

Digital Identity Systems and Legal Accountability: Privacy, Security and Trust in the Digital Society

Dr. Tharushi Perera¹, Prof. Rahul Deshmukh¹

¹ Faculty of Law and Digital Governance, University of Colombo, Colombo, Sri Lanka

² Department of Technology Law and Information Security, Indian Institute of Digital Studies, Pune, India.

Received: 18 Jan 2025 Revised: 28 Jan 2025 Accepted: 28 Jan 2025 Published: 17 Feb 2025

ABSTRACT

Digital identity systems have become an important component of modern digital infrastructure, enabling individuals to authenticate themselves while accessing governmental, financial, healthcare, educational, and commercial services. The increasing adoption of biometric authentication, mobile-based identity verification, digital signatures, and decentralized identity technologies has created significant opportunities for improving convenience, security, and service delivery. At the same time, digital identity systems generate substantial legal and technological concerns relating to privacy, data protection, identity theft, surveillance, cybersecurity, exclusion, and accountability. This article examines the technological architecture of digital identity systems and explores the principal legal challenges associated with their deployment. Particular attention is given to biometric identifiers, authentication mechanisms, identity databases, decentralized identity, data minimization, cybersecurity, and unauthorized identity use. The article argues that digital identity infrastructure should be designed around privacy, security, proportionality, and user control rather than technological efficiency alone. It proposes a rights-oriented framework based on strong authentication, encryption, decentralized storage, purpose limitation, transparent governance, independent auditing, and effective mechanisms for correcting identity-related errors. The article concludes that trustworthy digital identity requires close integration of technological security and legal accountability.

Keywords: Digital Identity; Cyber Law; Biometric Authentication; Privacy; Data Protection; Identity Theft; Digital Governance.

© 2025. The Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.

1. Introduction

Digital technologies have fundamentally changed commercial transactions. Contracts that were once negotiated and signed exclusively through physical documents can now be created, exchanged, signed, stored, and performed electronically.

The development of artificial intelligence represents the next stage of this transformation.

AI systems can analyze contractual documents, identify clauses, suggest modifications, compare commercial conditions, and assist organizations in negotiating agreements. More advanced systems may also interact with other software platforms and initiate transactions according to predefined instructions.

This creates an important legal question: **when an artificial intelligence system performs an action that appears to create or modify a contract, who should be legally responsible for that action?**

Traditional contract law generally focuses on concepts such as offer, acceptance, intention, consent, authority, and capacity. Automated systems do not possess human intention in the conventional sense.

Consequently, the increasing use of AI creates a need to examine how existing contractual principles can operate within automated digital environments.

This article analyzes these challenges and proposes a framework for legally accountable AI-assisted contracting.

2. Concept of Digital Contracts

A digital contract is an agreement created, communicated, accepted, or stored through electronic means.

Digital contracts may take several forms, including:

- electronically signed agreements;
- online terms and conditions;
- click-wrap agreements;
- electronic purchase agreements;
- automated business-to-business contracts;
- smart contracts; and
- agreements generated using AI systems.

Digital contracts can provide substantial efficiency advantages.

Parties may execute agreements remotely, maintain electronic records, and automate contractual processes.

However, technological convenience must be accompanied by mechanisms ensuring authenticity, consent, and reliable recordkeeping.

3. Artificial Intelligence in Contract Formation

AI can participate in different stages of contract formation.

During negotiation, an AI system may analyze the proposed terms and suggest alternatives.

During drafting, it may generate contractual clauses.

During execution, it may identify required signatures or approvals.

After execution, AI may monitor compliance with contractual obligations.

This creates a spectrum ranging from **AI-assisted contracting** to **highly automated contracting**.

The greater the level of autonomy, the more significant the legal questions concerning responsibility and attribution become.

4. Electronic Consent

Consent is a fundamental element of contractual relationships.

In conventional transactions, consent is generally expressed through words, signatures, conduct, or other recognizable actions.

In automated systems, acceptance may occur when software automatically selects an option or executes a transaction based on programmed instructions.

The legal issue is whether the automated action can be attributed to the person or organization operating the system.

A suitable framework should distinguish between unauthorized system behavior and actions that were reasonably within the scope of the system's authorized functions.

