriculture, finance, and health, while pairing that ambition with clear ethical and regulatory safeguards.[142] Kenya launched its National AI Strategy 2025–2030, focused on ethical, inclusive, innovation-led adoption.[143] Rwanda's National AI Policy (2023) emphasises fairness and transparency, sets guidance for public-sector use (including smart-city applications), and invests in regulator training.[144] Egypt's National AI Strategy (2025–2030) strikes a balance between economic objectives and oversight, requiring ethical thresholds for AI in public services and the development of monitoring frameworks across various sectors, including transportation.[145] Mauritius's National AI Strategy (2018) targets economy-wide gains in productivity and quality of life, pairing priority use cases with plans to build an innovation ecosystem and a fit-for-purpose regulatory framework.[146]

The Continental AI Strategy identifies agriculture as a key sector for AI innovation, promoting centres of excellence, knowledge sharing, and awareness-raising about AI's potential and risks. While these initiatives focus broadly on agriculture, their relevance extends to soil protection and management, as soil governance forms the ecological foundation of agricultural systems. Similarly, the Soil Initiative for Africa (SIA) integrates digital technologies across its priority areas, particularly in data-driven soil monitoring and integrated planning.[147] However, the SIA remains silent mainly on regulatory guidance for digital tools—highlighting the broader challenge of fragmented, uncoordinated national frameworks and the need for continental coherence in governing AI for sustainable soil management.

141 See https://www.techpolicy.press/scaffolding-for-the-south-africa-national-ai-policy-framework/, accessed 27 October 2025.

142 See https://africa.businessinsider.com/local/markets/from-data-to-ai-inside-nigerias-leading-blueprint-for-africas-digital-sovereignty/e6r7cxj, accessed 27 October 2025.

143 See https://www.covafrica.com/2025/04/kenyas-ai-strategy-2025-2030-signals-for-global-companies-operating-in-africa/, accessed 27 October 2025.

144 See https://theconversation.com/ai-policies-in-africa-lessons-from-ghana-and-rwanda-253642, accessed 27 October 2025.

145 See https://techafricanews.com/2025/09/04/egypt-aims-for-ai-leadership-in-the-middle-east-and-africa-with-new-national-strategy/, accessed 27 October 2025.

146 See https://www.legal500.com/developments/thought-leadership/ai-regulation-and-policy-in-africa/, accessed 27 October 2025.

147 See https://sia.faraafrica.org/, accessed 27 October 2025.

Against this backdrop, several major regulatory models dominate global debates on AI. Each provides valuable lessons for integrating AI into soil governance, though they carry essential limitations:

2.6.2.2. EU Artificial Intelligence Act (EU AI Act)

Adopted in June 2024 after years of negotiation, the EU AI Act is the first comprehensive legislative framework for AI.[148] According to Article 113, the regulation will formally take effect on 2 August 2026, although compliance with Chapters I and II will be required as of 2 February 2025. As of 2 August 2025, the AI Act's Chapter V obligations for General-Purpose AI apply to any model first placed on the EU market on or after that date. Models already on the market before 2 August 2025 have a two-year grace period—until 2 August 2027—to comply (Article 111(3)). A "general-purpose AI model" under the AI Act is a model trained with extensive datasets and compute that can generate language (text/audio), images, or video and shows broad functional generality—i.e., it can perform many distinct tasks and be integrated into a wide range of downstream systems. Models used only for research, development, or prototyping before market placement are excluded. Examples include GPT-4, Google Gemini, and Llama 3.1; social media chatbots are built on these models. On 18 July 2025, the European Commission published draft guidelines clarifying how the AI Act's provisions apply to these models.[149]

As a regulation, the Act applies directly in all Member States. In its 2020 White Paper, the European Commission highlighted risks such as privacy intrusions, constraints on freedom of expression, affronts to human dignity, and discriminatory outcomes (e.g., in hiring) as key AI harms—classifying them as non-material threats to fundamental rights, distinct from material risks to safety and health.[150] Accordingly, the Act's architecture is explicitly risk-based, classifying AI systems according to the level of risk they pose to health, security, or fundamental rights. This orientation has led many observers to describe the EU's regulatory model as explicitly human-centric, reflecting its emphasis on safeguarding public goods and fundamental values.[151]

148 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689; Ginzky & Ruppel (2025a: 261–263).

149 See https://digital-strategy.ec.europa.eu/en/library/guidelines-scope-obligations-providers-general-purpose-ai-models-under-ai-act, accessed 29 September 2025.

150 See https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf, accessed 29 September 2025.

151 Pirozolli (2024).

Under the EU's AI Act, systems deemed to pose "unacceptable" risk are outright prohibited.[152] These include manipulative AI targeting vulnerable groups (e.g., voice-activated toys that incite dangerous behaviour in children); social scoring systems; biometric categorisation and identification in public spaces. "High-risk" systems may operate only if they meet strict safeguards:[153] a lifecycle risk-management process (Article 9); training and testing on data suitable for the intended use (Article 10); comprehensive technical documentation (Article 11); automatic logging of key events (Article 12); clear information for deployers about risks and proper use (Article 13); and effective human oversight during operation (Article 14). These include AI used in critical infrastructure, education, employment, law enforcement, border control, and legal interpretation. Before being marketed or put into service, they must pass a conformity assessment (Article 16). In addition, general-purpose AI models are split into those that create systemic risks and those that do not (Article 52a), with different obligations applying to each category. Limited and minimal-risk systems (such as generative AI models like ChatGPT) fall into this category and are subject to transparency and copyright rules. To support innovation, the Act also mandates the creation of AI regulatory sandboxes, enabling the controlled testing of new systems. A regulatory sandbox is a soft-law tool commonly used for emerging technologies such as AI: it lets startups and other innovators trial their products in real-world conditions within a controlled, regulator-supervised setting.[154]

The European Commission has also released a General-Purpose AI Code of Practice, drafted by independent experts, and endorsed it as a suitable voluntary instrument for providers to show alignment with the AI Act.[155] The Code centres on transparency, copyright compliance, and model safety and security. Providers are invited to sign it, and by doing so, formally commit to following its principles.

For soil governance, the EU AI Act will apply where soil-related AI systems are placed on the EU market. However, criticism has emerged: environmental impacts are not explicitly included in the risk framework, and stakeholder participation (e.g., farmers, civil society) is not required in the risk classification process.[156] The AI Act leaves significant sustainability risks largely untouched. It contains no binding provisions on the energy and water use of data centres, the associated greenhouse-gas emissions, or the mounting problem of e-waste—issues flagged by the European Parliament's research service—beyond pointing to voluntary codes of conduct.[157] There are virtually

152 See https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence#ai-regulation-in-europe-the-first-comprehensive-framework-4, accessed 29 September 2025.
153 Ibid.
154 See https://www.trust.org/toolkit/part-2-emerging-ai-governance-in-africa/the-continental-response/, accessed 29 September 2025.
155 See https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1787, accessed 29 September 2025.
156 Müller (2022: A6).
157 Wörsdörfer (2023).

no explicit references to climate change, ecological sustainability, environmental protection, or "green AI."[158] As Floridi notes, the framework remains predominantly anthropocentric, centring on human rights impacts while sidelining environmental harms.[159] These omissions reduce transparency and inclusiveness, undermining the Act's potential to support sustainability.

Notably, some emerging economies in the Global South, including Mexico, are edging toward the EU's template.[160]

2.6.2.3. China's regulatory concept

China can be considered a frontrunner in AI regulation.[161] Since 2022, it has introduced a series of targeted measures: the Algorithm Recommendation Regulation (2022), which sets rules for fairness and transparency in recommendation systems; the Deep Synthesis Regulation (2023), which governs "deepfake" and synthetic media technologies; Generative AI Regulation (2023), which requires security assessments before deployment of generative AI; and the Ethical Review Measures (draft, 2023), which obliges universities, research bodies, and companies engaged in sensitive technologies to establish ethics committees.[162]

Unlike the EU, China does not classify AI systems by risk levels or prohibit particular applications. Instead, regulation is designed to ensure that AI serves state priorities, with an emphasis on ethics, security, and social stability. As a result, China's regulatory framework has often been characterised as "state-centric," in contrast to the EU's explicitly human-centric approach.[163]

Notably, China does not yet have a single comprehensive AI statute. Plans for an overarching AI law were removed from the 2025 legislative agenda, signalling a preference for a phased regulatory strategy rather than immediate codification.[164] Instead of adopting a unified framework, China currently relies on a combination of targeted regulations, sector-specific rules, technical standards, and regulatory pilots to govern AI development and deployment. This incremental approach allows regulators to test governance mechanisms, refine safety and transparency requirements, and respond to emerging risks while maintaining regulatory flexibility and limiting compliance burdens for industry. However, the absence of a unified statute also leaves companies navigating a fragmented governance landscape, with overlapping obligations across

158 Ibid.
159 Floridi (2021).
160 Ibid.
161 For full discussion, see Filipova (2024); Karpiuk-Wawryszuk & Kasprowicz (2025).
162 Quoted from Xu et al. (2023: 9-10); Ginzky & Ruppel (2025a: 263-264).
163 Randazzoa & Hill (2025: 4).
164 See https://eastasiaforum.org/2025/12/25/china-resets-the-path-to-comprehensive-ai-governance/, accessed 15 March 2026.

different regulatory instruments. Therefore, coordination among transparency rules, safety testing requirements, and data governance frameworks remains a key challenge within China's evolving AI governance model.

As in the EU, environmental considerations remain largely absent from China's AI governance framework.[165] This omission limits the relevance of the Chinese model for SSM, particularly in contexts where ecological protection and land-resource governance are central policy objectives.

2.6.2.4. Singapore's model framework

Although less publicised than the EU and China's approaches, Singapore provides essential guidance, having introduced its Model Artificial Intelligence Governance Framework in 2019 and updated it in 2020. The framework is built on two overarching principles: AI decisions should be explainable, transparent, and fair, and AI systems should be human-centric, safeguarding people's interests, safety, and well-being.[166]

These principles are elaborated through four areas of guidance. First, organisations are encouraged to establish or adapt internal governance structures to incorporate values, responsibilities, and risk management in algorithmic decision-making. Second, the framework helps determine the appropriate level of human involvement in AI decision-making, using tools such as a "probability–severity of harm" matrix to assess risk appetite. Third, it addresses operations management, outlining factors for developing, selecting, and maintaining AI models, with a particular focus on data management. Finally, it provides strategies for communicating with stakeholders and management on the use of AI solutions.

As a central technology hub in Asia, Singapore's approach has a regional influence, illustrating how voluntary frameworks can promote the responsible adoption of AI. Unlike regulatory mandates, the model relies on industry uptake, allowing for rapid refinement through practical experience.[167] Its rules- and risk-based approach balances innovation with protection, recognising that sustainable AI development requires advancing competitiveness while safeguarding rights and trust.

