ID: 737

A governance-by-design framework for secure ai-enabled digital agriculture platforms

Cevher Özden

Çukurova University, Faculty of Arts and Sciences, Department of Computer Sciences, 01250, Adana, Türkiye.

Abstract

Digital agriculture platforms now bring together a wide range of data sources, including sensor measurements, satellite imagery, meteorological records, farm-level observations, mobile applications, and AI-based models. This integration creates clear opportunities for precision agriculture, climate-smart production, evidence-informed advisory services, and more sustainable use of agricultural resources. Yet the same platforms also raise difficult questions about data ownership, cybersecurity, model reliability, privacy, and accountability in decision-making. In practice, many digital agriculture projects still give greater attention to predictive performance than to the governance and security structures required for responsible use. This imbalance becomes especially problematic when such systems are expected to inform real decisions that affect farmers, public institutions, production planning, and environmental sustainability.

This study develops a governance-by-design framework for secure AI-enabled digital agriculture platforms. The framework is organized around three mutually reinforcing layers: data governance, cybersecurity and AI risk management, and decision accountability. The data governance layer covers issues such as data ownership, access rights, consent, data quality, provenance, and responsible data sharing. The cybersecurity and AI risk management layer deals with identity management, role-based access control, API security, IoT and sensor vulnerabilities, data poisoning, model manipulation, system logging, and incident monitoring. The decision accountability layer focuses on how AI-generated recommendations should be explained, validated, documented, and linked to human oversight.

The central contribution of this study is its shift in perspective. Rather than treating digital agriculture platforms mainly as model-driven prediction tools, the study frames them as trustworthy decision-support infrastructures. By bringing together information systems governance, cybersecurity controls, and AI accountability principles, the proposed framework offers a conceptual basis for designing agricultural digital platforms that are secure, auditable, and responsibility-aware. In this respect, the framework can support researchers, software developers, agricultural institutions, and policymakers in building more reliable and accountable digital transformation strategies for agriculture.

Keywords: *Digital agriculture, Data governance, Cybersecurity, Artificial intelligence, Decision support systems, Agricultural information systems, Decision accountability*

Introduction

Digital agriculture is changing how agricultural production is monitored, how advisory services are delivered, and how institutions make decisions. This transformation is driven by the increasing use of sensor networks, satellite observations, farm management systems, mobile applications, cloud platforms, and AI-based analytics. Earlier studies on smart farming had already shown that big data, IoT, cloud computing, and AI extend decision-making capacity beyond the boundaries of individual farms and affect the wider agri-food supply chain (Wolfert et al., 2017). More recent social science research further underlines that digital agriculture should not be understood as a purely technical shift. It is also a socio-technical transition shaped by questions of ownership, privacy, ethics, farmer identity, institutional arrangements, and agricultural knowledge systems (Klerkx et al., 2019).

AI-enabled digital agriculture platforms can support many practical decisions, including irrigation scheduling, disease risk monitoring, fertilizer recommendations, climate-smart production, input optimization, and early-warning services. Yet these platforms are increasingly used in contexts where their outputs may have direct consequences for production costs, crop losses, environmental performance, and trust in institutions. For this reason, their design cannot be evaluated only through model accuracy. The responsible AI literature in agriculture has already warned that AI systems may introduce risks related to data reliability, interoperability, safety, security, unintended socio-ecological effects, and the under-representation of vulnerable producers (Tzachor et al., 2022).

Despite the growing interest in AI-supported agriculture, governance, cybersecurity, and accountability are still often handled as secondary concerns. This is a major weakness. Agricultural decision-support systems rely on heterogeneous data flows coming from farmers, sensors, public agencies, private service providers, and environmental monitoring infrastructures. When these flows are not governed carefully, digital agriculture platforms may reproduce or even intensify problems such as dependency, opacity, surveillance, misuse of data, and institutional risk. Recent reviews similarly point to continuing concerns about data privacy, ownership, stakeholder trust, infrastructure constraints, and the ethical deployment of AI in agricultural systems (Omotayo et al., 2025; Rouzky et al., 2025).

