

1/2026 anteprima

Rivista di diritto dei media

ISSN 2532-9146

Bridging UNCITRAL and EU AI Governance: A Normative Proposal for the Regulation of Automated Contracting

Sharmin N. Chougule, María Luisa Mena-Durán

Table of contents

1. Introduction. – 2. The Expanding Role of AI in Contracting: Distinguishing AI-Assisted Formation from Automated Performance. – 3. UNCITRAL, European Legal Framework and Their Gaps. – 3.1 UNCITRAL Model Law and Automated Contracting. – 3.2 EU AI Act and other efforts. – 3.3 Wendehorst’s 2024 Discussion Draft: Principles for AI in Contracting. – 3.4 Limitations in the ELI and Wendehorst Frameworks. – 3.5 Other European Provisions impacting Contract Law and Consumer Protection. – 4. Common Law vs. Civil Law Approaches: Comparative Analysis: European Regulatory Initiatives vs. U.S. Common Law. – 5. Conclusion: Policy Considerations and Future Directions.

1. Introduction

The emergence of artificial intelligence in contractual processes challenges foundational principles of European private law, particularly those governing offer and acceptance, intention, attribution, and liability. Unlike traditional electronic contracting, which operates under deterministic systems that merely transmit predefined declarations of will, advanced AI systems increasingly participate in the formation and execution of contracts through autonomous decision-making, data-driven inference, and adaptive negotiation capabilities. This development raises substantive questions as to whether existing doctrines of consent and contractual responsibility suffice to regulate non-human agents that are capable of independently generating contractual terms or triggering contractual performance without direct human awareness.

The European Commission is currently debating whether to introduce dedicated regulation for automated contracting, weighing frameworks such as the UNCITRAL Model Law on Automated Contracting¹ against the

¹ United Nations Commission on International Trade Law (UNCITRAL), *UNCITRAL Model Law on Automated Contracting with Guide to Enactment*, New York, 2025, available at *un.org* (accessed 5 May 2025).

potential need for a more EU-specific legal structure. The Commission is also analysing the EU-specific efforts like the European Law Institute (ELI) Guiding Principles and Model Rules on Digital Assistants for Consumer Contracts (“ELI Guiding Principles”)² and Professor Christiane Wendehorst’s guiding principles (“Prof. Wendehorst’s Principles”).³ These discussions underscore the complex interplay between technological innovation and legal certainty and reveal a regulatory and doctrinal gap, particularly regarding contract formation, liability, and enforcement. This paper explores these efforts and the evolving regulatory landscape for automated contracting, also drawing on insights from the recent 2025 Münster Colloquia on EU Law and the Digital Economy (“Münster Colloquia”).⁴ A brief comparative analysis of European and United States (U.S.) approaches to automated contracting is given to shed light on differences between civil⁵ and common law countries.

This article argues that the European Union must adopt a hybrid regulatory model that, *de iure condito*, builds upon the principle of functional equivalence to recognise the validity of AI-generated contracts and, *de iure condendo*, introduces a differentiated liability regime allocating responsibility between the deployer and the developer of the AI system, together with mandatory transparency and human-oversight obligations to ensure accountability and trust. This model integrates and systematises elements drawn from UNCITRAL’s Model Law, the ELI Guiding Principles, and the AI Act, while filling their respective gaps through a unified doctrinal and regulatory framework.

In order to develop this thesis, the article is structured as follows. Section 2 clarifies the conceptual foundations of artificial intelligence in contracting, by distinguishing between AI-assisted contract formation and automated performance. Section 3 looks into UNCITRAL’s Model Law and European efforts specific to automated contracting and limitations of these efforts. Section 4 makes a comparison between civil and common law jurisdictions to gauge if common law jurisdictions have an advantageous position. This paper then concludes with a synthesis of findings and implications for the future development of European contract law.

² European Law Institute (ELI), *Guiding Principles and Model Rules on Digital Assistants for Consumer Contracts*, Vienna, 2025 (ISBN: 978-3-9505495-4-6).

³ C. Wendehorst, *Discussion Draft: Principles for AI in Contracting (Version 2.1)*, in *Journal of European Consumer and Market Law*, 1, 2024, 43 ss.

⁴ Münster Colloquia on EU Law and the Digital Economy, *Conference on AI and Automated Contracting*, University of Münster, 9-10 January 2025, available at jura.uni-muenster.de (accessed 8 January 2025).

⁵ On the prevalence of the civil-law tradition among EU Member States, see K. Zweigert – H. Kötz, *An Introduction to Comparative Law*, Oxford, 1998, 68 ss., noting that all continental EU jurisdictions belong to the civil-law family, with only Ireland and, partly, Cyprus following common-law traditions.

2. The Expanding Role of AI in Contracting: Distinguishing AI-Assisted Formation from Automated Performance

Automated contracting is no longer confined to theoretical discussions; it has permeated multiple industries, transforming transactional dynamics in finance, healthcare, real estate, supply chains, and legal services. AI-driven contract lifecycle management platforms such as KPMG's Cognitive Contract Management (CCM),⁶ IBM Watson-integrated ContractPodAi,⁷ and JPMorgan's COiN (Contract Intelligence)⁸ system demonstrate the growing reliance on algorithmic tools and automated contracting for contract drafting, negotiation, compliance monitoring, and enforcement in our very own legal field. AI-powered tools like Juro,⁹ Ironclad,¹⁰ and Evisort¹¹ automate contract lifecycle management, while Kira Systems¹² and LawGeex¹³ analyse agreements for risks and inconsistencies. DocuSign CLM¹⁴ streamlines contract execution, and IBM Watson Contract Analyzer¹⁵ assists with due diligence and compliance. Despite these advancements, human oversight remains critical to ensuring contractual accuracy and mitigating algorithmic biases, while acknowledging the persistent risk of automation bias.¹⁶ Also, the industry-specific applications of automated contracting and their implications for legal accountability may differ. The applications of automated contracting vary across industries, leading to different legal accountability challenges. For example, in finan-

⁶ KPMG, *Contract Transition in M&A: Accelerating Value with AI*, 2022, available at [kpmg.com](https://www.kpmg.com) (accessed 31 January 2025).

⁷ IBM, *Watson Discovery and ContractPodAi: Transforming Legal Excellence with AI*, 2023 available at [ibm.com](https://www.ibm.com) (Accessed 31 January 2025).

⁸ Superior Data Science, *JP Morgan COiN: A Case Study of AI in Finance*, 2023, available at [superiordatascience.com](https://www.superiordatascience.com) (Accessed 31 January 2025); Product Monk, *Meet COiN: JPMorgan's Efficiency Wizard*, 2023, available at [productmonk.io](https://www.productmonk.io) (Accessed 31 January 2025).

⁹ Juro, *AI-Powered Contract Automation for Businesses*, 2025, available at [juro.com](https://www.juro.com) (accessed 31 January 2025).

¹⁰ Ironclad, *Contract Lifecycle Management with AI*, 2025, available at [ironcladapp.com](https://www.ironcladapp.com) (Accessed 31 January 2025).

¹¹ Evisort, *AI-Driven Contract Intelligence for Legal Teams*, 2025, available at [evisort.com](https://www.evisort.com) (accessed 31 January 2025).

¹² Kira Systems, *AI-Powered Contract Analysis for Risk Management*, 2025, available at [kirasystems.com](https://www.kirasystems.com) (Accessed 31 January 2025).

¹³ LawGeex, *Automating Legal Contract Review with AI*, 2025, available at [lawgeex.com](https://www.lawgeex.com) (accessed 31 January 2025).

¹⁴ DocuSign, *Contract Lifecycle Management (CLM) Solutions*, 2025, available at [docusign.com](https://www.docusign.com) (accessed 31 January 2025).

¹⁵ IBM, *Streamline Contract Management with Watson AI*, 2024, available at [ibm.com](https://www.ibm.com) (accessed 31 January 2025).

¹⁶ Automation-bias research shows that lawyers and other professionals tend to rely uncritically on machine recommendations, amplifying the risk of undetected errors in automated contracting. On automation bias in legal work see P. Laux – C. Ruschmeier, *Automation Bias and the Need for Human Oversight in Contract Review*, Working Paper, 2021, available at [ssrn.com](https://www.ssrn.com) (accessed 31 January 2025).

ce, AI-driven contracts must comply with strict regulatory requirements, while in supply chains, they focus on efficiency and risk allocation. In healthcare, automated contracts must address patient data protection and liability concerns. These differences affect how legal responsibility is assigned, who is accountable for errors, and how disputes are resolved.¹⁷ This sets the stage for examining whether current legal frameworks adequately address the challenges of automated contracting in the next section.

In the context of algorithmic contracting, it is essential to distinguish between AI-assisted formation and automated performance, as each raises distinct legal considerations. AI-assisted formation involves systems that operate during the pre-contractual phase—drafting terms, negotiating conditions, or even autonomously concluding agreements, where questions of consent, intention, and offer-acceptance mechanics are critical. By contrast, automated performance concerns the execution or fulfilment of contractual obligations, such as payment processing or delivery scheduling, once a contract has already been formed. While the latter generally poses fewer doctrinal challenges, it may give rise to issues of liability and risk allocation in cases of malfunction or non-performance. Recognising this divide allows for a more precise analysis of how existing legal frameworks should adapt to the different functions AI systems perform within contractual relationships.