The framework's emphasis on human-centricity goes beyond ethics, treating it as a business imperative. AI systems are expected to enhance human capabilities, respect autonomy, and preserve oversight in consequential decisions. This ensures that technology strengthens, rather than substitutes, human judgement—building the trust essential for widespread adoption.

165 See https://www.chathamhouse.org/2022/03/challenges-ai, accessed 29 September 2025; Birkstedt et al. (2023).

166 See https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf, accessed 29 September 2025.

167 Lousqui (2025).

Singapore's Model AI Governance Framework for Generative AI ("GenAI Framework"), issued on 30 May 2024 by the Infocomm Media Development Authority and the AI Verify Foundation, offers a detailed soft-law instrument that couples high-level principles with operational guidance across nine interlocking dimensions.[168] It assigns accountability *ex ante* across the technology stack and provides *ex post* redress mechanisms (including indemnities and insurance); sets out data-governance expectations focused on quality, lawfulness (privacy and copyright), and the use of privacy-enhancing technologies; requires trustworthy development and deployment through lifecycle safety practices, context-specific risk assessment, and standardised, plain-language disclosures; establishes proportionate incident management encompassing proactive vulnerability reporting and thresholds for mandatory notification; envisages third-party testing and assurance supported by standard benchmarks and, in time, accreditation; embeds security-by-design complemented by GenAI-specific controls (such as input-risk filters and digital forensics); promotes content provenance via watermarking, cryptographic proofs, and uniform labelling; prioritises safety and alignment research and development (e.g., reinforcement learning from AI feedback, post-training evaluations, and mechanistic interpretability) alongside public research institutes; and advances "AI for public good" through equitable access, improved public service delivery, workforce upskilling, and attention to environmental footprints. Framed for voluntary adoption by regulators and firms alike, the GenAI Framework is readily transposable to data-intensive domains such as soil information systems, where its emphasis on data quality, provenance, independent assurance, and clear user disclosures would materially strengthen the trustworthiness and local grounding of AI.

Regarding sustainability, the Framework acknowledges that generative AI entails significant energy and water consumption, with implications for climate objectives. It calls for coordinated action across the ecosystem to develop and deploy energy-efficient compute, track and measure the lifecycle carbon footprint of training and inference, and host AI workloads in data centres that apply best-in-class efficiency practices and utilise low-carbon energy sources or pathways. It assigns a primary role to AI developers and equipment manufacturers in conducting research and development on green computing techniques and in adopting energy-efficient hardware.

In January 2026, the Infocomm Media Development Authority introduced the Model AI Governance Framework for Agentic AI, the first comprehensive governance guide specifically addressing risks associated with agentic AI systems—AI systems capable of autonomously planning and executing multi-step tasks to achieve user-defined goals.[169] Like Singapore's earlier AI frameworks, the model remains voluntary but aims to help organisations manage regulatory exposure and legal accountability under existing laws. The framework identifies new risks arising from the increased

168 Allen et al. (2025); Avery Foundation (2024).

169 See https://www.eversheds-sutherland.com/en/global/insights/singapore-understanding-singapores-new-model-framework-for-agentic-ai-governance, accessed 15 March 2026.

autonomy of agentic systems, including erroneous or unauthorised actions, biased decision-making, data breaches, and disruptions to interconnected digital systems. To address these concerns, the guidance proposes governance measures across four key dimensions: assessing and bounding risks before deployment; ensuring clear human accountability and meaningful oversight; implementing technical safeguards such as testing, monitoring, and fail-safe mechanisms; and strengthening transparency and user responsibility through disclosure and training. The framework forms part of Singapore's broader "AI for Public Good" strategy and reflects the country's incremental, multi-layered approach to AI governance. Rather than imposing binding legislation, Singapore relies on voluntary governance frameworks, regulatory guidance, and industry standards to encourage responsible AI deployment while maintaining flexibility for innovation.

2.6.2.5. The USA's AI Action Plan

The US has so far favoured a market-led, sectoral patchwork: no comprehensive federal statute, a reliance on voluntary guidance and agency rules, and an increasingly uneven mosaic of state laws.[170] One of the most prominent soft-law initiatives is the Blueprint for an AI Bill of Rights, released in October 2022 by the White House Office of Science and Technology Policy.[171] The blueprint sets out five guiding principles intended to shape the responsible design, deployment, and governance of AI systems. These include the development of safe and effective systems, the protection of data privacy, notice and explanation when AI is used, safeguards against algorithmic discrimination, and the availability of human alternatives and oversight in high-stakes decisions. Although the Blueprint is non-binding, it has influenced federal procurement practices, agency risk assessments, and broader discussions on trustworthy AI governance. It reflects the US's broader regulatory philosophy, which relies on voluntary standards, sector-specific regulation, and public-private collaboration rather than comprehensive federal legislation.

On 23 July 2025, the Trump administration released a 28-page strategy, "Winning the Race: America's AI Action Plan", prepared pursuant to Executive Order 14179, which tasked presidential advisers to craft a roadmap to sustain and strengthen US leadership in AI in support of human flourishing, economic competitiveness, and national security.[172] The Action Plan itself is non-binding—it imposes no mandatory steps on agencies or the private sector—but outlines a comprehensive set of

170 See https://www.softwareimprovementgroup.com/us-ai-legislation-overview/, accessed 29 September 2025; Lousqui (2025).

171 See https://bidenwhitehouse.archives.gov/ostp/ai-bill-of-rights/, accessed 15 March 2026.

172 See https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf, accessed 29 September 2025.

recommended policy actions for federal departments across various domains. In parallel, President Trump issued three executive orders to operationalise the Plan's priorities: restricting federal procurement of "biased" AI models, streamlining permits for data centres and other AI infrastructure, and promoting an export strategy for US AI systems. Unlike the Plan, these orders create binding obligations for federal agencies. Taken together, the Action Plan and the accompanying orders constitute the administration's most precise and comprehensive AI policy guidance to date.

However, read as a whole, the Action Plan prioritises rapid deployment of AI infrastructure over environmental safeguards.[173] It recommends accelerated permitting by streamlining or reducing regulations under environmental laws and directs agencies to identify federal lands for large-scale data centre and generation projects. These measures de-prioritise soil stewardship—increasing the risk of soil sealing, erosion, and contamination—and are not consistent with a sustainability-oriented approach.

2.6.2.6. The UK's emerging AI framework

The UK has initially pursued a light-touch, sectoral approach to AI governance, relying primarily on existing regulatory frameworks rather than adopting a comprehensive AI statute.[174] In recent years, however, the UK has begun to move toward more structured regulation through a series of proposed and sector-specific laws.[175]

Several draft bills illustrate this shift. The Artificial Intelligence (Regulation and Workers' Rights) Bill (2023) focused on AI use in the workplace, proposing requirements for transparency, employee consultation, and safeguards against algorithmic discrimination, but it has not progressed through Parliament.[176] A broader Artificial Intelligence (Regulation) Bill introduced in 2024 proposes establishing a central AI Authority to coordinate regulators, promote regulatory sandboxes, and oversee accountability measures, such as appointing organisational AI officers and ensuring transparency regarding AI systems and training data.[177]

Additional legislative initiatives include the Public Authority Algorithmic and Automated Decision-Making Systems Bill (2024), which would require public authorities to conduct algorithmic impact assessments and publish transparency records before deploying automated decision systems.[178] In contrast to these horizontal proposals, the Automated Vehicles Act represents the UK's first enacted AI-specific

173 See https://diginomica.com/us-ai-action-plan-part-one-beware-its-local-and-environmental-consequences-warns-amc, accessed 29 September 2025.
174 Ritchie et al. (2025).
175 For a discussion, see Hilliard et al. (2026).
176 See https://www.tuc.org.uk/research-analysis/reports/artificial-intelligence-regulation-and-employment-rights-bill, accessed 20 March 2026.
177 See https://bills.parliament.uk/publications/59353/documents/6128, accessed 20 March 2026.
178 See https://bills.parliament.uk/bills/3760, accessed 20 March 2026.

legislation, focusing on the safety, licensing, liability, and oversight of autonomous vehicles.[179]

Despite these emerging initiatives, the UK's AI governance landscape remains fragmented. Existing laws—particularly data protection legislation—continue to serve as the primary enforcement mechanisms for AI-related harms, with regulatory actions largely led by the Information Commissioner's Office.[180]

2.6.2.7. South Korea's AI Basic Act

South Korea has adopted a comprehensive yet innovation-oriented approach to AI governance through the Framework Act on Artificial Intelligence Development and Establishment of a Foundation for Trustworthiness (AI Basic Act), which was enacted in December 2024 and entered into force on 22 January 2026.[181] Overseen by the Ministry of Science and Information and Communication Technology, the law establishes a national framework to promote AI development while ensuring safety, transparency, and public trust.

The Act adopts a risk-based governance model that applies to organisations whose AI activities affect South Korea, including foreign companies providing AI services to domestic users. Particular obligations apply to "high-impact AI" systems—those affecting sectors such as healthcare, transportation, energy, public administration, and biometric technologies.[182] Providers of such systems must implement risk management measures, disclose AI use, and may undergo voluntary inspections or certification mechanisms designed to strengthen trust. Generative AI services must also label AI-generated content and notify users when outputs are produced by AI systems.

Compared with the EU's regulatory framework, South Korea's approach is less restrictive and more innovation-focused.[183] Rather than imposing strict pre-market conformity assessments or prohibiting specific AI practices, the Act relies more heavily on post-market oversight, voluntary certification, and soft-law governance principles, while leaving low-risk AI largely unregulated. The law also incorporates industrial policy objectives, including regulatory sandboxes, research support, and infrastructure development to promote AI competitiveness.

Enforcement under the new framework is expected to remain relatively limited, with penalties capped at modest levels and a transitional grace period for

179 See https://www.legislation.gov.uk/ukpga/2024/10/contents, accessed 20 March 2026.
180 Unver & Odusola-Stevenson (2025).
181 For a discussion, see Hilliard et al. (2026).
182 See https://fpf.org/blog/south-koreas-new-ai-framework-act-a-balancing-act-between-innovation-and-regulation/, accessed 20 March 2026.
183 See https://www.theguardian.com/world/2026/jan/29/south-korea-world-first-ai-regulation-laws, accessed 20 March 2026.

compliance.[184] In practice, most AI-related enforcement actions have so far occurred under data protection law, overseen by the Personal Information Protection Commission.[185]

2.6.2.8. Brazil's emerging AI regulatory framework

Brazil has been among the first jurisdictions to explore comprehensive AI legislation. Since 2019, several bills have been introduced to establish principles and governance structures for artificial intelligence. Early proposals, including Bill No. 5051/2019 and Bill No. 21/2020, emphasised human dignity, privacy, transparency, and human oversight, seeking to ensure that AI systems enhance rather than replace human decision-making while safeguarding fundamental rights.[186] A subsequent proposal, Bill No. 872/2021, further highlighted principles such as autonomy, democratic oversight, bias prevention, and continuous risk management.[187]

The most advanced initiative is Bill No. 2338/2023, adopted in December 2024, which introduces a risk-based regulatory framework broadly comparable to the EU AI Act.[188] The law identifies a range of high-risk AI applications, including systems used in critical infrastructure, healthcare, employment decisions, credit assessment, biometric identification, law enforcement, migration management, and public administration. Providers of such systems must conduct impact assessments, implement risk management and data governance measures, ensure transparency, and comply with data protection legislation. The framework also prohibits certain high-risk practices, such as manipulative systems exploiting vulnerable groups or social scoring by public authorities.