This study proposes a governance-by-design framework for secure AI-enabled digital agriculture platforms. The framework brings together three complementary layers: data governance, cybersecurity and AI risk management, and decision accountability. The central claim is that digital agriculture platforms should not be designed merely as prediction engines. They should be treated as trustworthy decision-support infrastructures in which data rights, security controls, model-related risks, human oversight, and decision records are defined from the outset.

The contribution of the study is threefold. First, it reframes digital agriculture platforms as socio-technical information systems rather than isolated AI models. Second, it develops a layered framework that connects data governance, cybersecurity, and decision accountability within a single design logic. Third, it presents an illustrative use case showing how an AI-generated agricultural recommendation can be traced from data input to institutional accountability.

Problem Background

A first challenge is data governance. Digital agriculture platforms rely on large and diverse datasets, including farm-level records, environmental observations, agronomic measurements, geospatial layers, and operational data. These data may be generated through sensors, farm machinery, mobile applications, satellite imagery, weather stations, or public administrative systems. Yet the governance of agricultural data is still far from settled. Rouzky et al. (2025) note that smart farming lacks standardized data governance frameworks, that security mechanisms remain insufficiently explored, and that farmers often have limited awareness of data privacy and security issues.

A closely related issue is the ambiguity surrounding data ownership and control. As Atik (2022) argues, the debate cannot be resolved simply by assigning ownership rights to farmers, because the more difficult questions involve data lock-in, fragmentation, access barriers, and trust. This point is particularly important for AI-enabled digital agriculture platforms. Farmers may generate valuable data through their land, machinery, production practices, and local observations, while platform providers may control the infrastructure, analytics layer, and user-facing decision interface. Under such conditions, governance needs to clarify not only who "owns" the data, but also who is allowed to access, process, share, monetize, or reuse it.

Cybersecurity forms another critical concern. Smart agriculture systems are increasingly connected to IoT devices, cloud services, APIs, mobile applications, and external data providers. This connectivity expands the attack surface of agricultural information systems. A systematic literature review on cybersecurity in smart agriculture emphasizes that cyberattacks on agricultural ICT infrastructures can have serious consequences and that organizations need both technical safeguards and training processes to identify and respond to cyber threats (Campoverde-Molina & Luján-Mora, 2025). In this context, cybersecurity cannot be reduced to database protection. It must also cover identity management, device security, API protection, continuous monitoring, incident response, and supply-chain dependencies.

A further challenge relates to AI risk management. AI models may generate recommendations that are inaccurate, biased, opaque, or unsuitable for the local context in which they are applied. NIST's AI Risk Management Framework organizes AI risk management around four functions: Govern, Map, Measure, and Manage, with the Govern function operating across all stages of organizational AI risk management (NIST, 2023). This perspective is highly relevant for digital agriculture, where AI-based recommendations may shape farming practices, resource allocation, and institutional advisory services.

Decision accountability is also unresolved. AI-enabled platforms often produce recommendations, but the responsibility chain behind these recommendations is not always clear. If a recommendation leads to a poor outcome, responsibility may be distributed across several actors: the software developer, the data provider, the agricultural institution, the human expert, the model vendor, or the farmer who acted on the advice. Alexander et al. (2024) show that responsible AI in agriculture involves several gray areas, including data access, regulation, adoption barriers, and trust-building. For this reason, digital agriculture systems need explicit mechanisms for explanation, human validation, decision logging, and responsibility assignment.

Taken together, these issues show why AI-enabled digital agriculture platforms require a governance-by-design approach. Governance, cybersecurity, and accountability should not be attached to the platform later as external compliance requirements. They need to be embedded directly into the platform architecture from the beginning.

Material and Methods

The proposed framework is structured around three interdependent layers: the Data Governance Layer, the Cybersecurity and AI Risk Management Layer, and the Decision Accountability Layer. These layers do not operate in isolation; rather, they are linked through a decision-support flow that connects data inputs, risk controls, AI-based analysis, human oversight, and accountable decision records (Figure 1).