A closely related issue concerns the frequent confusion between algorithmic contracts and smart contracts, two concepts that overlap yet remain fundamentally distinct. While some authors treat these terms as interchangeable,¹⁸ closer analysis shows that their core functions emerge at different stages of the contractual lifecycle. Algorithmic contracts emphasise autonomy during the formation phase, as AI agents are capable of drafting, negotiating, or even determining contract terms with minimal human input. Smart contracts, by contrast, are primarily concerned with automation in the performance phase, executing contractual obligations automatically and without human intervention once predefined conditions are met.¹⁹ The technologies underlying these systems further illustrate their differences. Smart contracts are typically supported by cryptographic mechanisms and distributed ledger technologies (DLT), as seen in blockchain-based

¹⁷ In *Quoine v B2C2* [2020] SGCA(I) 2 an unattended pricing algorithm executed trades 250 × off-market and the platform later had to litigate the reversal. The case underscores that, even in ostensibly deterministic environments, human-in-the-loop controls remain indispensable for legal accountability.

In *Moffatt v. Air Canada*, 2024 BCCRT 149, the British Columbia Civil Resolution Tribunal found Air Canada liable for misinformation provided by its AI chatbot regarding bereavement fares. The tribunal ruled that Air Canada was responsible for the chatbot's inaccurate information, despite the airline's argument that the chatbot was a separate entity. This case is significant for establishing corporate accountability for information provided by AI systems on company websites.

¹⁸ J. Linarelli, *Artificial Intelligence and Contracts Formation: Back to Contract as Bargain?*, Working Paper No. 6, 2024, available at *ssrn.com* (accessed 25 July 2025); C. Wendehorst, *Discussion Draft: Principles for AI in Contracting*, cit., 49.

¹⁹ M. L. Mena Durán, *Artificial Intelligence in Contract Formation: The Shift from Automaton to Autonomy in the Case of Algorithmic Contracts*, Doctoral Thesis, King's College London, London, 2024.

platforms such as Ethereum, while algorithmic contracts rely more heavily on artificial intelligence and machine learning techniques to generate or refine contract terms.²⁰ Vitalik Buterin famously referred to smart contracts as autonomous software agents, but this characterisation blurs the line between automation (execution without human input) and autonomy (decision-making during contract formation).²¹ Scholars such as Scholz and Ebers emphasised the need to maintain this conceptual distinction to avoid regulatory and interpretative confusion.²²

The Law Commission's 2021 report on smart legal contracts provides helpful clarification by distinguishing between three categories of smart legal contracts:²³ (i) Natural language contracts with automated performance, where code merely executes pre-agreed obligations; (ii) Hybrid smart legal contracts, where natural language and code jointly define obligations and performance; and (iii) Solely code-based smart legal contracts, where all terms are defined and executed by code.

Algorithmic contracts partially overlap with the latter two categories but go beyond them by integrating AI's capacity for inference and autonomous decision-making in the formation phase. Thus, while smart contracts can be seen as execution tools, algorithmic contracts engage with the core contractual elements of offer, acceptance, and intention. Having established this conceptual foundation, Section 3 examines how international and European instruments address AI-driven contract formation.

3. UNCITRAL, European Legal Framework and Their Gaps

3.1 UNCITRAL Model Law and Automated Contracting

In July 2024, UNCITRAL finalised the Model Law on Automated Contracting (MLAC), a significant global benchmark for addressing AI and automation in contract formation. The UNCITRAL Model Law builds upon earlier e-commerce instruments (like the 1996 Model Law on Electronic Commerce and the 2005 Electronic Communications Convention) and aims to overcome legal obstacles to automated contracting by providing internationally accepted rules for recognising contracts made by automa-

²⁰ M. Ebers, *Artificial Intelligence, Contracting and Contract Law: An Introduction*, in M. Ebers – C. Poncibò – M. Zou (eds.), *Artificial Intelligence and the Law of Contracts*, Oxford, 2022, 19 ss.

²¹ V. Buterin, *A Next Generation Smart Contract & Decentralized Application Platform*, White Paper, 2014.

²² L. H. Scholz, *Algorithmic Contracts*, in *Yale Law Journal*, 128, 2017, 566 ss.; L. H. Scholz, *Algorithms and Contract Law*, in W. Barfield (ed.), *The Cambridge Handbook of the Law of Algorithms*, Cambridge, 2020, 141 ss.; J. Linarelli, *Artificial General Intelligence and Contract*, in *Law, Innovation and Technology*, 11, 2019, 330 ss.; Lord Sales, *Law and the Digital World*, Sir Henry Brooke Annual Lecture, 16 April 2021; C. Poncibò, *Artificial Intelligence as a Communication Tool in Contract Law*, in *European Review of Private Law*, 31, 2023, 239 ss.

²³ Law Commission of England and Wales, *Smart Legal Contracts: Advice to Government*, Law Com No 401, 2021.

ted systems. While not binding, the MLAC is intended as a template for national legislatures and possibly the EU to adopt or adapt, thereby harmonising approaches across jurisdictions.

The MLAC provides a foundational approach to regulating AI-assisted contract formation by distinguishing between deterministic and non-deterministic systems.²⁴ A deterministic system follows a set of predefined rules and always produces the same output for a given input. There is no randomness or unpredictability in its operations, but there can be errors. Examples include smart contracts, particularly those using a certain programming language. Researchers have found that Solidity's compilation to bytecode enables syntax error detection at compile-time, while runtime errors remain difficult to catch and typically occur during contract execution.²⁵ A non-deterministic system, more precisely described as a stochastic system in the context of machine learning, involves elements of randomness or learning. This means the same input may yield different outputs depending on various factors, such as how the AI model was trained, stochastic processes like data shuffling or dropout during training, or the exposure to novel data post-deployment. Although the model's internal logic remains algorithmically deterministic, these probabilistic outputs are characteristic of AI-driven contract negotiations, where machine lear-

²⁴ While the UNCITRAL Model Law calls such systems “non-deterministic”, machine-learning components are more precisely stochastic. Randomness is typically injected during training (e.g., data shuffling, stochastic-gradient updates), whereas the trained model's inference step is algorithmically deterministic, identical weights plus identical input always yield the same output. After the training, no random sampling is involved unless you explicitly add it (e.g., Monte-Carlo dropout, sampling from a language model with temperature > 0).

Once the system is applied in a real environment, what might disappear is predictability in the everyday sense, because the model can be exposed to inputs it has never seen. Those outputs are probabilistic estimates applied to novel data, the system's behaviour can remain uncertain and may be best characterised as stochastic rather than merely non-deterministic.

A critical distinction undergirding these technologies is the opacity of algorithmic reasoning, the lack of transparency in how an algorithm reaches its decisions or conclusions, manifesting through the inability to understand, access, or explain its reasoning process. This opacity may stem from intentional concealment (trade secrets, proprietary systems), technical complexity inherent in neural networks and machine learning models, or deliberate design choices favouring closed systems. Importantly, opacity must be distinguished from the black box problem, which constitutes a subset of opacity where reasoning is fundamentally unknowable even to the system's creators. While opacity denotes the inaccessible or unexplained nature of algorithmic reasoning, a condition potentially remediable through transparency obligations and disclosure mechanisms, the black box represents an epistemologically distinct phenomenon in which the reasoning remains inherently inscrutable. This distinction carries direct legal consequences for contract formation: opacity may be addressable through auditability requirements and explainability obligations, whereas the black box problem raises deeper questions about whether meaningful human oversight or informed consent is feasible at all. As automated contracting increasingly relies on non-deterministic AI systems capable of autonomous adaptation, this conceptual framework proves essential for calibrating liability, transparency, and accountability regimes.

²⁵ N. Atzei – M. Bartoletti – T. Cimoli, *A Survey of Attacks on Ethereum Smart Contracts (SoK)*, in M. Maffei – M. Ryan (eds.), *Principles of Security and Trust. POST 2017*, Lecture Notes in Computer Science, vol. 10204, Berlin – Heidelberg, 2017, 164 ss.

ning models predict terms based on context rather than fixed rules. This stochastic nature challenges the traditional assumptions of predictability and reliability in contract law. However, as a model law, it lacks direct applicability at the EU level and does not comprehensively address liability allocation, unexpected AI-driven actions, or consumer protection concerns. Also, since this is a supranational law, there are questions whether the MLAC's principles sufficiently align with European regulatory needs or whether additional legislative measures are necessary.

The MLAC emphasises technology neutrality and non-discrimination. Using an AI or algorithm to form a contract should not cause the contract to be denied legal effect just because no human was directly involved. This principle of non-discrimination against electronic agents echoes earlier e-commerce law and is now expressly extended to highly autonomous AI contracting. The MLAC also underscores party autonomy: parties remain free to choose whether to use automated systems in contracting and to tailor how those systems operate by agreement (subject to mandatory law).²⁶ In essence, automation is to be accommodated within the existing fabric of contract law, not treated as an alien phenomenon.

The MLAC provides concrete rules to ensure the validity and enforceability of contracts formed by AI-powered digital assistants. Notably, art. 5 states that a contract formed using an automated system shall not be denied validity or enforceability on the sole ground that no natural person reviewed or intervened in the process. This directly addresses contract formation certainty: even if two AI programs negotiate and agree on terms with zero human involvement at the time of agreement, the resulting contract is as valid as any traditional contract. Art. 5 (with an optional paragraph for contract performance) essentially enshrines that lack of human awareness is no defence to contract enforcement, a critical clarification for AI-to-AI contracting scenarios.