The legislation includes enforcement mechanisms such as fines of up to 2% of annual revenue or R$50 million, as well as potential suspension of AI systems. However, enforcement activity in Brazil remains limited and has largely arisen under data protection law rather than AI-specific regulation.[189] Oversight by the Autoridade

184 See https://www.littler.com/news-analysis/asap/understanding-south-koreas-new-ai-law-key-considerations-multinational-employers, accessed 20 March 2026.

185 See https://iapp.org/news/a/south-korea-s-pipc-flexes-its-muscles-what-to-know-about-ai-model-deletion-cross-border-transfers-and-more, accessed 20 March 2026.

186 See https://www.holisticai.com/blog/brazil-ai-legislation-proposals, accessed 20 March 2026.

187 For a discussion, see Hilliard et al. (2026).

188 See https://www.holisticai.com/blog/brazil-ai-legislation-proposals, accessed 20 March 2026.

189 See https://cms.law/en/int/expert-guides/ai-regulation-scanner/brazil#:~:text=Brazil%20does%20not%20yet%20have,%2C%20security%20measures%2C%20and%20accountability, accessed 8 April 2026.

Nacional de Proteção de Dados (ANPD) has included actions against companies such as Meta for unlawful processing of personal data used to train AI systems.[190]

2.6.2.9. Russia's experimental approach to AI governance

Russia initially adopted a light-touch approach to AI governance, relying on national strategies and government initiatives rather than comprehensive legislation. Early policy measures included the Federal Programme on the Digital Economy of the Russian Federation and the National Strategy for the Development of Artificial Intelligence (2019), which set out long-term objectives to advance AI capabilities through 2030.[191] The strategy emphasises cooperation between government, industry, and scientific institutions while promoting principles such as security, human autonomy, risk-based regulation, and the prohibition of delegating morally responsible decisions to AI systems. Amendments introduced in 2024 further refined governance principles and expanded access to datasets—such as medical, anonymised personal, and industrial data—to support AI development.

In terms of legislation, Russia has primarily focused on regulatory sandboxes rather than broad horizontal regulation.[192] The 2020 Moscow experimental legal regime (Law 123-FZ) established a framework that allows companies to test AI technologies outside existing regulations for up to 5 years.[193] This initiative was expanded nationwide through the Experimental Legal Regimes in Digital Innovation Law (258-FZ) of 2021, enabling controlled experimentation with AI technologies in sectors such as healthcare, transportation, finance, and agriculture.[194] Amendments adopted in 2024 introduced additional safeguards, including mandatory civil liability insurance for participants testing AI systems within these experimental regimes.

Enforcement activity related to AI remains limited in Russia. Most regulatory activity focuses on experimentation and technology development rather than punitive oversight. However, recent policy proposals suggest a shift towards more assertive state control, with Russia considering sweeping powers to ban or restrict foreign AI tools that do not comply with domestic regulatory requirements, including data localisation and alignment with so-called "traditional values".[195]

190 See https://fpf.org/blog/processing-of-personal-data-for-ai-training-in-brazil-takeaways-from-anpds-preliminary-decisions-in-the-meta-case/#:~:text=The%20ANPD%20issued%20a%20preventive,suspension%20of%20that%20processing%20activity, accessed 20 March 2026.

191 For a discussion, see Hilliard et al. (2026).

192 See https://law.asia/russia-ai-regulations-legal-framework-ethics/, accessed 20 March 2026.

193 See https://regulations.ai/regulations/RAI-RU-MO-FN1A2XX-2020, accessed 20 March 2026.

194 Mamina & Kobzeva (2021).

195 See https://www.reuters.com/business/russia-give-itself-sweeping-powers-ban-or-restrict-foreign-ai-tools-2026-03-20/, accessed 20 March 2026.

2.6.3. The international level

International debates on AI governance have accelerated in recent years, but binding global rules remain elusive.[196] Instead, the landscape is marked by non-binding principles, regional strategies, and fragmented bilateral initiatives.[197] For soil governance, this fragmentation creates uncertainty, as soil-related AI tools may be subject to inconsistent standards depending on where they are deployed. Notably, the OECD has proposed creating an international intergovernmental body, comparable in structure and mandate to the Intergovernmental Panel on Climate Change (IPCC), tasked with monitoring global AI developments, producing regular assessments, and making its analyses publicly accessible to policymakers and civil society alike. Such a body could provide the much-needed epistemic authority and shared evidence base to counteract fragmentation and build trust in global governance processes.[198]

The Council of Europe Framework Convention on AI (2024) is the most advanced initiative to date, developed under the auspices of the Council of Europe—a regional organisation distinct from, but overlapping with, the EU. The Convention represents the first attempt to establish binding international standards on AI governance, focusing on human rights, democracy, and the rule of law. However, it has not yet secured the necessary number of ratifications to enter into force. It was formally opened for ratification in September 2024.[199] To date, signatories include the EU, the UK, Canada, Georgia, Japan, and the US. In terms of its stated purpose, Article 1 of the Convention affirms that the design, development, and deployment of AI systems across their entire lifecycle must be "fully consistent with human rights, democracy, and the rule of law."[200]

On 10–11 February 2025, the second AI Summit was co-hosted by France and India, bringing together representatives from over 100 countries, as well as civil society, the private sector, and research institutions. The meeting concluded with the adoption of the *Statement on Inclusive and Sustainable Artificial Intelligence for People and Planet*. Signed by approximately sixty states, including China, the statement underscored the "importance of reinforcing the diversity of the AI ecosystem". It affirmed the need to continue multisectoral dialogue, with clear priorities and next steps. It also stressed that effectively harnessing AI's benefits will depend fundamentally on "trust and safety." Notably, Russia, the UK, and the US did not sign the statement.[201]

196 Ginzky & Ruppel (2025a: 264).
197 WTO (2024).
198 Ibid.
199 See https://www.elysee.fr/en/sommet-pour-l-action-sur-l-ia, accessed 29 September 2025.
200 Council of Europe Treaty Series - No. 225, Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (2024), available at https://rm.coe.int/1680afae3c, accessed 7 April 2026.
201 See https://www.elysee.fr/en/emmanuel-macron/2025/02/11/statement-on-inclusive-and-sustainable-artificial-intelligence-for-people-and-the-planet, accessed 29 September 2025.

Despite divergent approaches, a standard set of values is gaining traction. These principles were first advanced in academic circles[202] and subsequently developed under the auspices of international organisations such as the World Trade Organisation (WTO),[203] the OECD,[204] and the United Nations.[205] A notable example is the set of principles adopted by UNESCO in November 2021, which articulate core values to guide the development and deployment of AI. These include:[206] proportionality and "do no harm"; fairness and non-discrimination; transparency and explainability; human oversight and accountability; privacy and data protection; sustainability and climate responsibility; multi-stakeholder governance.[207]

One complementary proposal is Public Constitutional AI: instead of leaving "AI constitutions" to engineers or vendors, a jurisdiction would run a participatory process (including citizens' assemblies, public comment, civil-society input, and expert input) to draft a binding set of principles for high-risk and frontier systems.[208] Providers must train, fine-tune, and audit models against this public constitution, publish "constitutional audit" reports and failure cases, and offer contestability rights (including explanations, appeals, and remedies) to affected individuals. Regular reviews (e.g., every two to three years) update the rules as risks evolve. This shifts legitimacy from private policy to public law—tackling opacity and ensuring that AI used in soil governance and SSM aligns with locally endorsed rights and values.

On 18 August 2025, the UN General Assembly created two new mechanisms: the Global Dialogue on AI Governance and the Independent International Scientific Panel on AI. The Global Dialogue will convene annually (two days) to bring governments and stakeholders together to address the development of safe, secure, and trustworthy AI; promote interoperability and compatibility among national and regional governance approaches; ensure robust human oversight consistent with international law; and advance open-source software, open data and open AI models.[209] The Panel—a 40-member, multidisciplinary, geographically diverse body—will advise the UN on AI's opportunities, risks, and impacts, produce a flagship annual study, and serve as the expert engine that feeds analysis and options into the Global Dialogue. Although non-binding, these forums can set influential soft-law benchmarks—on transparency, auditability, and data governance—that will shape procurement terms, donor

202 Okolo et al. (2023) with further references.
203 Ruppel (2022b); WTO (2024).
204 OECD (2024a).
205 See https://unsceb.org/principles-ethical-use-artificial-intelligence-united-nations-system, accessed 29 September 2025.
206 See UNESCO (2021: 10). UNESCO clearly stated that the scope of application only refers to the mandates and tasks of UNESCO.
207 Ibid.: 20–25.
208 Abiri (2024).
209 UNGA A/79/L.118, 'Terms of reference and modalities for the establishment and functioning of the Independent International Scientific Panel on Artificial Intelligence and the Global Dialogue on Artificial Intelligence Governance' (18 August 2025).

conditionalities and domestic rulemaking. They offer African states and other Global South actors a venue to press for standards on locally representative training data for agricultural AI, protections for soil and farm data sovereignty, requirements for explainability ('black-box' mitigation), and attention to sustainability costs (energy and water use of AI infrastructures). Properly leveraged, the Dialogue and Panel could help align AI deployment in SSM with principles of equity, accountability and environmental stewardship.