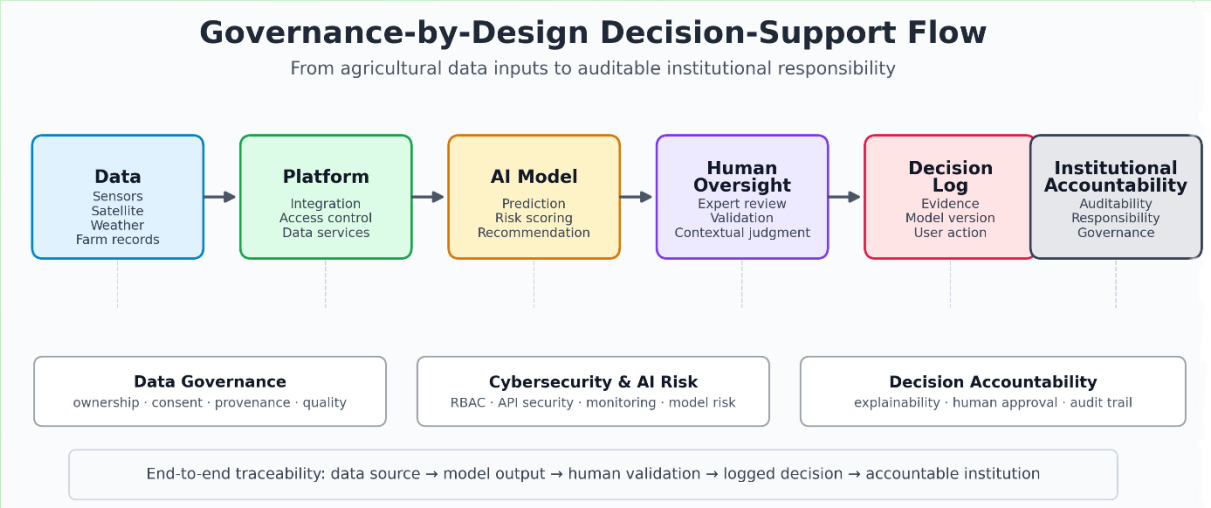

Figure 1. Conceptual flow for secure and accountable AI_enabled digital agriculture platforms.

This flow is based on the view that trustworthy agricultural decision support depends on traceability across the entire process, from input data to the final decision record. In other words, the platform should make it possible to answer five core questions: Which data were used? Who was authorized to use them? How was the system protected? How was the AI-generated recommendation produced and validated? And finally, who carries responsibility for the decision that is recorded or acted upon?

Data Governance Layer

The Data Governance Layer defines how agricultural data are collected, accessed, processed, shared, and retained throughout the platform. In AI-enabled agriculture, this layer should not be seen as a narrow technical data management function. It is also a mechanism for building trust among farmers, institutions, technology providers, and decision-makers. Wolfert et al. (2017) identify governance issues, including data ownership, privacy, and security, as key research concerns in smart farming. Similarly, Klerkx et al. (2019) show that power relations, ownership, privacy, and ethics are central themes in the wider digital agriculture debate.

This layer includes six core components:

1. **Data ownership and usage rights:** defining the legal and operational rights associated with farm-level, environmental, and platform-generated data.
2. **Access control policies:** specifying which users, institutions, service providers, and AI models are allowed to access specific types of data.
3. **Consent and purpose limitation:** ensuring that farmers and institutions are informed about how their data will be used and for what purposes.
4. **Data quality and validation:** documenting missing values, sensor errors, outdated records, inconsistent measurements, and other reliability issues.
5. **Data provenance:** recording the source, timestamp, transformation history, and reliability status of each data item used in the platform.
6. **Responsible data sharing:** defining the conditions under which data may be shared with researchers, public institutions, private vendors, or third-party analytics providers.

The purpose of this layer is to create a reliable and trustworthy data foundation for agricultural decision support. Without such a foundation, AI-generated recommendations may appear technically sophisticated, but they remain institutionally fragile and difficult to justify in real-world decision contexts.