5. Automated Agents

Automated agents are software systems capable of performing tasks without requiring continuous human intervention.

A commercial organization might configure an automated agent to purchase services whenever certain conditions are satisfied.

For example:

Price Condition → Availability Check → Automated Acceptance → Digital Transaction

If the agent enters into an agreement, questions may arise regarding whether the organization is bound by the resulting transaction.

The answer may depend upon authorization, system configuration, applicable contractual rules, and the circumstances surrounding the transaction.

6. AI-Generated Contractual Terms

Generative AI systems can produce contractual language rapidly.

This may reduce drafting time but introduces risks.

An AI system may generate:

- ambiguous language;
- contradictory clauses;
- inappropriate obligations;
- missing provisions; or
- terms inconsistent with the parties' commercial objectives.

Human review is therefore particularly important.

Organizations should not assume that AI-generated contractual language is automatically accurate or legally appropriate.

7. Smart Contracts

Smart contracts are technological mechanisms that can automatically execute predefined instructions.

A simplified example is:

Condition Satisfied → Automated Verification → Transaction Executed

Smart contracts can increase efficiency because certain contractual processes can occur automatically.

However, legal agreements and computer code are not necessarily identical.

A coded instruction may execute exactly as programmed even where the underlying commercial circumstances have changed.

This creates questions concerning modification, termination, mistake, and dispute resolution.

8. Contractual Errors

Automated systems may sometimes make incorrect decisions.

An AI system could misunderstand information, process inaccurate data, or generate an unintended contractual term.

This raises the question of whether a party should be able to challenge a contract created through an automated system.

A legal framework should establish mechanisms for addressing genuine technological errors while preventing parties from using automation as an excuse to avoid legitimate obligations.

9. Authentication

Digital contracting requires reliable authentication.

Electronic signatures, cryptographic credentials, multi-factor authentication, and digital identity systems can help establish the identity of contracting parties.

AI systems should also operate within clearly defined authorization frameworks.

For example, an automated agent should not possess unrestricted authority to enter into transactions exceeding predetermined limits.

Authentication and authorization should therefore operate together.

10. Audit Trails

An AI-enabled contracting system should maintain appropriate records concerning important actions.

An audit trail may document:

- when an instruction was issued;
- what information was processed;
- which AI system was used;
- what recommendation was generated;
- who approved the transaction; and
- when the agreement was executed.

Such records can become particularly important when a dispute arises.

Reliable audit trails can help reconstruct the sequence of events and determine whether an automated action was authorized.

11. Liability for AI Actions

One of the most significant legal issues concerns liability.

Suppose an AI system enters into a contract that causes financial loss.

Potentially relevant parties may include:

- the system operator;
- the contracting organization;
- the software developer;
- the AI service provider; and
- other technology suppliers.

Responsibility should not automatically be transferred to the AI system itself.

AI does not independently possess conventional legal responsibility merely because it performs an automated action.

Legal accountability should therefore remain connected to identifiable human or organizational actors.

12. AI and Contractual Interpretation

AI may also be used to interpret contracts.

Organizations can use automated systems to identify obligations, deadlines, risks, and potentially conflicting provisions.

However, contractual interpretation often depends upon context, commercial purpose, and the relationship between the parties.

An AI system may identify linguistic patterns but fail to understand the complete commercial context.

Human legal judgment therefore remains important in complex contractual disputes.

13. Data Protection

AI-based contracting systems may process significant quantities of information.

This can include:

- names;
- contact details;
- financial information;
- transaction histories;
- business information; and
- contractual records.

Organizations must therefore establish appropriate data-governance practices.

Information should be collected and processed for legitimate purposes and protected against unauthorized access.

14. Cybersecurity of Digital Contracts

Digital contracts can become targets for cyberattacks.

Attackers may attempt to:

- steal authentication credentials;
- modify contractual records;
- compromise signing systems;
- manipulate automated agents; or
- gain unauthorized access to confidential agreements.

Security measures should therefore include encryption, strong authentication, access control, monitoring, and secure storage.

For high-value transactions, additional verification mechanisms may be appropriate.

15. Human Oversight

Human oversight should remain an essential component of high-impact automated contracting.