From the AU Continental Artificial Intelligence Strategy (2024),[210] the UNESCO Recommendation on the Ethics of Artificial Intelligence,[211] and the Windhoek Statement on Artificial Intelligence in Southern Africa,[212] the following overlapping and mutually reinforcing principles emerge:

- Principle of Foundational Data Governance. AI systems are built on data, making their governance a central concern. This goes beyond mere collection to encompass questions of quality, ethics, and relevance. To be effective, data must be high-quality, inclusive, and locally grounded, so that AI solutions can avoid bias and remain applicable in African contexts. Equally important is the ethical and secure sharing of data, guided by robust frameworks that protect against misuse. At the same time, there is growing momentum toward openness—establishing trustworthy "gold standard" datasets, shared repositories, and a broader digital commons that can foster innovation while safeguarding legal and ethical standards.
- Principle of Rights-Based Protection and Agency. This principle centres on the individual, ensuring that the development of AI does not come at the expense of fundamental human rights. Legislative frameworks must embed privacy by design, requiring impact assessments, transparency, and independent oversight so that individuals remain in control of their personal data. Equally vital are safeguards to prevent harm, particularly in high-risk applications such as facial recognition and in handling sensitive biometric, genetic, or health data. Ultimately, protecting data subject rights, including the ability to access, correct, or delete personal information, remains a non-negotiable cornerstone of responsible AI governance.
- Principle of Contextual and Africa-Centric Innovation. AI must be designed for and by Africa, reflecting the continent's unique realities, challenges, and opportunities. Innovation should be channelled toward solving pressing regional issues such as health, agriculture, and climate change, rather than importing models that lack local relevance. This also requires valuing and integrating indigenous knowledge systems, ensuring that technologies resonate

210 AU (2024b).

211 See https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence, accessed 29 September 2025.

212 See https://unesdoc.unesco.org/ark:/48223/pf0000383197, accessed 29 September 2025.

with cultural and ecological contexts. Equally important is the pursuit of technological sovereignty: building local capacity so that Africa becomes not only a consumer but also a producer and shaper of AI, thereby safeguarding its digital future.

- Principle of Inclusive and Equitable Development. This principle seeks to ensure that the benefits of AI are distributed fairly and that no one is left behind. Bridging the digital divide requires active investment in foundational infrastructure such as electricity, connectivity, and data centres, particularly in rural and disadvantaged areas. Equally important is advancing gender equality and inclusion through gender-responsive policies, promoting women in STEM fields, and safeguarding against algorithmic biases that risk marginalising vulnerable groups. Finally, capacity-building efforts must prioritise youth, women, and other marginalised communities, enabling their full participation in the AI ecosystem and ensuring that digital transformation fosters equity rather than exclusion.
- Principle of Capacity and Ecosystem Building. Sustainable AI development requires holistic investment in human capital, infrastructure, and supportive environments. Education and literacy are foundational, ranging from broad public awareness campaigns to advanced academic programmes and dedicated centres of excellence. At the same time, infrastructure investment, particularly in computing capacity, green data centres, and high-performance computing, must be treated as essential rather than optional. Equally critical is support for innovation, through incubators, hubs, and creative funding mechanisms that can nurture start-ups and stimulate digital entrepreneurship across the continent.
- Principle of Proactive and Adaptive Governance. The fast pace of AI demands governance that is both anticipatory and flexible. Policymaking must look ahead to identify potential risks and opportunities, rather than merely reacting to harms that have already occurred. Legal and regulatory frameworks should also be regularly reviewed and revised to ensure they remain responsive to rapid technological change. Ultimately, effective governance requires genuine multi-stakeholder collaboration among governments, the private sector, civil society, and academia to balance innovation, accountability, and the public interest.
- Principle of Regional Collaboration and Global Partnership. No single country can manage the challenges of AI governance in isolation. This principle emphasises the importance of unity and active engagement on the global stage. Cross-border harmonisation is vital, with interoperable standards and regional policy alignment enabling collaboration and scale. At the same time, global engagement must ensure that African voices and expertise are meaningfully represented in international AI governance forums, shaping norms rather than

passively receiving imposed solutions. Shared resources, such as collaborative platforms, secure data sharing, and the exchange of best practices, are equally essential for building trust and strengthening collective capacity across borders.

Taken together, these principles move away from a purely technocratic view of AI. They advocate for a model where AI is a tool for sustainable development rather than just profits or surveillance; rooted in ethical values and human rights from its inception; built on a foundation of sovereignty and self-determination, ensuring Africa controls its own digital destiny; and inclusive by design, aiming to reduce existing inequalities rather than exacerbate them.

This framework presents a vision of AI that is not merely adopted from elsewhere but is consciously and deliberately built to serve the specific needs and values of the African continent and similar regions.

3. Africa, digital colonisation, and the struggle for soil data sovereignty

3.1. Dependency, surveillance, and exclusion

"The future is already here – it's just not evenly distributed."[213] This aphorism captures Africa's position in the global digital economy: on the cusp of technological transformation, yet at risk of repeating historical patterns of extraction and dependency. AI and digitalisation hold immense potential for soil protection and SSM. Still, without adequate governance, they may entrench inequalities and strip communities of their most fundamental resource. Nowhere is this tension more visible than in the treatment of soil data.

A cautionary parallel is Senegal's "Akon City": an American-owned USD 6 billion venture marketed in 2018 as a tech-utopian hub that would deliver jobs, hospitals, and "smart" infrastructure. However, it required large tracts of land near Mbodiène, with residents either relocated or pressured to relinquish their land amid disputes over compensation.[214] Years later, little of the promised city materialised, and in 2025, authorities pivoted away from the plan. The arc is familiar in AI rollouts: grand narratives of transformation justify displacement and private control, while local communities absorb the risks and costs.

Data derives value from use, not mere volume.[215] Its worth often rises combinatorially when linked with other datasets—becoming greater than the sum of its parts.[216]

213 See https://www.goodreads.com/quotes/681-the-future-is-already-here-it-s-just-not-evenly, accessed 29 September 2025.
214 See https://www.bbc.com/news/articles/c8xvrv21drjo, accessed 29 September 2025.
215 OECD/WTO (2025: 12).
216 Ibid.

Data also carries both inherent and option (potential) value: information unused today may be strategically valuable tomorrow. Because data is non-rivalrous and can be copied and shared at near-zero marginal cost, multiple actors can reuse it simultaneously for diverse purposes, multiplying its overall utility.[217] Soil data occupies a complex and ambiguous position in law and governance. By itself, it is often considered "non-personal." Yet once linked to geolocation coordinates, ownership records, or farm identifiers, it becomes sensitive, even personal information. This legal ambiguity is not merely theoretical. Decades of data governance experience demonstrate that datasets deemed "anonymised" or "non-personal" can often be re-identified with minimal auxiliary information. Classic examples from health and consumer data illustrate how cross-referencing supposedly de-identified datasets with publicly available records can accurately identify individuals.[218] These cases underscore a structural weakness in data protection regimes that rely on formal anonymisation while ignoring linkage risk and data aggregation dynamics.

Farmers across Africa often unknowingly surrender their data rights, which are frequently hidden in the fine print of contracts with agribusinesses or technology firms.[219] These contracts usually assign ownership of valuable datasets to multinational corporations, giving them disproportionate control over agricultural markets, credit systems, and even input supply chains.[220] The problem of data colonialism would intensify under such arrangements: when a handful of platforms control farm and soil data, producers lose any real say over how it is used or who captures the gains. The result is a kind of digital feudalism—value created by land and farmers' labour is siphoned off and concentrated in the hands of platform owners.[221] Instead of democratising information and empowering growers, AI is being harnessed to enforce enclosure, lock-in, and corporate extraction.

In practice, soil data is treated as a commodity, traded and monetised far from the fields where it originates. The African data centre market is projected to exceed USD 5 billion by 2026, but most facilities remain under foreign ownership.[222] The result is a widening gap in digital sovereignty that mirrors—and risks deepening—the North–South divide. The asymmetry in bargaining power leaves farmers with little capacity to negotiate terms or benefit from the economic value of their data. This imbalance raises fundamental questions of justice, sovereignty, and control over Africa's digital future. Scholars increasingly describe this situation as digital colonisation: the decentralised extraction and control of citizens' data, often without their explicit consent,

217 Ibid.
218 Cajueiro & Celestino (2026: 81).
219 Wiseman et al. (2019).
220 Lawyers Hub (2024).
221 See https://prism.sustainability-directory.com/scenario/algorithmic-bias-in-soil-health-management-systems/, accessed 29 September 2025.
222 See https://onixdatacentres.com/2024/05/07/data-centre-innovations-africa-adca-report/, accessed 29 September 2025.

through networks owned and operated by foreign technology companies.[223] It is not limited to Western firms. Chinese companies, too, have become central actors, introducing new forms of dependency.

In 2021, China's AI market was valued at roughly USD 23.196 billion, with projections of about USD 61.855 billion by 2025.[224] Between 2000 and 2014, China undertook digital projects in 44 African countries, with approximately half of these projects concentrated in Nigeria, Ethiopia, and Zimbabwe.[225] Over the past two decades, Huawei is estimated to have built around 50% of Africa's 3G networks and 70% of its 4G networks, deepening Chinese firms' embedment in the continent's information infrastructure.[226] Currently, more than 266 China-backed technology initiatives operate in Africa, many of which involve AI-related deployments, such as 5G infrastructure, data centres, smart-city platforms, and surveillance systems.[227] Hikvision opened a Johannesburg office and, via a local partner, deployed roughly 15,000 surveillance cameras across the city in 2019.[228] In 2021 alone, China reportedly earmarked USD 8.43 billion for Africa-focused digital and AI initiatives spanning high-performance computing, big data, the Internet of Things, AI, blockchain, quantum computing, cross-border e-commerce, smart cities, telemedicine, and internet finance.[229]

Therefore, the risk of dependency is not hypothetical. In 2016, for example, Facebook announced plans to build population-density maps for much of Africa using computer vision, population data, and high-resolution satellite imagery. Framed as "creating knowledge about Africa's population distribution," "connecting the unconnected," and "enabling humanitarian aid," the project effectively positioned a private platform as the authority over what counts as legitimate demographic knowledge.[230] In 2018, the Chinese AI start-up CloudWalk Technology signed an agreement with Zimbabwe to provide facial recognition systems. In exchange, Zimbabwe's citizens became a testing ground for algorithmic training datasets. Marketed as "win–win cooperation," the deal exemplified how access to African data can advance foreign technology while leaving African governments dependent on imported tools.[231] Since 2020, Google has invested over USD 200 million in AI-driven social initiatives worldwide, focusing on addressing challenges such as wildfires, hunger, and public health emergencies.[232] In July 2025, it opened an AI Community Centre in Ghana to foster local innovation and

223 Png (2022); Salami (2024).
224 Tinarwo & Babu (2023: 3).
225 Ibid.: 6.
226 Ibid.
227 Ibid.
228 Gravett (2022: 6).
229 Tinarwo & Babu (2023: 7).
230 Birhane (2020).
231 Travers (2024).
232 See https://restofworld.org/2025/africa-ai-for-good-big-tech/, accessed 29 September 2025.

pledged an additional USD 37 million to "AI for Good" projects across Africa.[233] Other major technology companies, including Microsoft, Meta, Amazon, and Apple, are pursuing similar ventures. McKinsey & Company estimates that the widespread adoption of generative AI in Africa could generate up to USD 100 billion in annual economic value across sectors.[234] Google currently operates two AI laboratories on the continent, located in Accra, Ghana, and Nairobi, Kenya. From these hubs, at least three models have been released addressing climate change, public health, and urban planning. Its global hydrological model, for instance, utilises satellite data to forecast floods up to seven days in advance, covering approximately 460 million people across 41 African countries.[235] In March 2025, Google launched MetNet in Nairobi—an AI-powered precipitation-forecasting tool available through Google Search—that helps farmers make crucial decisions, such as timing fertiliser applications to avoid rainfall losses.[236] Chinese Agricultural Technology Development Centres have become flagship aid projects, with 23 now operating across Africa, initially financed by China's Ministry of Commerce.[237] In Zambia, the Sunagri Investments–run centre showcases "smart farming" tools such as drones.[238] China has also donated five plant-protection drones to Zambia to help raise agricultural productivity.[239]

Yet while these initiatives are presented as serving the public good, they also consolidate corporate influence over vulnerable communities. Microsoft's Project Ellora, for example, has faced scrutiny in India for using rural labourers to collect speech data, despite their limited access to smartphones or the internet and the unlikelihood that they would benefit from the resulting technology.[240] Similarly, in Argentina, the company drew backlash for gathering personal data from young girls in Salta province under the pretext of predicting teenage pregnancies years in advance.[241] In Africa, too, the billions poured into cloud data centres, undersea cables, and startup ecosystems

233 See https://www.connectingafrica.com/ai/google-commits-37m-to-advancing-ai-in-africa, accessed 29 September 2025.

234 See https://www.mckinsey.com/capabilities/quantumblack/our-insights/leading-not-lagging-africas-gen-ai-opportunity, accessed 29 September 2025.