Cybersecurity and AI Risk Management Layer

The Cybersecurity and AI Risk Management Layer protects the platform, data flows, models, devices, and users against both technical and organizational risks. Smart agriculture platforms are not simple software systems; they operate through connected sensors, mobile applications, cloud dashboards, APIs, external data services, and AI-based decision engines. For this reason, they require a broad cybersecurity and risk management perspective. The NIST Cybersecurity Framework 2.0 places governance at the center of cybersecurity risk management by emphasizing the need to define and monitor strategy, expectations, policies, roles, responsibilities, oversight mechanisms, and supply-chain risk management practices (NIST, 2024).

This layer addresses two groups of risks. The first group includes conventional cybersecurity risks such as unauthorized access, weak authentication, API vulnerabilities, device compromise, data exfiltration, ransomware,

and service disruption. The second group consists of AI-specific risks, including data poisoning, model manipulation, adversarial inputs, model drift, poor calibration, and excessive dependence on automated recommendations.

The main controls in this layer include:

- identity and access management,
- role-based access control,
- secure API design,
- encryption of sensitive data,
- IoT and sensor hardening,
- system logging and anomaly detection,
- backup and recovery mechanisms,
- incident response procedures,
- supplier and third-party risk management,
- AI model monitoring and periodic validation.

This layer treats cybersecurity as a direct component of agricultural decision quality. For example, if a disease-risk alert is generated from manipulated sensor data, the problem is not merely a technical breach. It also becomes a decision-support failure, because the platform may guide farmers, experts, or institutions toward an incorrect action.

Decision Accountability Layer

The Decision Accountability Layer defines how AI-generated recommendations are explained, validated, recorded, and linked to human responsibility. In agricultural decision support, a platform should not merely produce outputs such as "irrigate," "apply fertilizer," or "disease risk is high." It should also clarify why such a recommendation was produced, which data sources were used, how confident the system is, which model version generated the output, and whether expert validation is needed before action is taken.

This layer is consistent with the responsible AI literature, which places strong emphasis on trust, transparency, and accountability. Alexander et al. (2024) show that responsible AI in agriculture and food-system technologies requires attention to data access, regulation, adoption barriers, and trust-building. Similarly, Tzachor et al. (2022) argue that AI applications in agriculture should be assessed not only through isolated performance metrics, but also in terms of systemic risks, externalities, and broader socio-ecological consequences.

The Decision Accountability Layer includes the following elements:

- explanation of the AI-generated recommendation,
- uncertainty or confidence information,
- model version and timestamp,
- summary of data provenance,
- expert validation status,
- farmer or institutional decision record,
- assignment of responsibility,
- post-decision feedback and outcome tracking.

Through these elements, the layer transforms an AI output into an auditable decision-support artifact. Its main role is to ensure that recommendations are not only generated, but also made traceable, reviewable, and institutionally accountable (Table 1).

The proposed framework is organized around three interdependent governance layers: data governance, cybersecurity and AI risk management, and decision accountability. Together, these layers move AI-enabled digital agriculture platforms beyond a narrow focus on prediction performance. Instead, they position such platforms as trustworthy decision-support infrastructures where data use, security controls, model-related risks, explanations, human oversight, and institutional responsibility are addressed as part of the system design. Figure 2 illustrates this layered governance architecture and shows how it supports secure, auditable, explainable, and accountable agricultural decision support.

Illustrative Use Case

Consider a digital agriculture platform that produces disease-risk recommendations for tomato producers. The platform draws on several data sources, including weather station records, humidity measurements, satellite-derived vegetation indicators, farmer-submitted field observations, historical disease occurrence, and an AI-based risk model. Based on these inputs, the system generates the following recommendation: "High disease risk is detected for the next 72 hours; preventive action is recommended."