MLAC further tackles contracts in code and dynamic terms. Art. 6 ensures that contracts are not invalid merely because their terms are represented in computer code or incorporate data that changes continuously (for example, an IoT contract with price terms linked to market data feeds). This provision is forward-looking: it legitimises smart contracts where obligations might be encoded in software and contracts that self-modify based on external data sources, both increasingly relevant with AI systems that adjust terms on the fly.

On the question of attribution and liability, art. 7 provides a default rule: actions taken by an automated system are attributed to the party on whose behalf the system operates. Specifically, between contracting parties, the parties can agree on an attribution rule (e.g. if using a third-party AI platform, they might allocate responsibility by contract). In the absence

²⁶ M. S. Gal, *Algorithmic Challenges to Autonomous Choice*, in *Michigan Technology Law Review*, 25, 2018, 59 ss., 63. By choosing to entrust algorithms with the negotiation or drafting of obligations, parties implicitly accept the legal and practical consequences of outcomes determined by complex, data-driven processes. While this delegation may diminish predictability and direct oversight, it remains consistent with the principle of freedom of contract, which binds individuals to the results of their voluntary choices; see M. L. Mena Durán, *Artificial Intelligence in Contract Formation: The Shift from Automaton to Autonomy in the Case of Algorithmic Contracts*, cit.

of such an agreement, the law attributes the action to the person who uses the system for that purpose. In practical terms, if a company deploys an AI agent to negotiate a deal, that company is responsible for the AI's contracting acts as if it had done them itself. Critically, art. 7(3) adds that attribution is not negated «on the sole ground that the outcome was unexpected». In other words, a party cannot escape a contract by arguing that its AI agent behaved in unforeseen ways, at least not automatically; the act is still attributed to them. This tackles the liability issue of AI malfunctions or unanticipated behavior: the default position is that the user of the AI bears the risk. However, MLAC recognises that this issue is delicate, so it leaves room for other laws to determine the consequences of such attribution in extreme cases (for instance, contract law doctrines of mistake or consumer protection rules could still apply via art. 7(4)). This discussion can be further refined by drawing on Cristina Frattoné's distinction between automation mistakes and autonomy mistakes. Automation mistakes refer to errors caused by technical faults or data issues, essentially failures in execution, whereas autonomy mistakes stem from the AI system's independent, though logic-based, decision-making that leads to unintended outcomes.²⁷ Introducing this distinction may help clarify the types of unexpected AI actions addressed under the attribution framework in art. 7(3) of MLAC, and when the exceptional rule in art. 8, which permits a party to avoid enforcement of an action attributed to them in unforeseen cases, might apply.

The question of terminology, whether to designate the human party as “user”, “operator”, or “deployer”, is non-trivial. While the EU AI Act adopts “deployer” for the entity putting AI into use, contract law scholarship often prefers “operator” to emphasise active control over parameters. This article adopts “operator” to capture both the party using the AI and the one responsible for setting its contractual objectives, consistent with Wendehorst's framing.

Prof. Florian Möslin at the Münster Colloquia²⁸ examined how AI-driven contract formation necessitates a recalibration of classical contract law principles, particularly regarding the role of default rules in establishing standard terms when algorithmic systems negotiate on behalf of parties. Prof. Möslin argues that the allocation of liability between the deployer, developer, and other stakeholders involved in automated tran-

²⁷ C. Frattoné, *Algorithmic Mistakes in Machine-Made Contracts: The Legal Consequences of Errors in Automated Contract Formation*, in *Uniform Law Review*, 28, 2023, 407 ss., available at doi.org (accessed 31 January 2025).

²⁸ F. Möslin, *AI Contracting and Default Rules*, paper presented at the Münster Colloquia on EU Law and the Digital Economy, Conference on AI and Automated Contracting, University of Münster, 9–10 January 2025, available at jura.uni-muenster.de (accessed 13 November 2025).

The challenge of reconciling algorithmic autonomy with legal attribution extends to default contractual rules. AI systems that autonomously negotiate contracts must be accompanied by explicit default rule frameworks. Prof. Möslin argues that civil law jurisdictions, which rely heavily on mandatory default rules, face particular challenges when algorithmic systems operate without human intervention during critical negotiation phases, requiring a recalibration of both statutory and contractual default mechanisms to protect party interests and ensure legal certainty.

sactions requires explicit contractual design and legislative intervention to ensure that default rules do not inadvertently disadvantage parties or create unintended legal consequences.

To address truly aberrant AI behaviour, the Model Law includes an optional provision, art. 8, on unexpected actions. This provision (which states can choose to enact or not) creates a narrow exception: if an automated system's action is attributed to Party A, the other Party B cannot enforce that action as part of the contract if, under the circumstances, (a) Party A could not reasonably have expected the action, and (b) Party B knew or should have known Party A didn't expect it. This effectively codifies a kind of mistake/knowledge²⁹ rule for AI outputs: it prevents opportunistic enforcement of a contract term that one party's AI agreed to, when the other party realised it was a mistake or out-of-scope. Art. 8 thus introduces a measured safety valve for the most unanticipated AI-driven transactions, protecting parties from being bound by egregious AI errors – but only where the other side had reason to know something was amiss. The inclusion of this optional rule acknowledges that while automation should generally bind the user, fairness may require exceptions in edge cases of AI unpredictability. States worried about abuse could opt not to enact art. 8 or could tighten their standards.) This narrow unexpected actions exception in art. 8 closely mirrors the common-law doctrine of unilateral mistake, which voids a contract when one party was fundamentally mistaken about a term and the other party knew or ought to have known of the mistake. Both art. 8 and the unilateral mistake doctrine aim to prevent opportunistic enforcement of agreements when true assent was absent or impaired.

The MLAC also touches on transparency and disclosure indirectly. Art. 9 (Information requirements) clarifies that nothing in the model law overrides any existing legal obligations to disclose information about the design or operation of an automated system. In other words, if other law, perhaps consumer law or financial regulations, imposes duties to inform the counterparty or a regulator about how an AI negotiator works, those duties remain intact. Art. 9 importantly signals the importance of information disclosure in the operation of automated systems, as UNCITRAL's summary notes, but the model law itself stops short of imposing new disclosure mandates. It defers to other applicable law to require transparency about AI use (for instance, a national law could require businesses to inform consumers when they are contracting with an AI). The model law's stance here is cautious: it acknowledges transparency as a concern but leaves specifics to national policymakers, likely because appropriate disclosure might vary by context (B2B vs B2C, etc.). Under art. 50 of the EU AI Act, businesses are required to inform individuals when they interact with an AI system, unless this is obvious from the context.³⁰ While this obligation will apply from August 2026, national laws can already

²⁹ J. Tan Ming En, *Non-deterministic Artificial Intelligence and the Future of the Law on Unilateral Mistakes in Singapore*, in *Singapore Academy of Law Journal*, 34, 2022, 93 ss.

³⁰ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on Artificial Intelligence (AI Act), in OJ L 168, 13.6.2024, p. 1–153, art. 50.

adopt such provisions in advance. The UNCITRAL Model Law, by deferring to existing or future national laws, accommodates varying levels of transparency across jurisdictions. In contrast, the U.S. currently lacks a binding federal requirement of this nature, while the UK is considering sector-specific transparency measures.³¹

Finally, art. 10 (Non-avoidance) ensures no one can use AI to circumvent legal obligations. It states that a party cannot be relieved from the legal consequences of failing to comply with a law on the sole ground that it used an automated system. This is a catch-all rule of accountability: using an AI agent is not a get-out-of-jail-free card for legal duties. For example, if consumer protection law requires certain contract terms or procedures, a trader can't escape liability by blaming its AI for not following the law.

Collectively, the UNCITRAL Model Law provides a blueprint for addressing the fundamental uncertainties of AI contracting. The UNCITRAL Model Law on Automated Contracting (2024) has similar legal consequences to those established by Directive 2000/31/EC (the E-Commerce Directive), in that it confirms the validity of contracts formed through technological means. Like the Directive's affirmation of electronic contracting, the Model Law does not alter the substantive rules of contract formation but rather ensures that the use of automated systems does not undermine the legal effect or enforceability of agreements, thereby promoting certainty and functional equivalence in digital commerce. It establishes baseline validity of AI-formed contracts, a default liability allocation (attribution to the user of AI), a possible escape hatch for extreme AI-generated mistakes (art. 8) and reaffirms transparency and accountability principles. While comprehensive in these respects, UNCITRAL deliberately scoped the model law as a modest overlay to existing contract law, not a complete code. It does not seek to address legal issues beyond the contractual setting and does not cover AI ethics or algorithmic fairness, which are beyond contract law. Some complex issues, like how to handle AI systems that are non-deterministic (learning systems whose actions are not fully predictable even by their programmers), are not deeply regulated by the model law beyond the general rules noted. The Guide to Enactment (forthcoming) likely provides further guidance on such issues.