235 See https://blog.google/intl/en-africa/company-news/outreach-and-initiatives/5-ways-were-bringing-ai-innovations-to-people-across-africa/#:~:text=Forecasting%20floods%20up%20to%207%20days%20in%20advance&text=Google%20Research's%20global%20hydrological%20AI,460M%20people%20across%20the%20continent, accessed 29 September 2025.

236 See https://medium.com/@FromLagosto/googles-ai-forecasts-rain-for-africa-a-game-changer-in-weather-prediction-567b5c8f02eb, accessed 29 September 2025.

237 See https://www.iied.org/chinese-engagement-african-agriculture-not-what-it-seems, accessed 30 October 2025.

238 See https://chinaglobalsouth.com/analysis/case-study-chinese-agricultural-firm-uses-drones-to-fight-pests-in-zambia/, accessed 30 October 2025.

239 See http://www.china.org.cn/world/Off_the_Wire/2025-03/19/content_117775557.htm, accessed 30 October 2025.

240 See https://restofworld.org/2025/africa-ai-for-good-big-tech/, accessed 29 September 2025.

241 See https://notmy.ai/news/case-study-plataforma-tecnologica-de-intervencion-social-argentina-and-brazil/, accessed 29 September 2025.

should not be mistaken for altruism. Training local developers or expanding internet access through ventures such as Starlink may increase connectivity, but it also binds users to corporate platforms where alternatives are scarce. It is the digital equivalent of building a highway into a remote town and then charging a toll for every car: the infrastructure is valuable, but the toll—continuous dependence on proprietary systems—is the real business model.[242]

At the agricultural level, smallholder farmers, who form the backbone of African food systems, often cannot access digital tools that require costly hardware, broadband internet, or advanced literacy.[243] Even when technology arrives, it is frequently introduced through "doing good in Africa" programmes in which a major tech company sponsors apps, sensors, or platforms for local communities. For example, in recent years, pesticide and fertiliser companies have rolled out a surge of mobile "decision-support" apps for farmers—purporting to advise on what to plant, how much to spray, and when to harvest.[244] The offer looks generous and is gratefully accepted. Still, the hidden price is data extraction: the company harvests farm- and community-level data at scale, which then feeds its proprietary products and markets—the real money lies in the data, not the donation. These tools are also commonly bundled with input packages supplied by the same corporations that own the data and algorithms, creating lock-in to closed ecosystems that tilt the playing field against local innovators and turn farmers into data providers without informed consent, benefit-sharing, or data-sovereignty protections. Meanwhile, governments struggle to regulate technologies and cross-border data flows that evolve far faster than legislative processes.

In data-rich regions and on capital-intensive farms, technology providers can harvest large volumes of high-frequency information, including regular soil assays, plot-level field trials, yield monitors on new tractors, drone imagery, and in-field sensor streams.[245] They train algorithms on these datasets and market highly granular prescriptions for fertiliser rates, pesticide applications, and harvest timing. The predominance of monocropping on such operations further simplifies modelling and narrows uncertainty, making optimisation comparatively straightforward. Smallholders face the inverse conditions. Decades of structural adjustment have hollowed out public extension across much of the Global South, leaving little coordinated collection of field data. Most small farms cannot afford the machinery and sensors that feed commercial platforms. The result is sparse, noisy, and uneven datasets, from which providers can draw only low-quality inferences. Models trained primarily on data from large, monocropped systems then generalise poorly to diverse, intercropped, or rain-fed smallholder contexts—producing advice that is at best irrelevant and at worst harmful, while

242 See https://medium.com/woza-business/africa-rising-or-africa-exploited-big-techs-world-domination-plan-0c41dc1024ed, accessed 29 September 2025.

243 Abdulai et al. (2023).

244 See https://grain.org/en/article/6595-digital-control-how-big-tech-moves-into-food-and-farming-and-what-it-means, accessed 29 September 2025.

245 See https://www.myfarmweb.com/.

deepening existing inequalities in access to agronomic knowledge and digital services.[246]

For Africa, digital sovereignty is inextricably linked to soil sovereignty. Soils underpin food security, livelihoods, and resilience to climate change, yet they are under mounting pressure from erosion, nutrient depletion, desertification, and competing land uses. AI is often presented as a way for Africa to leapfrog developmental constraints by providing tools such as digital soil maps, predictive modelling, and precision agriculture systems. These could indeed optimise fertiliser use, conserve water, and provide early warnings of soil degradation.[247] There are promising soil- and agriculture-focused initiatives, such as Nuru, which was developed in collaboration with Tanzanian farmers. This initiative utilises a mobile app that functions offline to detect cassava plant diseases, safeguarding a staple crop for over 500 million people.[248] Then there is AI Farmer (formerly Hi Saai) in South Africa, which provides digital extension services that bridge access gaps for smallholder farmers.[249] Around 100 AI start-ups have been established, attracting over USD 140 million in seed funding, primarily concentrated in Nigeria's fintech sector.[250] South Africa leads in AI start-ups, followed by Nigeria and Kenya. Africa's first AI factory—a collaboration between Cassava Technologies and Nvidia—is being built in South Africa, with further facilities planned across Kenya, Nigeria, Morocco, and Egypt.[251] Still, the advancement and rollout of AI technologies remain highly uneven globally, with a pronounced divide between developed and developing countries.[252]

These examples demonstrate the potential of locally adapted AI, particularly when designed for accessibility and offline use. Yet they remain exceptions in an ecosystem dominated by multinational corporations. The contrast is instructive: while local initiatives show what is possible, the prevailing reality is that most farmers continue to face deep-seated concerns about trust, ownership, and control of their data. Farmers consistently express mistrust of digital service providers, citing issues such as:[253] lack of clarity around ownership and use of data collected through farm machinery and smart farming tools; risk of farms being re-identified by combining de-identified datasets with satellite imagery and government soil maps; fears that soil data on carbon content, fertiliser use, or biodiversity could lead to taxation, regulation, or negative consumer perceptions. Attitudes often differ when data is shared with government

246 See https://grain.org/en/article/6595-digital-control-how-big-tech-moves-into-food-and-farming-and-what-it-means, accessed 29 September 2025.
247 Castro et al. (2024); Kumar et al. (2024); Awais et al. (2023).
248 Arakpogun et al. (2021).
249 See https://saai.org/en/saai-launches-artificial-intelligence-platform-for-family-farmers/, accessed 29 September 2025.
250 Arakpogun et al. (2021).
251 See https://iafrica.com/africas-first-ai-factory-underway-as-cassava-and-nvidia-deploy-3000-gpus-in-south-africa/, accessed 29 September 2025.
252 Arakpogun et al. (2021).
253 Chichaibelu et al. (2023).

agencies, academic researchers, or private companies, reflecting different levels of trust and perceived risk.[254]

Consent cannot be meaningful if farmers do not understand the potential uses of their data or lack the ability to enforce their rights. Agricultural data has increasingly become a valuable asset and tradable commodity.[255] The way in which benefits and risks are distributed during this technological transition is primarily shaped by who controls the data and determines its uses.

Beyond individual datasets, there is significant power in data aggregation at scale. At present, this concentration of value primarily resides with powerful corporate actors—not only in the agricultural input and farm machinery industries, but also within the broader sphere of "Big Tech.".[256] Digital technologies will only benefit farmers if they have both access to the data and the capacity to influence its governance, that is, to decide how the data may be used, by whom, and for what purposes. Certain types of agricultural data, such as income or household information, are highly sensitive and require stringent safeguards. Others, such as weather records, are generally not viewed as problematic when shared publicly.[257]

Ensuring that data ownership contributes to data justice requires more than formal rights on paper. It must be coupled with capacity-building for farmers and workers to understand their entitlements, as well as structural enforcement mechanisms.[258] Otherwise, the prevailing system continues to place the burden of privacy protection on the individual "data subject"—the farmer or worker—who often lacks the time, expertise, or resources to navigate and exercise these rights.[259]

3.2. The South African example

South Africa offers a microcosm of the challenges surrounding agricultural and soil data governance in Africa. There is no single regulator for soil data; instead, governance is shaped indirectly by multiple laws and regulations. At the highest level, the Constitution of 1996 establishes rights that frame the use of data: the privacy rights (Section 14), dignity (Section 10), equality (Section 9), freedom and security (Section 12), access to information (Section 32), and freedom of expression, including scientific research (Section 16). The Constitutional Court has emphasised that privacy safeguards a "sphere of private intimacy and autonomy without interference," though this sphere is limited.[260] These values, combined with the Constitution's supremacy

254 Ruder & Wittman (2025).
255 Uyar et al. (2024).
256 Ruder & Wittman (2025).
257 Ibid.
258 Barton et al. (2025).
259 Ruder & Wittman (2025).
260 *Botha v Smuts* [2024] ZACC 22 (9 October 2024) at para 84.

(Section 2) and commitment to the rule of law, provide the foundation for regulating personal and environmental data, including soil data.

At the regional level, the Southern African Development Community (SADC) Model Law on Data Protection provides a valuable point of comparison.[261] Under the Model Law, soil data classification depends on whether it is linked to identifiable individuals or communities. Purely environmental information, such as soil chemistry, moisture levels, or erosion risk, typically does not qualify as personal data. However, when soil data is tied to farmers, households, or communal tenure systems through GPS coordinates or land records, it falls within the scope of personal data. It must be processed lawfully and fairly, with the consent of those affected. The Model Law also permits collection without consent where it serves the public interest, scientific research, or environmental protection, provided that safeguards are in place. In principle, this enables large-scale soil monitoring for climate change adaptation or food security, provided it is overseen by a competent authority to ensure transparency and accountability. Importantly, anonymisation and aggregation are framed as key tools for balancing governance needs with the rights and expectations of farmers and communities.