Table 1. Governance-by-Design Framework for Secure AI-Enabled Digital Agriculture Platforms

Layer	Core Question	Main Risk	Control Mechanism	Decision-Support Effect
Data Governance	Who controls and uses the data?	Unauthorized use, unclear ownership, poor data quality, data misuse	Data ownership rules, access policies, consent, provenance, quality checks, responsible sharing	Creates a reliable and legitimate data foundation
Cybersecurity and AI Risk Management	How is the platform protected?	Cyberattack, data poisoning, API vulnerability, model manipulation, service disruption	Authentication, RBAC, API security, encryption, IoT hardening, logging, model monitoring, incident response	Supports secure and resilient platform operation
Decision Accountability	Who is responsible for the recommendation and final decision?	Wrong, opaque, or unvalidated AI recommendation	Human oversight, explainability, uncertainty reporting, decision logs, responsibility assignment	Enables auditable and accountable decision support

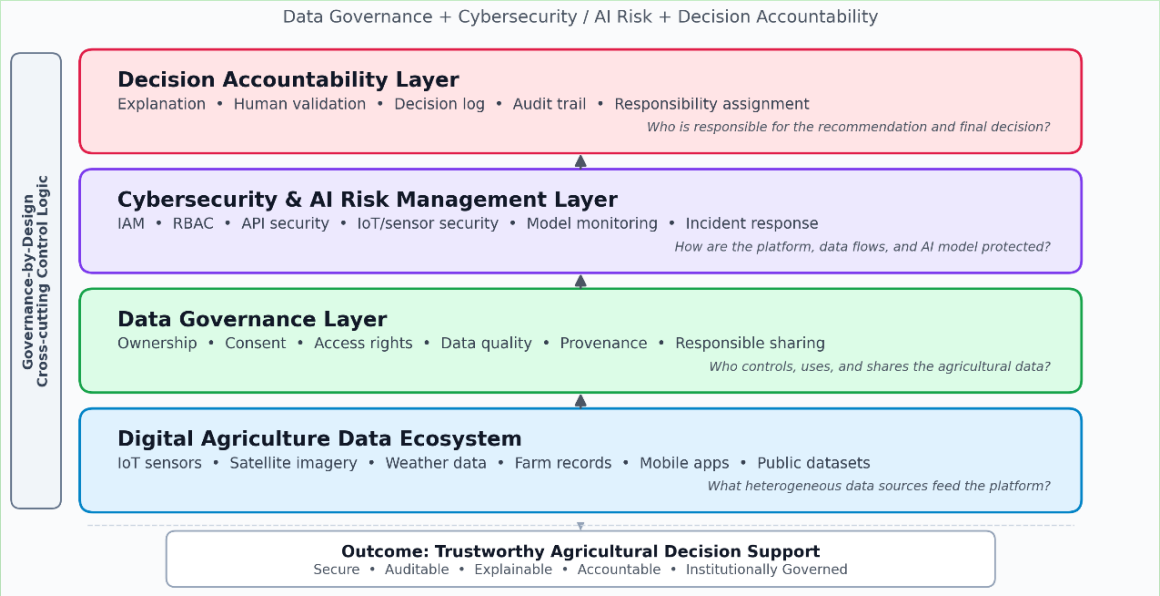

Figure 2. Three-layer governance architecture for secure AI-enabled digital agriculture platforms

In a conventional model-centric system, this recommendation might be presented directly to a farmer or agricultural advisor. In the proposed governance-by-design framework, however, the recommendation is not treated as a standalone model output. Before it becomes an actionable decision-support item, it is examined through three governance layers.

The Data Governance Layer first checks whether the data used in the recommendation are authorized, up to date, and traceable. The platform records the data sources, collection time, consent status, missing data indicators, and transformation history. For instance, the system should indicate whether the humidity data were obtained from a local sensor, a public meteorological service, or a third-party API. It should also show whether the farmer-submitted field observation was manually entered, automatically collected, or inferred from another source.

The Cybersecurity and AI Risk Management Layer then evaluates whether the data flow and system environment can be trusted. If a sensor produces abnormal values, an API call fails, an unusual login attempt is detected, or the model operates outside its validated range, the recommendation should be flagged for additional review. This step is critical because agricultural advice generated from compromised, incomplete, or low-quality data may result in unnecessary pesticide use, economic loss, or environmental harm.