For EU purposes, the MLAC offers a ready-made solution that could be adopted (perhaps with tweaks) to harmonise AI contract law across Member States. It addresses many of the key points of legal uncertainty (formation validity, attribution of liability, etc.) in a balanced way. The question the European Commission faces is whether simply encouraging adoption of the MLAC (at national or EU level) is sufficient, or whether an alternative version with additional provisions is needed. A relevant criticism previously articulated by Emily Weitzenboeck in relation to the Model Law on Electronic Commerce, the UETA, UCITA, and Directive 2000/31/EC, also applies to the UNCITRAL Model Law on Automated Contracting. While these instruments affirm the legal validity of contracts formed through technological means, they do so without providing sub-

³¹ UK Department for Science, Innovation and Technology (DSIT), *A Pro-Innovation Approach to AI Regulation: Government Response*, 6 February 2024, available at gov.uk (accessed 9 May 2025).

stantial doctrinal justification or engaging with foundational principles of contract law.³² The regulatory emphasis remains on functional equivalence and legal certainty, but this often comes at the expense of a deeper theoretical account of autonomy, intention, and consent in technologically mediated contracting. As noted at Münster, the MLAC's generality may leave certain gaps, for instance, specific guidance on non-deterministic AI that the model law doesn't explicitly distinguish. Issues like dynamic renegotiation by AI or biased decision-making might require more tailored rules (perhaps around consumer consent or auditability). These are areas where the ELI Principles³³ and Prof. Wendehorst's draft³⁴ step in, potentially proposing additional provisions beyond UNCITRAL's baseline.

3.2 EU AI Act and other efforts

Beyond international initiatives, European scholars and institutions have developed complementary studies.³⁵ While the EU AI Act establishes overarching rules for AI governance,³⁶ it does not explicitly regulate automated contracting. There is an absence of provisions addressing contract attribution of risks and liability, disclosure obligations, and mechanisms for addressing unexpected AI-generated contract outcomes.³⁷ Insights from

³² E. M. Weitzenboeck, *Electronic Agents and the Formation of Contracts*, in *International Journal of Law and Information Technology*, 9, 2001, 204 ss.

³³ ELI, *Guiding Principles and Model Rules on Digital Assistants for Consumer Contracts*, cit.

³⁴ C. Wendehorst, *Principles for AI in Contracting*, cit.,

³⁵ At the Münster Colloquia:

F. Möslin, *AI Contracting and Default Rules*, cit. Prof. Florian Möslin (Philipps-University Marburg) has specifically addressed how algorithmic contracting challenges traditional default rule mechanisms in civil law jurisdictions, particularly regarding how deployer liability interacts with the formation of AI-generated contracts.

C. Twigg-Flesner, *Attribution of Pre-contractual Information and Knowledge: The ELI Model Rules on Algorithmic Contracts and Beyond*, paper presented at the Münster Colloquia on EU Law and the Digital Economy, Conference on AI and Automated Contracting, University of Münster, 9–10 January 2025, available at jura.uni-muenster.de (accessed 13 November 2025).

Prof. Christian Twigg-Flesner (University of Warwick) examined how pre-contractual information and knowledge attribution must be recalibrated within the ELI Model Rules on Algorithmic Contracts, particularly given the challenges of ensuring that algorithmic systems adequately disclose material terms and risks to consumers before contract formation.

C. Busch, *Augmented Consumers and Algorithmic Consumers in AI Contracting*, paper presented at the Münster Colloquia on EU Law and the Digital Economy, Conference on AI and Automated Contracting, University of Münster, 9–10 January 2025, available at jura.uni-muenster.de (accessed 13 November 2025). Complementing this analysis, Prof. Christoph Busch (University of Osnabrück) investigated the transformation of consumer agency in AI-driven transactions, arguing that algorithmic contracting requires a reconceptualization of the consumer as both an augmented party (enhanced by decision-support tools) and a vulnerable subject requiring protective mechanisms against algorithmic opacity and bias.

³⁶ Regulation (EU) 2024/1689.

³⁷ The European Union does not possess a general competence to harmonise contract law. Its regulatory interventions rely primarily on art. 114 TFEU, which supports measures necessary for the functioning of the internal market, and art. 169 TFEU, concerning

ELI Guiding Principles and Prof. Wendehorst's Principles provide additional considerations for addressing these legal gaps.

The ELI, an independent non-profit organisation that develops law reform proposals, has been at the forefront of crafting a European-specific approach to AI in contracting. The ELI Guiding Principles and Model Rules on Digital Assistants for Consumer Contracts (DACC Model Rules) project of 2022–2025 focuses particularly on the use of automated decision-making (ADM) and AI in consumer contracts, though many principles are broadly applicable.³⁸ The rationale is that consumer protection law faces distinct challenges when AI tools so-called digital assistants act on behalf of consumers or traders in transactions. The project's first phase produced an ELI Interim Report on EU Consumer Law and Automated Decision-Making (Dec 2023) assessing the adequacy of the existing EU consumer acquis for Automated Decision-Making, and setting out general principles for adaptation. The second phase, formulated the actual Guiding Principles and DACC Model Rules (a quasi, "black letter" framework) for algorithmic contracts, B2C and C2B contexts in depth.

The ELI Guiding Principles and DACC Model Rules were formally adopted on 15 April 2025 and published on 19 May 2025. Structured into five chapters comprising articles with commentaries, the Model Rules establish general principles, design requirements for digital assistants, legal frameworks governing their supply, regulation of algorithmic contracts, and third-party liability provisions. ELI observes that algorithms and AI are now used in all phases of the contract lifecycle, from advertising/offers, to negotiation and formation, to performance and enforcement. This raises questions both of validity (are these AI-mediated contracts legally sound?) and fairness (are consumers adequately protected when, say, their AI-powered digital assistant contracts with a seller's algorithm?). The goal is to ensure Europe has a clear and predictable legal framework that both enables innovation allowing automated contracting to flourish and ensures effective safeguards for parties' rights and interests, especially weaker parties like consumers. In ELI's view, increased legal certainty for automated contracting is vital to unlock AI's economic potential while maintaining trust.

The European Law Institute Interim Report identified eight guiding principles aimed at adapting EU consumer law to the challenges posed by algorithmic decision-making and AI-driven contracting, each of which reveals specific areas requiring regulatory clarification. First, it addresses the attribution of AI-powered digital assistant's actions to the consumer, clarifying when and under what conditions a consumer should be legally

consumer protection. Consequently, EU legislation in this area is limited and sector-specific, targeting issues that affect cross-border transactions. Key instruments include Directive 93/13/EEC on unfair terms in consumer contracts, which prohibits clauses that create a significant imbalance to the detriment of the consumer, and Directive 2011/83/EU on consumer rights, which harmonises pre-contractual information duties, the right of withdrawal, and rules for distance and off-premises contracts. However, fundamental aspects of contract law such as formation, validity, and interpretation remain under the competence of the Member States.

³⁸ ELI, *Guiding Principles and Model Rules on Digital Assistants for Consumer Contracts*, cit.

bound by actions autonomously undertaken by their AI-powered digital assistant. Second, the Report reaffirms that consumer law continues to apply fully to algorithmic contracts, ensuring that protective mechanisms such as the right of withdrawal and information duties remain effective even when contractual interactions occur through AI intermediaries rather than through direct human engagement. Third, it examines the fulfilment of pre-contractual information duties, seeking to determine how mandatory disclosures can be meaningfully provided in scenarios where an AI system, rather than the consumer, is responsible for the decision-making process. Fourth, it includes a principle on non-discrimination, which aims to prevent AI systems from generating discriminatory outcomes, such as personalised pricing or filtered offers that could disadvantage certain consumer groups. Fifth, it considers disclosure obligations related to the use and functioning of automated decision-making systems, requiring transparency regarding the deployment of AI in contractual processes. Sixth, the report introduces the need to protect digital assistants from manipulation, particularly by preventing traders from influencing the behaviour of AI-powered digital assistant through misleading or strategically engineered data inputs. Seventh, it emphasises the necessity of determining and disclosing the operational parameters governing digital assistants, thereby ensuring that consumers have clarity over the criteria according to which their AI-powered digital assistant negotiates or concludes contracts. Finally, it highlights the issue of conflicts of interest, calling for regulatory safeguards to address situations in which the operator of a consumer's AI-powered digital assistant may have interests of its own, such as commercial affiliations, that could distort the assistant's decision-making to the detriment of the consumer.

These principles collectively aim to make consumer law AI-ready, ensuring that fundamental safeguards (like informed consent, fairness, and transparency) are preserved in an era of automated contracting. The Interim Report concluded that most existing EU consumer directives are almost ADM-ready with only minor adjustments needed. For example, rules on providing contract terms or withdrawal rights can largely accommodate AI but perhaps need explicit clarification that if an AI concludes a contract, the consumer can still exercise their rights. The report recommended that a few new provisions be added to align the law with the ELI principles.

DACC Model Rules affirm that contracts formed by AI are valid, but will stress aligning the AI's actions with the intent of the human parties. Wendehorst's Principles, discussed later in this paper, emphasise the importance of aligning AI's actions with the intent of the contracting parties. This implies a principle that even if AI negotiates, it must operate within the scope of authority given by the user. The human party's intent³⁹ (perhaps as configured in the AI's parameters) is key. Following Sartor's terminolo-

³⁹ M. Herbosch, *Contracting with Artificial Intelligence: A Comparative Analysis of the Intent to Contract*, in *Rabels Zeitschrift für ausländisches und internationales Privatrecht*, 88, 2024, NIX, 1 ss. Herbosch addresses the role of intent in contract formation: the "distance between the abstract intent to form a contract and the specific contract that the system output may have formed". Refer to the "limited value of intent" as stressed by the ECJ jurisprudence that human intent often plays a constrained role in binding contract formation.

gy, since the ultimate objective is always set by the human operator, delegating the decision-making process to AI merely explains the attribution of intent to the user, rather than creating any independent intention on the part of the AI. If the AI deviates, the law should have a way to discern whether the resulting contract reflects any real agreement. This aligns with the principle that intent, at least under English law, is tested objectively: the focus is on whether a reasonable observer would interpret the AI's actions as representing the user's manifested intent.⁴⁰ Wendehorst/ELI appear to advocate clarity that AI is a tool of its user not an independent actor with its own intent.⁴¹

The DACC Model Rules stress the need for clarity in attributing accountability for AI's actions to its deployers, whether natural or legal persons. This mirrors UNCITRAL's approach: the party deploying is generally responsible. Consumers and traders using AI assistants are bound by their AI's actions as if performed personally, subject to protective exceptions. In consumer cases, attribution to the consumer was principle number 1 likely ensuring a consumer isn't denied a remedy just because their AI-powered digital assistant clicked the button, but also possibly ensuring the consumer can be held to a contract their AI-powered digital assistant made if it was operating under their authority. The flip side is liability of traders using AI-powered digital assistant: if a business's AI errs, the business should be accountable to the consumer. Both aspects reinforce that the legal person behind the AI bears the consequences, not the AI itself since AI has no legal personality.