South Africa's domestic regime, however, reveals the gaps between regional aspirations and national implementation. Environmental statutes, such as the National Environmental Management Act 107 of 1998 (NEMA), regulate access to and the protection of ecological information. Yet soil data remains uncoordinated and scattered across government departments, universities, agribusinesses, and international organisations, with accessibility varying from open access (government/research) to restricted proprietary use (private firms). The Protection of Personal Information Act (POPIA) 4 of 2013, which has been in force since July 2021, is South Africa's primary data protection law. While POPIA protects the processing of personal information of natural and juristic persons, it does not expressly regulate non-personal data such as soil metrics.[262] Nevertheless, soil data linked to identifiable farmers or landowners may indirectly fall under its scope.

The Electronic Communications and Transactions Act 25 of 2002 (ECTA) is South Africa's primary statute governing electronic communications and e-commerce, designed to prevent abuses in the digital environment. Section 20 specifically addresses "automated transactions," i.e., contracts concluded where one or both parties use an automated system. It confirms that a binding agreement—and corresponding contractual rights—arises upon the conclusion of such a transaction, and that the parties are bound even if they did not personally review the system's actions. Section 20 also provides that a material error in an automated transaction can render the

261 See https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf, accessed 29 September 2025.

262 Coetzee (2024).

agreement void, subject to specified conditions. Accordingly, contracts formed using AI as an electronic agent fall within Section 20's scope and protections.

POPIA lays down eight conditions for lawful processing: accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards, and data subject participation. Farmers must provide consent, be notified of the collection, and retain the right to access or correct their information. The Act also regulates automated decision-making (Section 71), prohibiting legally consequential decisions based solely on automated processing unless contractual or legal safeguards are in place to ensure fairness and transparency.

Under Section 72, a responsible party may transfer personal information to a foreign country only where a lawful transfer basis exists. This is satisfied if the foreign recipient is subject to a law, binding corporate rules, or a contract that affords an adequate level of protection—i.e., provisions substantially similar to POPIA's conditions for lawful processing and to Section 72's onward-transfer restrictions. Alternatively, a transfer may proceed with the data subject's consent; where it is necessary for performance of a contract with the data subject (or pre-contract measures at their request); where it is necessary for the conclusion or performance of a contract in the data subject's interests between the responsible party and a third party; or, in limited cases, where the transfer is for the data subject's benefit and it is not reasonably practicable to obtain consent, but the data subject would likely have consented.

Yet vague wording leaves key questions unresolved: Is human confirmation after an automated decision sufficient?[263] What transparency obligations apply? Compounding this, POPIA does not obligate decision-makers to notify data subjects when automated decisions are made, making enforcement of rights difficult.[264]

AI systems often transform the data they ingest—reconstructing it into latent features, combining it with other sources, and continuously updating models—thereby limiting organisations' oversight of how the information they collected is modified and reused. The opacity of these processes makes it hard for individuals to understand how their data is being used, undermining meaningful notice and informed consent.[265]

This weakness reflects broader structural concerns. POPIA deliberately avoids regulating ownership.[266] A defensible view is that a newly created piece of digital information comes into being ownerless (*res nullius*). Its original acquisition occurs by appropriation/occupation: the first person who both intends to own it and exercises effective control over it becomes its owner, meaning universities, agribusinesses, or technology firms can establish control and claim ownership.[267] Ownership rights then

263 Davis & Trott (2024).

264 See https://www.derebus.org.za/has-popia-adequately-prepared-people-to-exercise-their-right-not-to-be-subject-to-automated-decision-making/, accessed 29 September 2025.

265 Davis & Trott (2024); Mbonye / Moodley / Nyika (2024).

266 Thaldar (2025); See https://theconversation.com/who-owns-digital-data-about-you-south-african-legal-scholar-weighs-up-property-and-privacy-rights-249741, accessed 29 September 2025.

267 Ibid.

enable data to be licensed or monetised as an economic asset, often without reciprocal benefit to the farmers or communities who generated the underlying information. Put differently, on a property view, a new instance of personal information can be owned, but not necessarily by the data subject. The party best placed to acquire ownership is the one on whose device the information is first recorded (i.e., tech company), since that party exercises control from the outset and needs only the intention to own to acquire title.[268]

This is particularly concerning in light of recent research that found existing mechanisms in data protection law (e.g., the right of access to information, as provided for in Section 5(g) of POPIA) ineffective for determining how a data subject's personal information is used in automated processing.[269] The research found that some of the largest companies are unable to provide meaningful responses to data subjects' requests to understand whether and how their personal information is used in automated processing and whether this is in line with the provisions of POPIA.

South Africa has begun to grapple with these gaps through broader digital and AI policy initiatives. Key developments include:

- AI Governance: Establishment of the Fourth Industrial Revolution (4IR) Commission (2019),[270] AI Institute of South Africa (2022),[271] and the draft National AI Plan (2024).[272]
- Research Oversight: The Academy of Science of South Africa (ASSAf) Code of Conduct for Research, initially developed for approval by the Information Regulator, has since been reconstituted as a voluntary POPIA Compliance Framework following regulatory feedback.[273] While not formally adopted as a binding code, it remains an important governance instrument that complements POPIA in guiding research activities in South Africa, including the sharing of data with international collaborators.[274]
- National AI Policy Framework (2024): Nine strategic pillars, including ethical AI, transparency, fairness, privacy, and bias mitigation.[275]

268 Ibid.
269 Davis et al. (2022).
270 See https://www.gov.za/news/media-statements/president-cyril-ramaphosa-appoints-commission-fourth-industrial-revolution-09, accessed 27 October 2025.
271 See https://aii-sa.co.za/, https://www.cair.org.za/, accessed 27 October 2025.
272 See https://www.michalsons.com/focus-areas/artificial-intelligence-law/national-ai-policy-guidance-and-overview, https://www.ppmattorneys.co.za/south-africas-draft-national-ai-plan/, https://www.werksmans.com/legal-updates-and-opinions/the-ai-national-policy-south-africas-initial-step-to-establish-an-ai-policy-and-regulatory-framework/, accessed 27 October 2025.
273 Gooden & Thaldar (2024).
274 Academy of Science of South Africa (2025:4).
275 See https://www.dcdt.gov.za/sa-national-ai-policy-framework/file/338-sa-national-ai-policy-framework.html, accessed 27 October 2025.

- National Data and Cloud Policy (2024): Promotes data sovereignty, cloud security, and digital transformation.[276]
- On 3 December 2024, during its G20 presidency, South Africa launched a Task Force on AI, Data Governance, and Innovation for Sustainable Development.[277]
- The Department of Communications and Digital Technologies has submitted the Draft National AI Policy to Cabinet for approval and gazetting in South Africa, with publication anticipated in March 2026.[278] Following approval and official gazetting, the Draft AI Policy will be released for public consultation. The government has adopted a sector-specific, multi-regulator approach rather than establishing a single dedicated AI authority, thereby embedding AI governance within existing regulatory frameworks.[279] The policy is structured around six core pillars aimed at promoting the responsible development and ethical deployment of AI: capacity and talent development; AI for inclusive growth and job creation; responsible governance; ethical and inclusive AI; cultural preservation and international integration; and human-centred deployment.

The above was merely a brief explanation of the problem, using South Africa as an example, but AI regulation in Africa is severely lacking.

Scholars have noted that the rise of digital technologies has placed significant pressure on international human rights law, as existing legal frameworks were not designed to address data-driven surveillance, profiling, and automated decision-making.[280] Rather than negotiating new binding treaties, regulators and courts have largely responded by stretching existing norms of international human rights law through dynamic interpretation, applying established rights—such as privacy, dignity, autonomy, and equality—to new technological contexts.[281] This strategy has produced a fragmented and uneven protective landscape. On the one hand, many digital risks have been addressed through legal regimes that sit outside international human rights law, including data protection, consumer protection, and administrative law.[282] While these frameworks offer important procedural safeguards, they are typically individualised, sector-specific, and weakly enforced, and they struggle to address structural power asymmetries or collective harms. On the other hand, courts have sought to integrate

276 See https://www.michalsons.com/blog/south-african-national-policy-on-data-and-the-cloud/74319, accessed 27 October 2025.
277 See https://g20.org/g20-south-africa/g20-presidency/, accessed 27 October 2025.
278 See https://www.fasken.com/en/knowledge/2026/03/ai-regulation-progress-in-south-africa-a-further-step-in-the-right-direction-2, accessed 20 March 2026.
279 See https://www.bakermckenzie.com/en/insight/publications/2026/02/south-african-ai-policy-moves-towards-approval, accessed 20 March 2026.
280 International Commission of Jurists (2022:24); Bakiner (2023); Rodrigues (2020).
281 Shany (2025: 458).
282 Ibid.

certain "digital rights" into existing human rights treaties through purposive interpretation, on the premise that formal treaty reform is politically unlikely.[283] The literature identifies a paradox at the heart of this approach. The more unlikely new international human rights treaties appear, the more interpretative flexibility is relied upon to fill normative gaps.[284] Yet this reliance simultaneously reduces incentives to develop clearer, binding instruments to address systemic digital harms. As a result, interpretative expansion often masks—rather than resolves—the absence of comprehensive legal protection.

This dynamic is directly relevant to the governance of soil data in Africa. In most African countries, the only relevant law addressing automated decision-making is data protection legislation, which has significant gaps regarding AI, including algorithmic bias, accountability, transparency, and the broader societal effects of automation.[285] Significant legal ambiguity also surrounds issues such as deepfakes, AI-generated art, and the ownership rights of works created by AI. To strengthen soil protection through digitalisation and AI, South Africa and African states more broadly must move beyond fragmented personal data regimes. This requires a National Soil Data Policy to define ownership and access rights; AI-specific environmental regulations to ensure accountability in soil monitoring; open and inclusive data-sharing frameworks that balance private and public interests; and investments in digital literacy to empower farmers as co-creators of value in the soil data economy.[286]

4. Latest dynamics and developments

The rapid evolution of AI, digital trade, and data governance is reshaping global economic, legal, and environmental systems. The 2024–2025 cycle has seen unprecedented convergence between trade law, intellectual property (IP), digital sovereignty, and sustainability policy, indicating a shift from fragmented innovation approaches toward coordinated digital governance. Within this landscape, Africa is increasingly positioned as both a laboratory for experimentation and a catalyst for new models of global cooperation.