Finally, the Decision Accountability Layer converts the AI output into an auditable recommendation. At this stage, the platform records the model version, confidence level, key evidence, uncertainty warning, expert validation status, and final user action. If an agricultural expert reviews the recommendation before it is communicated to farmers, this approval is attached to the decision log. If no human review is available, the system should clearly state that the recommendation is automated and advisory rather than fully validated (Table 2).

Table 2. A simplified decision record may include:

Field	Example Record
Recommendation ID	DR-2026-0611-0001
Recommendation Type	Tomato disease-risk alert
Data Sources	Weather station, satellite index, farmer observation
Model Version	DiseaseRisk-AI-v1.3
Confidence Level	0.82
Key Evidence	High humidity, recent rainfall, vegetation stress
Human Review	Approved by agricultural advisor
User Action	Farmer notified through mobile application
Accountability Status	Advisory recommendation; expert-reviewed
Audit Trail	Data, model, reviewer, and notification logs stored

This example demonstrates how the proposed framework prevents the AI system from becoming a black-box advisory tool. Instead, the platform becomes a traceable decision-support infrastructure where data, security, model behavior, human oversight, and institutional responsibility are connected.

Discussion

The proposed framework contributes to the field of Management Information Systems by positioning digital agriculture platforms as organizational decision-support systems rather than as narrow technical applications. This distinction is important because agricultural platforms bring together multiple stakeholders, including farmers, advisors, cooperatives, ministries, technology providers, researchers, and private-sector service providers. These actors do not approach the platform with the same priorities. Their expectations may differ in terms of data access, trust, privacy, responsibility, system reliability, and institutional control.

From an information systems perspective, the framework links platform governance directly to decision quality. A model may perform well in technical terms, but it can still fail as a decision-support system if data rights are unclear, security mechanisms are weak, recommendations cannot be explained, or accountability is left undefined. This argument is consistent with the broader digital agriculture literature, which shows that digitalization is not only a matter of technical innovation. It also involves institutional arrangements, power relations, ethics, and responsible innovation (Klerkx et al., 2019; Wolfert et al., 2017).

From a cybersecurity perspective, the framework extends the discussion from data protection to decision protection. In agricultural platforms, cyber incidents may affect not only the confidentiality or availability of information, but also the quality of agricultural advice. Manipulated irrigation data may lead to inefficient water use. Compromised disease-risk alerts may result in unnecessary chemical applications. Unavailable advisory services may delay time-sensitive farm decisions. For this reason, cybersecurity should be embedded throughout the decision-support lifecycle, not treated as a separate technical layer.

From an AI governance perspective, the framework addresses the growing need for responsible and trustworthy AI in agriculture. Existing studies show that AI adoption in agricultural systems is shaped by trust, ethical concerns, infrastructure limitations, data access, and governance challenges (Alexander et al., 2024; Omotayo et al., 2025; Tzachor et al., 2022). The proposed framework translates these broad concerns into concrete platform-level mechanisms, including provenance tracking, access policies, security monitoring, model validation, human oversight, and decision logging.

The framework also has practical value for agricultural institutions, software developers, and policymakers. For institutions, it can serve as a checklist for assessing whether a digital agriculture platform is suitable for real-world advisory use. For software developers, it clarifies which governance, security, and accountability mechanisms should be incorporated from the early design stage. For policymakers, it offers a conceptual basis for regulating AI-enabled agricultural decision-support systems without reducing evaluation to model accuracy alone.

This study nevertheless has limitations. It presents a conceptual framework and does not empirically validate the proposed structure through an operational platform. Future research should test the framework in concrete agricultural decision-support settings, such as irrigation advisory systems, disease early-warning platforms, fertilizer recommendation tools, climate-risk dashboards, or public agricultural e-government services. Further studies may also develop maturity models, audit checklists, or scoring instruments to assess the governance readiness of AI-enabled digital agriculture platforms.