The DACC Model Rules require that parties especially businesses disclose their use of AI in negotiations or contract formation to the other side particularly if the other side is a consumer. Indeed, the ELI principles propose mechanisms such as pre-contractual disclosures to ensure AI systems operate within agreed legal and business objectives. For instance, a trader's duty might include informing a consumer that an algorithm, not a human, will assess their offer and on what basis at least in general terms. This ties into fairness, a consumer should know if they are dealing with a bot and how that might affect them. This approach aligns with art. 50 of the EU

⁴⁰ Smith v. Hughes (1871) LR 6 QB 597.

⁴¹ J. Linarelli, *A Philosophy of Contract Law for Artificial Intelligence: Shared Intentionality*, in M. Ebers – C. Poncibò – M. Zou (eds.), *Contracting and Contract Law in the Age of Artificial Intelligence*, Oxford, forthcoming, available at [papers.ssrn](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4811111) (accessed 9 May 2025).

Linarelli deepens this point that legal frameworks may evolve to recognise more nuanced or distributed forms of intent, especially when decisions emerge from complex, semi-autonomous systems. It complements ELI/Wendehorst's view that contracts formed by AI must still reflect the human party's purpose and scope of authority.

Lirikë Kamberi, *The Integration of AI in Contract Law: Formation, Enforcement, and Legal Challenges from an International Perspective*, Master's Thesis, University of Vienna, 2023, available at [phaidra.univie.ac.at](https://phaidra.univie.ac.at/handle/document/28111), 28 ss.

Kamberi offers a clear and relevant analysis of intent in AI contracting. She explains that, under the objective theory, contracts formed by AI can be valid if the AI's actions outwardly manifest intent, even without human involvement at the moment of formation. She also acknowledges that this works well for "weak AI" but may fall short as strong AI systems act more autonomously, potentially requiring a shift toward recognizing more nuanced or hybrid forms of intent. I believe that in terms of a deterministic system, intent can be met to a certain extent at least.

AI Act, which requires businesses to inform individuals when they interact with an AI system, unless this is evident from the context.⁴² Although this obligation will only apply from August 2026, national legislators could adopt similar provisions earlier. ELI's vision arguably goes further, as it suggests that relevant operational parameters, such as the conditions under which a consumer's digital assistant automatically agrees to purchases, should be transparent to ensure genuine consent and to prevent traders from exploiting undisclosed settings. Such disclosure obligations address the power imbalances and information asymmetry inherent in AI-driven interactions, thereby supporting fairness, informed decision-making, and consumer trust.⁴³

It could also include disclosure of certain parameters: e.g., if the consumer's own AI-powered digital assistant is set to auto-buy items up to a certain price or with certain data access, those parameters might need to be transparent so the consumer consents and the trader cannot exploit unknown settings. Greater transparency obligations would address power imbalances and information asymmetry introduced by AI.

Given ELI's awareness of unexpected outcomes/outputs as a key issue requiring harmonisation, the Model Rules incorporate a rule akin to UNCITRAL's art. 8 or other fallback liability provisions. The proposals, such as fall-back liability provisions and procedural safeguards, aim to address accountability for unexpected AI actions. For example, DACC Model Rules provide that if an AI's action falls outside a consumer's reasonable expectations, perhaps contrary to the consumer's given instructions or usual preferences, and the business knew this or should have known, then the consumer is not bound. This would protect consumers from, say, their AI-powered digital assistant making an absurd purchase due to a glitch. Traders, meanwhile, might be protected if their AI-powered digital assistant was manipulated by the other side or if an outcome was probably not intended. Essentially, ELI recommends a safety net in line with equitable principles to handle AI-induced errors or misalignment, very much in spirit with UNCITRAL's optional rule but perhaps tailored for consumer scenarios.

The DACC Model Rules impose design requirements ensuring consumers remain in control of digital assistants through parameter-setting, contract prevention mechanisms, and deactivation capabilities. Additionally, the Model Rules require digital assistants to be protected from manipulation, preventing traders from exploiting or biasing consumer-deployed AI. Conflicts of interest arising from digital assistant use must be disclosed, addressing situations where AI operators have commercial affiliations distorting decision-making to consumers' detriment.

ELI's project coordinated closely with UNCITRAL. ELI representatives participated as observers in UNCITRAL Working Group sessions, ensuring cross-fertilisation and consistency. ELI does not reinvent basic validity and attribution rules but supplements them with European consumer law perspectives, particularly mandatory disclosures and fairness checks.

⁴² Regulation (EU) 2024/1689, art. 50.

⁴³ F. Di Porto, *Algorithmic Disclosure Rules*, in *Artificial Intelligence and Law*, 31, 2023, 13 ss.

While UNCITRAL leaves disclosure to other law, ELI mandates explicit disclosure obligations. Similarly, UNCITRAL's optional approach to unexpected outcomes becomes a structured consumer protection mechanism in the DACC Model Rules framework.

Both the ELI Model Rules and Wendehorst's draft remain non-binding as of late 2025, though the published DACC Model Rules represent the most comprehensive transnational soft law dedicated to digital assistants. They are designed to inspire EU or national legislation and guide courts in the interim. As Wendehorst notes, these principles aim to «[g]uide the application of existing law and the development of new law in relation to automated contracting».⁴⁴ In Europe's civil law tradition, such principles can influence judicial reasoning even before formal adoption, given the absence of statutory guidance on AI contracts.

3.3 Wendehorst's 2024 Discussion Draft: Principles for AI in Contracting

Professor Christiane Wendehorst's "Discussion Draft: Principles for AI in Contracting (Version 2.1)" is an influential academic contribution that complements the ELI project.⁴⁵ It sets out proposed legal principles addressing automated contracting with advanced AI. Wendehorst's contribution is significant in that it distills the core issues and corresponding solutions into a coherent set of principles, thereby addressing the uncertainty she identifies in this area.⁴⁶ As an academic draft, it doesn't have legal force, but it has been discussed at conferences (including the Münster Colloquium) and informs the ELI's work (Wendehorst is co-reporter on the ELI project).

Wendehorst notes that the proliferation of highly autonomous electronic agents in contracting has outpaced legal adaptation.⁴⁷ She observes that around the world, the first major disputes involving AI contracts are reaching courts, yet basic questions, e.g., should liability lie with the AI's developer, the user, the AI itself, or someone else – lack clear answers. There is surprisingly little legislation on automated contracting, creating gaps in legal certainty.⁴⁸ Thus, her draft principles aim to provide clarity and guide both application of existing law and the development of new law. They are meant as a template or inspiration for legislators and judges, similar in spirit to restatements or model principles in other fields.

Prof. Wendehorst's draft allows a clear understanding of the substance and structure of the proposed principles.

The Principles for AI in Contracting affirm that the use of AI in contracting does not negate the validity of a contract, aligning with the approach taken in UNCITRAL instruments and in U.S. frameworks such as

⁴⁴ C. Wendehorst, *Discussion Draft: Principles for AI in Contracting*, cit., 43.

⁴⁵ *Ibid*

⁴⁶ C. Wendehorst, *Principles for AI in Contracting*, cit., 16 ss.

⁴⁷ *Ibid.*, 1 ss.

⁴⁸ *Ibid.*, 1 ss., 12 ss.

the UETA. They confirm that machine-generated communications (data messages) may constitute legally relevant declarations of will, even in the absence of contemporaneous human awareness, and that contracts concluded with the assistance of AI should not be denied effect on the basis of form or capacity requirements alone. This position mirrors traditional doctrines on formality and capacity, under which the lack of real-time human presence does not preclude contractual validity where intent and expression are established. Consistently with UNCITRAL and UETA, the Principles anchor intention in the human decision to deploy and configure the system:⁴⁹ i.e., the «intention flows from the programming and use of the machine».⁵⁰ This anchors validity in the user's decision to entrust the AI, rather than requiring a real-time human intent.

A core principle is that AI systems have no independent legal intent; their actions must be attributable to a legal person. Wendehorst emphasises aligning AI actions with the parties' intent, which implies a principle that an AI's actions are deemed the actions of the party on whose behalf it operates (similar to UNCITRAL art.7 and UETA Section 14). This reflects classical agency principles, particularly those involving automated representatives, where the principal bears legal responsibility for authorised actions. She likely frames it as an agency principle for AI: the deploying party bears responsibility for the AI's contracts.⁵¹ This would resolve the “who is bound?” question in favour of the human/business behind the AI, not the developer or the AI. However, Wendehorst's introduction also raises the possibility of looking at the developer or something else in cases of unanticipated transactions. That suggests her principles might include guidance on when a developer or third party could be liable, possibly not in contract since the developer isn't party to the contract, but perhaps in compensation to the user for the AI's error. The primary contract-law rule, however, is likely that between the contracting parties, the one who put forth the AI is treated as making the contract. This is consistent with ELI's stance that AI is an agent of its deployer.