The conversation around AI often oscillates between utopian optimism and dystopian anxiety. Yet the central challenge is neither technological progress nor automation itself, but the unequal distribution of its benefits. As millions of jobs face disruption, the key question is not whether AI will transform labour markets, but who will capture the gains it generates. Without broad access to capital, infrastructure, and income security, AI risks deepening existing inequalities rather than expanding global

283 Ibid.: 463–468; For a discussion, see Pajuste (2025).
284 Ibid.: 461.
285 Davis & Trott (2024).
286 See https://www.fluxmans.com/article/ai-regulation-south-africa, accessed 29 September 2025.

opportunity. In this sense, AI is not a neutral force: it amplifies pre-existing asymmetries in wealth, capacity, and institutional strength. This dynamic is already visible across the Global South. Middle-income economies such as Brazil, China, India, and Indonesia are increasingly able to integrate AI into existing industrial systems.[287] By contrast, many African economies—where informal employment dominates—remain structurally unprepared for large-scale AI adoption.[288] At the lower end of the income spectrum, countries risk losing their comparative advantage in labour-intensive service sectors without gaining footholds in AI-driven industries, as automation accelerates a pattern of "jobless growth." At its core, AI is reshaping the global distribution of income by shifting returns from labour to capital. Countries with strong technological ecosystems can accumulate domestic AI capital, while others remain dependent on foreign platforms and infrastructure. This creates a new axis of inequality within the Global South itself, dividing AI adopters from AI-dependent economies.[289]

AI governance is transitioning from voluntary ethical principles to binding law. Risk-based, transparency-driven frameworks are becoming the global norm, with extraterritorial effects that influence domestic policymaking. Alongside these developments, multi-stakeholder initiatives at global and regional levels aim to align technological innovation with human rights, safety, accountability, and societal benefit. The International Bar Association's Strategic Plan exemplifies this trend, proposing measures to integrate AI responsibly into the legal profession by supporting smaller firms through training and financial incentives, developing governance standards on privacy and data security, and revising ethical guidelines to ensure AI-generated work complies with professional standards.[290] Similarly, new international instruments, such as the OECD's Expert Group on AI Futures, the EU's AI Act, the UN's Global Digital Compact (GDC), and the AU's AI Strategy, seek to bridge the digital, data, and innovation divides. The GDC, annexed to the Pact for the Future, provides a blueprint for global cooperation by promoting inclusive connectivity, digital literacy, human rights–based governance, and ethical oversight of emerging technologies, ensuring that technological progress supports sustainable and equitable development.[291]

Evolving notions of digital sovereignty complement these frameworks. Control over data, infrastructure, and code has become a central geopolitical objective.[292] In practice, however, the pursuit of digital sovereignty may also enable more intrusive forms of state control. Recent evidence highlights the rapid expansion of AI-enabled mass surveillance systems across parts of Africa, often implemented through foreign

287 See https://www.giga-hamburg.de/en/publications/giga-focus/automation-and-inequality-social-safety-nets-in-the-age-of-ai, accessed 20 March 2026.
288 Ibid.
289 Ibid.
290 IBA (2024: 10).
291 See UN (2023a and b).
292 Fritzsche & Spoiala (2022: 21).

technology partnerships.[293] Reports indicate that several African governments have invested heavily in AI-powered facial recognition, biometric tracking, and smart surveillance infrastructure, frequently justified in terms of urban modernisation and security.[294] Yet in many cases, these systems operate in contexts of limited regulatory oversight, raising serious concerns about proportionality, legality, and the protection of fundamental rights. These developments illustrate that digital sovereignty is not inherently emancipatory: without robust legal safeguards, it may instead reinforce new forms of technological dependency and state-led control.

While Europe advances human-centric governance through initiatives such as the Digital Markets Act, the AI Act, and the Global Gateway, China extends its influence through the Digital Silk Road.[295] Africa finds itself navigating between these competing models while asserting its technological autonomy through regional initiatives such as the AU–EU Digital for Development Hub, which promotes data sovereignty, shared standards, and multi-stakeholder dialogue.[296] The EU's experience in building a Digital Single Market provides valuable lessons for Africa's own efforts to develop a continental digital market under the African Continental Free Trade Area Agreement (AfCFTA).[297] Still, success will depend on capacity building, localisation of standards, and sustained investment in digital skills.

Recent initiatives further illustrate Africa's growing emphasis on building sovereign digital capacity through strategic partnerships. In February 2026, the African Union Commission concluded a landmark Memorandum of Understanding with Google to advance AI and digital transformation across the continent.[298] Moving beyond mere technology adoption, the partnership focuses on strengthening long-term resilience through investments in digital and cloud infrastructure, skills development, research and innovation ecosystems, and responsible AI governance frameworks. Crucially, it reflects a shift from digital access towards digital agency, emphasising locally relevant innovation, multilingual AI systems, and the development of domestic technical capacity. Such initiatives signal an emerging model of cooperative digital sovereignty in which Africa seeks to shape, rather than simply adopt, global technological systems.

At the same time, international trade institutions are becoming critical arenas for AI-trade governance. Through instruments such as the Technical Barriers to Trade (TBT) Agreement, the Trade-Related Aspects of Intellectual Property Rights (TRIPS)

293 See https://www.theguardian.com/global-development/2026/mar/12/invasive-ai-led-mass-surveillance-in-africa-violating-freedoms-warn-experts, accessed 20 March 2026.
294 Ibid.
295 Daniels et al. (2022: 5–7).
296 Fritzsche & Spoiala (2022: 24-25); see https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/, accessed 27 October 2025.
297 Daniels et al. (2022: 6).
298 See https://au.int/en/pressreleases/20260217/auc-google-sign-partnership-advance-africas-sovereign-ai-digital-capacity, accessed 20 March 2026.

Agreement, and the General Agreement on Trade in Services (GATS), the WTO facilitates transparency, harmonisation, and mutual recognition of AI-related goods and services.[299] The WTO's World Trade Report 2025 estimates that, given supportive policies, AI could increase the value of international trade in goods and services by almost 40% by 2040, driven by productivity gains and lower trading costs.[300] However, to ensure those gains are broadly shared, the report emphasises the need to close the digital divide, invest in skills, and maintain an open and predictable trading system. The TBT Agreement encourages members to participate in developing international standards and to use them as the foundation for domestic regulation, thereby reducing unnecessary divergence and compliance costs.[301] Mutual Recognition Agreements (MRAs) further enable countries to recognise each other's certifications, facilitating the cross-border flow of digital products. However, developing economies often lack the capacity to fully engage in these technical forums. Within Africa, it is estimated that digital upgrades could benefit 600,000 formally registered firms and 40 million microbusinesses.[302] A case in point is WFP's 'Maano—Virtual Farmers Market' pilot in Zambia: an app that links smallholders with traders, provides real-time price signals, and closes transactions securely.[303] The AfCFTA Digital Trade Protocol could transform this landscape, provided it reflects regional realities and strengthens institutional capacity to manage innovation responsibly.[304] Embedding practical, farmer-facing use cases—such as e-payments, e-signatures, data protection, platform interoperability, and SME onboarding—would help translate connectivity into inclusive market access.

Algorithms—the foundational components that enable AI to learn, predict, and make autonomous decisions—play an increasingly central role in the commerce sector. They enhance efficiency in financial trading and online pricing, yet they also raise complex issues under competition law.[305] While increased price transparency can promote competition, algorithmic pricing can lead to coordinated behaviour, price discrimination, or the exploitation of market power.[306] Competition law, traditionally concerned with consumer welfare in terms of price, choice, quality, and innovation, must now adapt to the algorithmic economy. Detecting algorithmic collusion, dominance abuse, and resale price maintenance has become an enforcement challenge, underscoring the need for robust oversight and accountability mechanisms to ensure that technological advancement aligns with fair-market principles.

Beyond competition law, digitalisation and AI are also reshaping traditional understandings of intellectual property and inventorship, including in the agricultural sector.

299 WTO (2024); da Fonseca Azevedo (2024: 8).
300 WTO (2025: 6).
301 WTO (2024: 68); WTO (2021: 20–21).
302 Signé (2024: 150).
303 See https://innovation.wfp.org/project/virtual-farmers-market, accessed 30 October 2025.
304 Lemma et al. (2024).
305 Barfield (2018: 2).
306 Bostoen (2025: 178).

Digital, data-driven agriculture is poised to play a pivotal role in increasing global food output by approximately 60% to feed an estimated 9.3 billion people by 2050.[307] With millions of on-farm sensors now deployed, an average farm currently generates about 500,000 data points per day, a figure projected to climb to around 4 million daily by 2036.[308] Agricultural farm data (and, by extension, soil data) is less likely to be protected under current copyright systems.[309] While raw data itself is not patentable, its analysis may lead to patentable inventions. Derivative works—such as analytical reports or digital models generated from farm data—could qualify for copyright protection.[310] This highlights the importance of clear agreements governing farmers' data disclosure, ensuring that ownership or benefit-sharing arrangements are established for any inventions or intellectual property derived from shared data. To foster trust between farmers and ag-tech providers while laws catch up, several voluntary, farmer-centric data agreements have emerged. These include the US Privacy and Security Principles for Farm Data, the Australian Farm Data Code, France's Charte sur l'utilisation des données agricoles, Switzerland's Charter on the Digitalisation of Agriculture and Food, and the EU's Code of Conduct.[311] These instruments generally recognise farmers' ownership or control over their data and establish baseline rules for privacy, security, access, and fair use.

More broadly, as AI systems increasingly contribute to creative and inventive processes, questions arise over authorship, ownership, and patent eligibility.[312] Most jurisdictions maintain that only natural or juristic persons can be inventors, yet South Africa's acceptance of the DABUS patent in 2021 signals a potential paradigm shift.[313] These trends also open debates about whether AI should be granted some form of legal personhood.[314] Under TRIPS, transparency and disclosure requirements for AI-generated innovations are becoming vital for balancing innovation incentives with accessibility.[315] These developments illustrate how AI is transforming the moral and legal foundations of creativity, demanding a re-examination of existing IP frameworks to ensure that protection mechanisms remain relevant in the digital age.

Meanwhile, digitalisation is redefining sustainability imperatives. AI can model energy efficiency, forecast environmental risks, and optimise resource management, but it also contributes to carbon emissions, electronic waste, and widening

307 Yu et al. (2025: 1).
308 Ibid.
309 Uddin (2024: 5).
310 Ibid.: 11.
311 Ibid.: 2.
312 WIPO (2019: 19).
313 See https://www.nortonrosefulbright.com/en-za/knowledge/publications/2a3c551a/ai-inventorship-on-the-horizon-part-1, accessed 27 October 2025.
314 See Forrest (2024); Baeyaert (2025).
315 WTO (2024: 44, 46 & 75–76).

inequalities.[316] The emerging field of digital sustainability law links AI regulation to environmental commitments under the WTO and the Paris Agreement, positioning sustainability and inclusivity as benchmarks for legitimate digital transformation.[317] Africa's Continental AI Strategy reinforces this view, framing digitalisation not merely as an economic opportunity but as a pathway toward ecological resilience and intergenerational justice.