A practical model can distinguish between low-risk and high-risk transactions.

For routine transactions below a predefined threshold, automation may operate with limited intervention.

For high-value or strategically significant agreements, human approval should be required.
This creates a balanced approach:

Low Risk → Automated Processing

High Risk → AI Recommendation + Human Approval

16. Transparency and Explainability

Contracting parties should understand when AI significantly influences a contractual decision. Transparency does not necessarily require disclosure of every technical detail of an AI model.

However, organizations should be able to explain:

- the role of AI;
- the relevant decision-making process;
- the information considered; and
- the identity of the responsible organization.

Explainability becomes particularly important when an automated decision has significant financial consequences.

17. International Digital Commerce

Digital contracts frequently involve parties located in different countries.

This creates additional questions concerning:

- applicable law;
- jurisdiction;
- electronic signatures;
- cross-border transactions;
- data transfers; and
- recognition of electronic records.

AI-enabled contracting can increase the volume and speed of international transactions.

Legal systems will therefore need mechanisms capable of addressing automated cross-border contracting.

18. Proposed AI Contracting Framework

A responsible AI-contracting framework can consist of six stages.

Stage 1 – Identification

The parties and relevant digital identities are verified.

Stage 2 – Authorization

The AI system's permitted authority is clearly defined.

Stage 3 – AI Processing

The system analyzes contractual information and generates recommendations.

Stage 4 – Human Review

Important transactions are reviewed by an authorized person.

Stage 5 – Secure Execution

The final contract is executed through a secure electronic-signature mechanism.

Stage 6 – Audit and Monitoring

The transaction and subsequent contractual events are securely recorded.

This framework combines technological automation with human accountability.

19. Risk-Based Regulation

Not every AI-enabled contract creates the same level of risk.

A simple commercial transaction may require minimal human intervention.

A major financial agreement, employment contract, or strategic business transaction may require substantially greater oversight.

Regulation should therefore be risk-based.

Factors that may determine the required level of oversight include:

- financial value;
- sensitivity of information;
- potential impact on individuals;
- degree of AI autonomy;
- complexity of the transaction; and
- potential consequences of error.

20. Future of AI-Based Contracting

AI is likely to become increasingly integrated into commercial transactions.

Future systems may negotiate contractual terms, monitor performance, identify breaches, and automatically initiate remedial procedures.

AI may also interact with smart contracts and digital identity systems.

These developments could significantly reduce transaction costs.

However, greater automation will increase the importance of clear rules concerning authorization, liability, transparency, cybersecurity, and dispute resolution.

The future of contract law will therefore increasingly involve interaction between legal principles and computational systems.

21. Conclusion

Artificial intelligence is transforming the way contracts are drafted, negotiated, executed, and managed.

AI-assisted contracting can provide substantial benefits by reducing administrative work, analyzing complex documents, identifying contractual risks, and facilitating faster commercial transactions.

However, automated contracting also creates important legal challenges.

Questions concerning consent, authorization, attribution, contractual errors, liability, authentication, privacy, and cybersecurity become increasingly significant when AI systems participate in contractual processes.

A responsible approach should not treat AI as an independent legal actor. Instead, accountability should remain connected to the individuals and organizations that design, deploy, authorize, and operate automated systems.

A combination of secure digital identity, clearly defined system authority, audit trails, human oversight, explainability, cybersecurity, and risk-based governance can provide an appropriate foundation for AI-enabled contracting.

Ultimately, the future of digital contract law will depend upon achieving an effective balance between **automation and accountability**. AI can make contractual transactions faster and

more efficient, but technological efficiency should operate within a framework that preserves certainty, fairness, security, and meaningful human responsibility.

Declarations

Conflict of interest: The authors declare that they have no conflict of interest.

Funding: This review received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Ethical approval: Not applicable. This article is a review of published literature and did not involve human participants or animal subjects.

Data availability: No new data were generated or analyzed in support of this review. All sources relied upon are cited in the References.

Use of AI tools: No generative artificial intelligence tool was used in the conception, drafting or analysis of this article. The authors take full responsibility for the content.

Author contributions: Author contributed to the conception of the review, the survey of the literature, and the drafting and revision of the manuscript. Author read and approved the final version.