Wendehorst appears to advocate for transparency obligations. Her principles likely call for parties to disclose when they are using AI in contracting and possibly to disclose certain characteristics of the AI if relevant to the other party's decision. This ensures informed consent in AI-mediated

⁴⁹ P. Cramer – J. Mollod – C. Rimmer, *Contract Law in the Age of Agentic AI: Who's Really Clicking Accept?*, in *newmedialaw.proskauer.com*, 8 April 2025.

⁵⁰ *Ibid.*

⁵¹ On the varied terminology used to describe parties interacting with AI systems, see E. Mik, *Much Ado About Artificial Intelligence or: The Automation of Contract Formation*, in *Journal of Business Law*, 2021, 501 ss., 505; A. Ooi, *Artificial Intelligence and Party Attribution in Contract Formation*, in *Journal of Law and Technology*, 15 (2024), 99–100. The EU Artificial Intelligence Act adopts the term “*deployer*” to describe the entity that puts an AI system into use, although this designation is uncommon in contract-law discourse. See also T. Allen – R. Widdison, *Can Computers Make Contracts?*, in *Harvard Journal of Law and Technology*, 9 (1996), 25 ss., 39; M. S. Gal, *Algorithmic Challenges to Autonomous Choice*, in *Michigan Technology Law Review*, 25 (2018), 59 ss., 63. In line with C. Wendehorst's *Principles for AI in Contracting*, this study uses the term “*operator*” to capture both the party relying on the AI system and the party responsible for configuring it: C. Wendehorst, *Principles for AI in Contracting*, cit., 43 ss., 49.

dealings. It ties to ELI's pre-contractual disclosure principle. For instance, a principle might be that a party using an AI system to negotiate or conclude a contract should inform the other party of that fact, unless it is apparent from the circumstances. Such a rule would protect, say, a consumer from unknowingly negotiating against a sophisticated algorithm and, conversely, allow a business to understand if it is dealing with an AI-driven request. Additionally, if the AI has known limitations or propensities, e.g., it cannot process certain information, or it prioritises certain factors, disclosing that could be important, especially in consumer contexts or where asymmetry exists.

Although contract principles might not heavily delve into AI design, Wendehorst might include a principle addressing the duty of those deploying AI to use appropriate systems and prevent harm. For instance, a notion that if you employ an AI in contracting, you should ensure it has been properly tested/monitored so as to avoid causing contractual harms like severe errors. If not a formal principle, this concern is reflected in suggestions that law might look at the developer for certain faults.⁵² In the absence of specific regulation, this could translate into an implied obligation of diligence in using AI.

Wendehorst clearly is concerned with AI making unanticipated transactions or transactions resulting from technical errors.⁵³ One of her principles likely deals with the scenario of AI mistakes. Perhaps a principle akin to, if an AI system makes a contract beyond the scope authorised by its user due to an autonomous decision or error, the law should provide appropriate remedies (such as voidability) when enforcement would be unjust, and the counterparty knew or should have known of the mistake. This echoes UNCITRAL's unexpected outcome rule but could be framed in more general contract law terms (mistake, lack of true assent, etc.). This scenario closely resembles the doctrine of unilateral mistake, which precludes enforcement when one party is aware, or ought to be aware, of the other's error and seeks to exploit it. Wendehorst might propose criteria for when a contract is not binding due to AI deviation, balancing the need for reliability in automated contracts with fairness. Fall-back liability provisions and procedural safeguards are contemplated to handle unexpected AI actions, suggesting a structured approach to exceptions.

Implicitly, the principles reject treating the AI as a contracting party.⁵⁴

⁵² C. Wendehorst, *Principles for AI in Contracting*, cit., 41 ss., 26 ss.

⁵³ *Ibid.*, 2 ss., 23.

⁵⁴ Scholarly debates on the legal personhood of artificial agents have evolved from early explorations of electronic agents as semi-autonomous contracting entities: J.-F. Lerouge, *The Use of Electronic Agents Questioned Under Contractual Law*, in *Journal of Computer & Information Law*, 18, 1999, 403 ss.; I. Kerr, *Ensuring the Assent of Electronic Agents*, in *Berkeley Technology Law Journal*, 17, 2001, 123 ss.; A. J. Bellia, *Contracting with Electronic Agents*, in *Emory Law Journal*, 50, 2001, 1047 ss., these authors rejected the notion of granting legal personhood, emphasising the absence of consent, patrimony, or liability. E. M. Weitzenboeck, *Electronic Agents and the Formation of Contracts*, cit., examined personhood as one of several doctrinal solutions but found it unworkable. Later, F. Andrade et al., *Contracting Agents: Legal Personality and Representation*, in *Artificial Intelligence and Law*, 15, 2007, 357 ss., revisited the concept, drawing analogies with corporate entities but acknowledging unresolved difficulties in liability and enforcement. More recent

Wendehorst's framing always involves attributing to some human/legal person. This affirms the foundational principle that legal subjectivity and contractual capacity reside in natural or legal persons, not in tools or technologies. This is an important policy stance, differing from a hypothetical radical solution of granting AI legal personality (an idea floated in European Parliament discussions years ago but largely dismissed). By confirming AI is not a legal subject but a tool, the principles channel responsibility to existing persons.

Wendehorst likely stresses that clarity is needed not just nationally but ideally internationally. While not a principle per se, her commentary encourages jurisdictions to align, hence her support of UNCITRAL's global model. This is more of a meta-point in her paper: that global consistency on fundamental rules like the validity of AI contracts is desirable to avoid legal fragmentation as automated contracts span borders.

Prof. Wendehorst's draft, being version 2.1, indicates it's evolving. It was first drafted in 2022 and refined through 2023–early 2024. The evolution likely incorporated feedback from developments like the UNCITRAL drafting sessions and interim ELI findings. At the 2025 Münster Colloquium, her principles were discussed and lightly referred to as Wendehorst's Principles, indicating they were a key reference point. They, together with the ELI Principles, highlight the consensus in Europe that AI in contracting should be treated through the lens of existing contract law doctrine (intent, attribution, consent) but sharpened with specific guidance and safeguards.

Importantly, Wendehorst is quoted as stressing the need for developing principles that can inspire future law and guide courts. She acknowledges both the dearth of legislation and the scarcity of case law to date on these issues.⁵⁵ Her approach is thus proactive: rather than wait for courts to improvise solutions, articulate principles now to shape consistent evolution of the law. This pragmatic yet forward-looking approach resonates with practitioners, it provides a reference for advising clients today, in contracts, one might incorporate some of these ideas in clauses allocating risk of AI error, for instance, and paves the way for eventual codification.

Wendehorst's principles aim to demystify AI contracting by mapping it onto familiar legal concepts: contracts formed by AI are still contracts offer/acceptance still applies, just via electronic agents;⁵⁶ the mind behind the contract is the human who deployed the AI;⁵⁷ information duties and good faith require transparency about AI involvement;⁵⁸ and if AI misfires, traditional doctrines like mistake, duty to correct errors, etc., should

approaches, such as G. Sartor, *Cognitive Automata and the Law: Electronic Contracting and the Intentionality of Software Agents*, in *Artificial Intelligence and Law*, 17, 2009, 253 ss., and S. Chopra – L. White, *A Legal Theory for Autonomous Artificial Agents*, University of Michigan Press, 2011, shift focus from legal personhood to attribution, agency principles, and the intentional stance.

⁵⁵ C. Wendehorst, *Principles for AI in Contracting*, cit., 3 ss.

⁵⁶ *Ibid.*, 25, 34.

⁵⁷ *Ibid.*, 3, 24, 40.

⁵⁸ *Ibid.*, 36.

be invoked to prevent unfairness.⁵⁹ Her framework thus illustrates that AI contracting, while novel in mechanism, does not require a reinvention of contract law; rather, it calls for doctrinally consistent adaptations. These principles are a bridge between the status quo and a future where either legislation is enacted or case law develops providing an interim set of guidelines for all stakeholders.

3.4 Limitations in the ELI and Wendehorst Frameworks

While both discuss AI as a tool, they do not fully account for situations where AI exceeds its programmed scope or makes contract-related decisions that are unforeseeable by its human operator. The principle of full attribution to the human operator assumes control over AI behavior, but in cases where machine learning-based AI autonomously adapts and modifies its own parameters, traditional liability frameworks become inadequate. Future legal frameworks should clarify whether strict liability, vicarious liability, or a novel AI-specific liability should apply when an AI breaches contractual terms autonomously or acts contrary to commercial expectations.⁶⁰ This is particularly crucial for B2B environments, where AI is increasingly used to negotiate, amend, and execute contracts without direct human supervision. A liability framework should distinguish between deterministic AI tools and self-learning AI systems, setting thresholds for attribution, foreseeability, and fault in AI-related breaches.

By attributing contractual responsibility to the AI operator/deployer, both implicitly relegate developer liability to secondary or non-contractual terrain. However, this allocation proves inadequate where AI system defects originate in design, training, or algorithmic architecture rather than operator error. A coherent framework must distinguish between operator liability (for authorised use and parameter-setting) and developer liability (for system design failures). The distinction matters particularly where developers retain control over core AI behaviour: algorithmic decision-making, training datasets, output boundaries, and known limitations. Under European law, the proposed AI Liability Directive (currently withdrawn) contemplated rebuttable presumptions of causality favouring victims against developers. While contract law itself cannot impose privity-based liability on non-contracting parties, tort law, particularly the revised Product Liability Directive, can hold developers accountable for defective AI systems that cause contractual harm. A developer should bear liability where: (i) the AI system contains a defect in design or training that causes foreseeable contractual errors; (ii) the developer failed to disclose known limita-

⁵⁹ *Ibid.*, 3, 5, 9.