Across these diverse developments, a more profound structural transformation is becoming visible: the gradual convergence of AI regulation, digital trade, intellectual property, and environmental governance into a single, interoperability-driven system. Several interlocking dynamics define this emerging digital order—the assertion of data and technological sovereignty as a foundation of self-determination; the integration of sustainability and equity as prerequisites for legitimacy; and the growing reliance on evidence-based, transparent policymaking to guide innovation responsibly. Together, they mark a shift from fragmented technological experimentation to coordinated digital stewardship. For Africa, this transformation represents both a challenge and an opportunity. Through the Continental AI Strategy, the Digital Transformation Strategy (2020–2030), and the AfCFTA Digital Trade Protocol, the AU is laying the groundwork for a distinctly African model of digital governance—people-centred, rights-based, and ecologically grounded. Success will depend on closing the AI and data divides through infrastructure investment, institutional capacity-building, and equitable access. Recent AU–G20 cooperation might facilitate this: At the G20 on AI for Africa Conference (September–October 2025), UNESCO launched the AI Initiative for Africa to scale ethical, people-centred AI—committing to train 15,000 civil servants, 5,000 judges and prosecutors on using AI, and, via the SPAARK-AI Alliance of public-administration schools (now spanning 45 African states), to cascade this capacity continent-wide.[318] Working with the AU on its continental AI strategy, UNESCO also unveiled a Technology Policy Assistance Facility with case studies, training resources, and expert directories to help governments craft AI roadmaps aligned with international standards.

Ultimately, these intertwined trends point toward a maturing global digital order that seeks to balance innovation with accountability, autonomy with interdependence, and growth with sustainability.

316 See https://www.unep.org/topics/digital-transformations/sustainable-digitalization, accessed 27 October 2025.

317 Aslam et al. (2025).

318 See https://www.unesco.org/en/articles/ai-africa-unesco-unveils-new-solutions-its-development-g20, accessed 6 November 2025.

5. Conclusion: governing AI and digitalisation for sustainable soils

The UN Trade and Development's *Technology and Innovation Report 2025* depicts a bifurcated AI landscape. A small cohort—approximately 100 firms, primarily based in the US and China—accounts for roughly 40% of private research and development. At the same time, 118 countries, mainly in the Global South, are underrepresented in rule-making arenas.[319] The market is expected to inflate to an estimated USD 4.8 trillion by 2033, with valuations tripling in 2023 and nearly tripling again in 2024.[320] Compute and infrastructure are likewise concentrated: the US holds about one third of TOP500 supercomputers and over half of total computational performance; China is second with 80 machines but under a tenth of US compute; most hyperscale data centres remain US-based, with only a few developing economies (notably Brazil, China, India, and the Russian Federation) hosting comparable assets.[321] Training costs for frontier models have increased by approximately 2.4 times per year since 2016 and are now dominated by hardware, pushing development into the hands of large tech companies.[322] In 2023, the US accounted for ~70% of global private AI investment (USD 67 billion), followed by China (USD 7.8 billion) and India (USD 1.4 billion), which ranked tenth.[323] Between 2000 and 2023, the US and China accounted for approximately one-third of AI publications and around 60% of AI patents.[324] Most GenAI breakthroughs—and top-tier talent (≈approximately 50% from China, 18% from the US, and 12% from Europe)—are clustered in these regions.[325]

That concentration is not a neutral backdrop. It determines who writes the code, curates the datasets, and defines the "best practices" now being adopted in agriculture, environmental governance, and law. As AI moves into SSM, these upstream asymmetries risk being reproduced downstream—in how soils are mapped, monitored, and monetised, and in who captures the value of the data. For SSM, these tools hold enormous promise, from improving monitoring and planning to strengthening accountability. Yet their deployment also raises profound risks: high energy and water consumption, widening socioeconomic divides, market concentration, opaque data practices, and the erosion of trust, as farmers and communities lack real agency over their information.

Realising the benefits of digitalisation requires more than technological optimism. Reliable, site-specific field data remains indispensable, and without it, even the most sophisticated systems cannot deliver meaningful insights. Equally important is governance: who controls data, how it is shared, and under what conditions. Without clear

319 UNCTAD (2025: 8–9).
320 Ibid.: 6.
321 Ibid.: 21.
322 Ibid.: 22.
323 Ibid.
324 Ibid.: 23.
325 Ibid.

rights, farmers risk becoming data subjects rather than empowered participants in digital transitions.

At the international level, broad principles for AI are beginning to take shape; yet a global consensus on key concepts remains elusive. The absence of specific standards for risk assessment and public goods, such as democracy, human rights, and climate stability, leaves critical gaps. Proposals, such as an intergovernmental panel on AI modelled on the IPCC, illustrate how a collective framework for monitoring, evaluation, and knowledge sharing could develop.

Nationally, effective legislation will require interdisciplinary approaches that integrate soil science, digital innovation, and legal design. Discussions on soil management and digitalisation can no longer proceed in parallel; they must converge. Existing models, such as the EU AI Act, provide valuable guidance; however, frameworks must remain flexible and adaptable to the rapid pace of technological change.

While AI has advanced soil research, three gaps persist: (1) over-reliance on narrow predictors instead of spatial/temporal and decision-making approaches; (2) scarce data from neglected regions; and (3) non-comparable soil-health indices.[326] Legally, these map onto duties to: require transparency of methods and guardrails for any soil-relevant AI used in permitting, subsidies, planning, or enforcement; build a data-protection-compliant Soil Data Commons that prioritises underserved regions; and adopt national, versioned, openly specified soil-health indices for cross-site, multi-year reporting.

AI also forces uncomfortable legal questions. In contexts where environmental protection laws exist only on paper—undermined by corruption, capture, or weak enforcement—AI systems trained on ecological thresholds and legal criteria could, in theory, enforce rules more consistently than compromised human institutions.[327] Yet handing enforcement to opaque "black-box" models creates new risks: when code is inscrutable, errors cannot be contested, bias is hard to detect, and discretion can be laundered through algorithmic outputs. That combination—apparent objectivity coupled with opacity—both threatens entrenched discretionary power and offers it a new veil, making governments reluctant to delegate and communities unable to scrutinise. The lesson is clear: legal systems fail less from a lack of tools than from a lack of political will. AI may expose these failures, but it cannot resolve them without strong oversight, algorithmic transparency (including explainability, audit trails, and the right to challenge automated decisions), and democratic legitimacy.

Unlike earlier technologies, modern AI—especially deep-learning systems—cannot be straightforwardly inspected, specified, or audited against regulations; their behaviour arises unpredictably from training rather than deliberate design.[328] Still, the proven oversight models from high-risk sectors, such as aviation and nuclear energy,

326 Birkstedt et al. (2023).
327 Kumar (2025).
328 Judge et al. (2025).

should not be abandoned. Policymakers must instead manage the risks posed by today's opaque models while supporting the development of AI architectures that can be rigorously proven safe. Drawing from AI safety research and prior regulatory experience, effective governance will likely depend on consolidated authority, licensing regimes, mandatory disclosure of training data and model parameters, formal verification of system behaviour, and the capacity for rapid intervention.[329]

We should not frame AI regulation as a battle of extremes. Instead, it should represent a careful effort to strike a balance between individual and societal safety and the need to foster innovation. Navigating these trade-offs requires clarity and a nuanced understanding of several critical issues. Defining AI remains inherently difficult; vague definitions introduce legal uncertainty and weaken regulatory effectiveness.[330] Because AI applications differ across sectors, technologies, and data types, a uniform regulatory approach may prove both ineffective and counterproductive.[331] Yet there is broad agreement that AI systems must uphold privacy, fairness, transparency, accountability, and the preservation of individual freedoms.[332] Regulation should safeguard these principles precisely and proportionately.

Given AI's sectoral diversity, effective governance requires inclusive processes that bring together governments, scientists, legal experts, and civil society. Certification mechanisms can clarify liability and incentivise adherence to safety standards, while regulatory sandboxes provide controlled environments to test innovations before deployment.[333] Policymakers must also ensure regulators have sufficient technical expertise, invite public participation, and craft frameworks that remain adaptive to technological change.[334] Over-regulation risks stagnation; under-regulation risks harm. The solution lies in flexible, evidence-based regulation that protects rights while promoting responsible progress.

Crucially, this requires a shift in how regulation itself is conceived. Rather than relying on static "set-and-forget" legal frameworks, governments must adopt more responsive, adaptive approaches that evolve with technological change. This includes embedding anticipatory governance tools—such as horizon scanning, strategic foresight, and early-stage stakeholder engagement—within regulatory processes, alongside iterative policy cycles that allow for continuous learning, feedback, and adjustment.[335] Such approaches can help close persistent information gaps and better align legal frameworks with rapidly changing technological realities. At the same time, digital technologies themselves offer new tools for improving regulatory design and implementation. Advanced data analytics, regulatory experimentation, and digital

329 Ibid.
330 Cajueiro & Celestino (2026: 90).
331 Ibid.
332 Ibid.
333 Ibid.
334 Ibid.
335 OECD (2025a: 87).

monitoring systems can support more evidence-based decision-making, enhance enforcement capacity, and reduce administrative burdens in increasingly complex governance environments.[336] However, realising these benefits depends on strengthening institutional capacity and coordination. Without investment in skills, expertise, and cross-sectoral collaboration, there is a risk that digital innovations will fall between regulatory silos, exacerbating fragmentation rather than resolving it.[337] Future-ready governance, therefore, depends not only on better rules but on stronger institutions. Building cohesive, well-resourced, and technically capable regulatory systems—at both national and international levels—is essential to ensure that digitalisation supports, rather than undermines, sustainable soil management and broader socio-ecological objectives.[338]

The way forward lies in hybrid governance systems, which combine AI's speed, consistency, and pattern recognition with human judgment, ethical safeguards, and robust accountability. To harness AI's potential for soils while mitigating its risks, a layered governance model is essential: binding regulation, moral guidance, and strong local agency, particularly in the Global South. That, in turn, demands data: African governments should update national soil maps and build publicly accessible, interoperable soil-data platforms; partner with universities, research institutes, and extension services to generate and validate high-quality local datasets; and require that agricultural AI be trained, tested, and benchmarked on locally representative data rather than foreign proxies. For Africa, this means developing context-sensitive, socially grounded soil governance frameworks—rooted in local knowledge, open standards, and clear rights to access and benefit from data—rather than importing external models wholesale.

Ultimately, the question is not simply how to govern AI, but to what end. If digitalisation is to advance soil law, its foundations must be justice, sustainability, and human dignity, not efficiency or profit alone. These values must be embedded into the very architecture of AI systems that generate, interpret, and disseminate soil data. In this emerging legal order, the challenge is not to resist digital change, but to ensure that technological innovation strengthens the protection of soils—our most fragile and indispensable resource. Only then can AI and digitalisation become true allies in building a more just, democratic, and sustainable future.

336 Ibid.
337 Ibid.
338 Ibid.