Conclusion

This study proposed a governance-by-design framework for secure AI-enabled digital agriculture platforms. The framework was organized around three layers: data governance, cybersecurity and AI risk management, and decision accountability. Its main argument is that digital agriculture platforms should not be assessed only through

predictive performance. They should also be evaluated according to how responsibly data are governed, how securely systems operate, how AI models are monitored, how recommendations are explained, and how decisions are recorded and audited.

The proposed framework shifts the design perspective from model-centric prediction to trustworthy decision-support infrastructure. Within this perspective, AI is not treated as an autonomous decision-maker. Rather, it functions as one component of a governed agricultural information system. Data provenance, access control, cybersecurity safeguards, human oversight, and decision logging therefore become core design requirements, not optional additions.

For agricultural institutions, the framework offers a way to support safer and more accountable digital transformation. For researchers, it connects digital agriculture with information systems governance, cybersecurity, and responsible AI. For software developers, it provides guidance on how governance and accountability mechanisms can be embedded into platform architecture from the beginning. Future research should operationalize the framework through case studies, prototype implementations, maturity assessments, and empirical validation in real agricultural advisory contexts.

Declarations

Ethical Approval Certificate

Not applicable. This study is a conceptual framework study and did not involve human participants, animals, clinical procedures, experimental interventions, or survey-based data collection requiring ethical approval.

Author Contribution Statement

Cevher Özden: Conceptualization, methodology, literature review, framework design, visualization, writing the original draft, review and editing.

Fund Statement

This work received no specific grant from any funding agency, commercial organization, or non-profit institution.

Conflict of Interest

The author declares no conflict of interest.

Acknowledgments

The author did not receive any administrative, technical, or material support requiring acknowledgment.

References

Alexander, C. S., Yarborough, M., & Smith, A. (2024). Who is responsible for 'responsible AI'?: Navigating challenges to build trust in AI agriculture and food system technology. *Precision Agriculture, 25*(1), 146–185. https://doi.org/10.1007/s11119-023-10063-3

Atik, C. (2022). Towards comprehensive European agricultural data governance: Moving beyond the "data ownership" debate. *International Review of Intellectual Property and Competition Law, 53*(5), 701–742. https://doi.org/10.1007/s40319-022-01191-w

Campoverde-Molina, M., & Luján-Mora, S. (2025). Cybersecurity in smart agriculture: A systematic literature review. *Computers & Security, 150*, Article 104284. https://doi.org/10.1016/j.cose.2024.104284

Klerkx, L., Jakku, E., & Labarthe, P. (2019). A review of social science on digital agriculture, smart farming and agriculture 4.0: New contributions and a future research agenda. *NJAS: Wageningen Journal of Life Sciences, 90–91*, Article 100315. https://doi.org/10.1016/j.njas.2019.100315

National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.100-1

National Institute of Standards and Technology. (2024). *The NIST cybersecurity framework (CSF) 2.0* (NIST CSWP 29). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

Omotayo, A. O., Adediran, S. A., Omotoso, A. B., Olagunju, K. O., & Omotayo, O. P. (2025). Artificial intelligence in agriculture: Ethics, impact possibilities, and pathways for policy. *Computers and Electronics in Agriculture, 239*, Article 110927. https://doi.org/10.1016/j.compag.2025.110927

Rouzky, R., Sarrafzadeh, A., Sowells-Boone, E., Pasandi, H. B., & Goins, G. (2025). Data governance in smart farming: A systematic review of challenges and gaps. *Information Processing in Agriculture*. Advance online publication. https://doi.org/10.1016/j.inpa.2025.11.006

Tzachor, A., Devare, M., King, B., Avin, S., & Ó hÉigeartaigh, S. (2022). Responsible artificial intelligence in agriculture requires systemic understanding of risks and externalities. *Nature Machine Intelligence, 4*, 104–109. https://doi.org/10.1038/s42256-022-00440-4

Wolfert, S., Ge, L., Verdouw, C., & Bogaardt, M.-J. (2017). Big Data in Smart Farming—A review. *Agricultural Systems, 153*, 69–80. https://doi.org/10.1016/j.agsy.2017.01.023