⁶⁰ In February 2025, European Commission, *Withdrawal of the Artificial Intelligence Liability Directive Proposal*, 2025, citing “no foreseeable agreement” among EU institutions. The AILD aimed to harmonize non-contractual civil liability rules for AI-related harm, introducing measures such as a rebuttable presumption of causality and disclosure obligations. The withdrawal raised concerns about legal fragmentation and the adequacy of existing liability frameworks for AI-induced damages across Member States.

tions or vulnerabilities; or (iii) the system's autonomous capabilities exceed those reasonably marketed to operators. This tiered approach preserves the operator's primary attribution while creating incentives for developers to exercise due diligence in system design and transparency, thereby closing the producer accountability gap left open by current contract-focused instruments.

Both documents lack explicit provisions requiring AI transparency in automated contracting. Given the complexity of machine learning models, contracting parties, particularly consumers, may be unaware of how AI-generated contract terms are formed. This raises fairness, accountability, and interpretability concerns, as parties may not have access to clear justifications for AI-driven contractual decisions. EU consumer law must address the rise of AI-powered assistants ("Custobots") in consumption decisions, including the need to balance mandatory disclosures, AI vulnerabilities, and potential shifts in information duties as AI systems take on more decision-making roles.

A regulatory framework should mandate AI explainability and auditability, ensuring that contracting algorithms provide human-readable explanations of key contract terms, risks, and obligations. Additionally, data provenance and input validation mechanisms should be required to trace how contractual decisions are made, preventing fraud, manipulation, or unfair contractual obligations. The EU AI Act's high-risk AI classification should apply to AI-driven contract negotiation tools, imposing stricter compliance obligations.

Neither document fully examines blockchain-based smart contracts and their interaction with traditional contract law. While Prof. Wendehorst's Principles acknowledge algorithmic contracting, they do not address self-executing smart contracts on distributed ledger technologies (DLTs), which pose unique legal challenges, including immutability, automation risks, and lack of legal override mechanisms. When fusing the AI aspect to the smart contract through IOT, for example, in the case of parametric insurances for payouts, it is important to address the issues of contract formation and performance. Also, to note, what is applicable to AI contracting in legal terms but is not directly applicable to AI-driven or AI-infused smart contracts.

Further, in terms of the EU law on smart contracts, art. 36 of the Data Act introduces a unique provision on smart contracts in data-sharing agreements, ensuring safe termination and compliance safeguards.⁶¹ While it acknowledges their role in data governance, it does not explicitly establish them as the primary enforcement tool for data-sharing obligations. But is it foolproof? Not entirely. The EU's stance on automated contracting, including deterministic AI in this context and smart contracts, remains an evolving challenge. Art. 36 lacks clear technical enforcement mechanisms and leaves critical gaps in compliance, reversibility, and liability. The effectiveness of this provision will depend on its implementation, industry standardisation, and the development of interoperable frameworks that

⁶¹ Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act), in OJ L 342/1, 22.12.2023, art. 36.

bridge legal and technological constraints.

Both documents assume that existing contract law applies to AI-generated contracts without addressing jurisdictional conflicts in cross-border AI contracting. When an AI system autonomously forms a contract across multiple jurisdictions, questions arise concerning which legal framework applies, how disputes should be resolved, and whether AI-generated agreements can be enforced extraterritorially. This is particularly relevant for autonomous trading algorithms, AI-powered supply chain contracts, and cross-border smart contracts, where the governing law may be unclear or contested. Future regulatory frameworks should include default jurisdictional rules for AI-driven contracts, possibly modelled on private international law principles such as those found in the Rome I Regulation (EU) and the Hague Principles on Choice of Law.⁶² Additionally, AI-generated contracts should include explicit jurisdictional clauses to mitigate uncertainty and ensure enforceability.

Both documents lack concrete requirements for human oversight in AI-driven contracting. While AI can autonomously execute contracts, certain high-risk transactions, such as financial agreements, healthcare service contracts, or consumer credit agreements, should include mandatory human-in-the-loop (HITL) review mechanisms. AI-driven contracts should be subject to tiered oversight levels, where high-value or high-risk transactions require human approval while low-risk, standardised contracts can proceed autonomously. Additionally, businesses deploying contracting AI systems should maintain real-time monitoring systems to detect unexpected deviations, potential legal violations, or contract execution failures. Establishing audit logs for AI decisions would ensure accountability and provide regulators with evidence in case of disputes.

Both documents overlook the need for interoperability standards in AI contract generation systems. Currently, AI contracting systems operate in silos, using proprietary algorithms and data models that hinder cross-platform compatibility. A lack of standardisation creates legal uncertainty when AI systems interpret contract clauses differently across platforms. Establishing global AI contracting standards, similar to INCOTERMS for international trade contracts,⁶³ would enhance predictability, enforceability, and compatibility across AI-driven legal frameworks. Additionally, an ISO-style regulatory framework for AI contracting could define baseline rules for AI contract negotiation, execution, and dispute resolution.

Neither document sufficiently addresses data privacy risks in AI-driven contract generation. AI contracting systems rely on large datasets to predict contract terms, personalise agreements, and assess contractual risks, but

⁶² Regulation (EU) No. 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Brussels I Recast); Regulation (EC) No. 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II); Regulation (EC) No. 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I).

⁶³ International Chamber of Commerce (ICC), *INCOTERMS® 2020: Rules for the Use of Trade Terms in Domestic and International Contracts*, Paris, 2019.

this raises GDPR compliance issues when personal data is processed without explicit consent. Contracting platforms should be required to implement data minimisation principles, transparency in AI decision-making, and opt-out mechanisms for automated contract personalisation. Furthermore, privacy-preserving AI techniques, such as federated learning or homomorphic encryption, should be encouraged to ensure that contract data is processed securely without exposing sensitive information.

3.5 Other European Provisions impacting Contract Law and Consumer Protection

Current platform regulations, such as the E-Commerce Directive (2000/31/EC),⁶⁴ provide a foundation for addressing certain aspects of algorithmic decision-making, particularly in the context of online services. However, these directives fall short of comprehensively regulating automated contracting. The E-Commerce Directive focuses on ensuring transparency and liability exemptions for information society services, yet it does not address the complexity of automated decisions, such as dynamic contract modifications or platform-driven AI-based decisions that impact contractual relationships. For a more thorough regulatory framework, this section explores whether existing legal frameworks are sufficiently adaptable to AI-driven contracting or whether specific measures addressing AI's evolving role in contract law, along with targeted legislative reform, are required.

The scarcity of legal cases on automated contracting is notable. Because discussions remain largely hypothetical in the absence of litigation, observers (including Prof. Wendehorst) have focused on developing guiding principles to pre-emptively clarify the law. Such scarcity of legal cases on automated contracting can be attributed to a combination of factors. On one hand, existing foundational elements of contract formation, or what we can refer to as rules under the Principles of European Contract Law (PECL),⁶⁵ which are specific, structured norms that directly determine legal outcomes, such as offer, acceptance, and intention, are broad and flexible enough to address disputes involving automation, potentially reducing the need for litigation. On the other hand, a lack of awareness about the unique challenges posed by automated contracting, such as attribution of actions and liability for errors, might deter parties from bringing these issues to court. Furthermore, businesses often resolve disputes informally or through private arbitration to avoid setting legal precedents that could lead to regulatory scrutiny. Prof. Wendehorst highlights the «surprisingly

⁶⁴ Given that the E-Commerce Directive (Directive 2000/31/EC) confirms the legal validity of contracts concluded by electronic means, it can be understood to extend to contracts concluded by AI systems, insofar as the contract is formed through an electronic process. While the Directive does not explicitly mention artificial intelligence, its technology-neutral language and objective of facilitating electronic commerce support the interpretation that AI-driven contract formation falls within its scope.

⁶⁵ Commission on European Contract Law, Principles of European Contract Law (PECL).

little legislation on automated contracting» but not the scarcity of legal precedents.⁶⁶ Prof. Wendehorst stresses the need for developing principles that can inspire the future development of law as well as guide courts and practitioners in future automated contract-related disputes.

ELI Guiding Principles and Prof. Wendehorst’s Principles give solid scaffolding for consumer AI contracting basics but leave the heavier structural beams of data governance, cross-border enforcement, B2B use, bias audits, agency doctrine, and IP ownership for later builders to install. Prof. Wendehorst’s Principles are drafted for general automated contracting, whereas ELI focuses only on consumer deals. Business-to-business, platform-to-consumer, and “custobot” supply-chain scenarios therefore still lack a coherent framework. Neither instrument sets out how to decide the forum, applicable law, or enforcement when an AI agent concludes a transaction across multiple countries, a gap already flagged by private-international-law commentators.⁶⁷ Common-law questions such as when a human principal is bound (or can revoke) an AI agent’s acts, or how to unwind an unauthorised order, are still “murky waters” in practice.⁶⁸ Both texts expect non-manipulation, but they stop short of prescribing concrete bias-testing, fairness metrics, or redress mechanisms for high-risk agent misalignment that regulators are now demanding. Questions over who owns and who is liable for IP generated or infringed by autonomous agents are highlighted in current case law commentary but are not tackled in either set of principles. Further, the pending EU Digital Fairness Act is a consumer-interface fix, not a full AI-contracting code. It targets dark patterns, addictive design, influencer marketing and profiling transparency, and aims to plug those specific fairness gaps in current consumer law. It says nothing about ratification rules for autonomous agents, cross-border contract law, B2B deals, IP ownership or other open issues we listed, so most of those gaps remain.

4. Common Law vs. Civil Law Approaches: Comparative Analysis: European Regulatory Initiatives vs. U.S. Common Law

Another consideration in this regard is the flexibility of common law systems. Unlike codified legal systems, common law jurisdictions rely on a precedent-based approach, which shapes the evolution of contract law through judicial decisions. While common law is often perceived as more adaptable due to the absence of a comprehensive civil code, judicial constraints, such as adherence to precedent, also play a significant role in shaping its application.⁶⁹ As has been observed in legal theory, certainty and

⁶⁶ C. Wendehorst, *Principles for AI in Contracting*, cit., 3.

⁶⁷ W.S. Galkin, *AI Impact on Contract Law*, in *galkinlaw.com*, 9 May 2025.

⁶⁸ Lewis Silkin LLP, *The Rise of AI Agents: Pizza, Parameters and Problems*, in *lexology.com*, 28 January 2025.

⁶⁹ For a more in-depth analysis of the superior effectiveness of common law as opposed to civil law see N. Garoupa – C.G. Ligerre, *The Syndrome of the Efficiency of the Common Law*,

flexibility in law often serve overlapping purposes. While certainty aims to provide stability and predictability, flexibility ensures that legal norms remain adaptable to new and unforeseen circumstances.⁷⁰ This tension is especially pronounced in the domain of automated contracting, where evolving technologies demand both consistent application and context-sensitive adaptation. How this approach interacts with the complexities of automated contracting remains an open question, as it may allow for nuanced interpretations based on emerging cases while also presenting challenges in ensuring consistency and predictability.

Assuming that the common law's adaptability can be advantageous, it evolves through judicial decisions, allowing courts to interpret and adapt contract law elements in the context of AI systems. This adaptability provides a valuable framework for addressing novel issues, such as determining liability for AI's autonomous actions or assessing whether AI systems align with the contractual intent of the parties. As AI technology progresses, common law jurisdictions may be positioned to develop innovative solutions, influencing global discussions on regulating algorithmic contracts.

However, this flexibility does not come without its challenges. While the U.S. may be seen as a favourable environment for AI-driven corporate ventures due to its legal flexibility, there are concerns about the protection of contractual parties, particularly consumers and smaller businesses, who may not have the same negotiating power as large corporations and their decision makers (typically board members). The absence of comprehensive regulation on automated contracting in the U.S. means that the contract law under the Uniform Commercial Code (UCC)⁷¹ and state-level common law serve as the governing framework, supplemented by sector-specific regulations where applicable. Yet, this reliance on existing legal structures raises questions about the sufficiency of protections for less powerful parties in the face of technological advancements and the increasing dominance of major corporate players.

Additionally, the U.S. legal framework provides protections for businesses through mechanisms such as freedom of contract and intellectual property rights. However, it is important to note that intellectual property law, particularly in the context of AI technologies, has faced significant scrutiny due to the unprecedented number of claims regarding violations of IP rights. These cases have highlighted some of the limitations of IP law, particularly in addressing the unique challenges posed by AI's autonomous capabilities.

In terms of legislation, many U.S. states have enacted or at least supplemented their legislation addressing blockchain technology, smart contracts, and verifiable credentials. These legislative efforts aim to provide legal recognition and frameworks for the use of smart contracts and related technologies within their jurisdictions. However, this reference is limited in scope, as the focus here is on automated contracting, which extends beyond smart contracts to include AI-driven contract formation,

in *Boston University International Law Journal*, 29, 2011, 287 ss.

⁷⁰ M. Sales, *Certainty and Flexibility in Legal Norms*, Working Paper, 2025, 2.

⁷¹ Uniform Law Commission, *Uniform Commercial Code (UCC)*.

execution, and enforcement. Prof. Wendehorst highlights the limited legislative attention to automated contracting, with existing laws such as the U.S. Uniform Electronic Transactions Act (UETA) 1999,⁷² the Model Computer Information Transactions Act (MCITA) (1999/2002),⁷³ and the Draft UCC Article 2 (2003)⁷⁴ only offering partial guidance rather than a comprehensive legal framework. Prof. Wendehorst observes, these offer «partial guidance rather than a comprehensive legal framework». UETA covers formation and signatures, MCITA, only law in two states, addresses software licensing and has provisions on electronic errors, and the UCC drafts would have addressed electronic contracting in sales. But none squarely grapple with advanced AI autonomy or liability nuances. Thus, gaps remain – for example, if an AI behaves fraudulently (could the user be liable for fraud if they didn't know the AI would do that?), or how to handle AI collusion (antitrust law question), or whether an AI's "knowledge" could be imputed to the principal for purposes like contract enforcement, e.g., noticing an offer term that a human might have overlooked. These questions the common law will handle incrementally. The U.S. approach, favouring freedom of contract and existing legal structures, raises questions about the sufficiency of protections for less powerful parties in the face of major corporate players. A big AI user (say, Amazon) and a consumer are not on equal footing; without specific rules, the consumer relies on courts to protect them via general doctrines. There's an ongoing debate in U.S. legal circles about whether any new laws are needed (some have proposed updates to the UCC or new uniform laws to address AI agents, but nothing concrete has passed).

The U.S. handles AI contracting under status quo contract law: valid if it looks like a contract, the user bears responsibility, there are no special duties to disclose AI use, and terms stand unless voidable under traditional defenses. It's a pragmatic approach that treats AI as just another tool (like a telephone or fax in earlier times) rather than a game-changer that demands new contract rules. This minimisation of legal change works well for now in many scenarios, but it may be tested by more complex AI behaviours. U.S. law, being largely reactive, will evolve as cases present new twists, a process that could lead to unique precedents (case law) rather than a cohesive statute.

A U.S. Professor, at the Münster Colloquia it was argued that, despite the unpredictable nature of automated contracting, the existing guardrails in contract law can still protect consumer intent.⁷⁵ This assertion reinforces the argument that common law's inherent flexibility, coupled with judicial interpretation, aims to provide a safety net for contractual parties, ensuring that AI-driven contracts remain aligned with fundamental legal

⁷² Uniform Law Commission, *Final Act – 2021 Uniform Law Commission Drafting Committee*, 2021.

⁷³ *Ibid.*

⁷⁴ Uniform Law Commission, *Uniform Commercial Code (UCC), Draft Article 2*, 2003.

⁷⁵ H. Gabriel, *What Does It Mean to Have "The Intention to Contract" in an AI Contract?*, paper presented at the Münster Colloquia on EU Law and the Digital Economy, Conference on AI and Automated Contracting, University of Münster, 9–10 January 2025, available at jura.uni-muenster.de (accessed 13 November 2025).

principles. For instance, courts can invoke the covenant of good faith if one party's AI behaviour undermines fair dealing, or they can interpret contracts in light of reasonableness to prevent AI literalism from imposing harsh outcomes. Indeed, courts can still use the existing guardrails of contract law to protect consumers. The fact that they can use them does not, however, make those contractual rules the most adequate.

The U.S. stance is underpinned by a belief in the flexibility of common law to evolve organically. As noted, common law adapts through judicial decisions; American courts can extend principles or create nuanced distinctions as new fact patterns (like AI contracting disputes) come before them. Proponents of this approach argue it allows innovation to flourish without waiting for legislation and avoids the risk of rules that might soon become obsolete in the face of rapidly advancing AI tech. This view was echoed at the Münster Colloquium by the U.S. professor. The flip side is the concern that common law development may be slow and uneven. Until many cases are litigated, uncertainty remains. And common law evolution happens through often costly litigation, which can be burdensome, especially for individuals or small businesses. Additionally, American common law's adaptability might be constrained by adherence to precedent, a court might feel bound by old analogies that don't perfectly fit AI contexts. There's also the issue of fragmentation: with 50 state jurisdictions, different courts might reach divergent conclusions on AI-related issues, leading to inconsistency though adoption of UETA by most states mitigates some differences on formation.

The European and U.S. approaches to AI contracting reveal a philosophical divide: *ex ante* rulemaking and harmonisation versus *ex post* adjudication and flexibility. This section compares how each addresses the key issues of contract formation, liability allocation, disclosure, and enforceability, highlighting the implications for legal certainty and party protection. Both jurisdictions ultimately affirm that contracts formed by AI are valid, but they arrive there differently. In Europe, the intent is to explicitly codify this principle (through instruments like the UNCITRAL MLAC and potential EU laws) to remove any doubt. Art. 5 of UNCITRAL and Wendehorst's first principles provide clear statutory assurance that lack of human involvement is no cause for invalidity. The U.S., by contrast, relies on existing legal principles (UETA and case law) that have already implicitly or explicitly recognised automated contracting (Uniform Electronic Transactions Act n.d.). UETA's adoption in 49 states gives near-uniform coverage, so practically there isn't doubt in the U.S. either that AI contracts can be valid. The difference is one of framing: the EU would articulate this in new legislation (for coherence across member states), whereas the U.S. points to the established e-commerce laws and says the matter is settled. For cross-border contracts, Europe's approach might foster greater confidence if, say, an EU directive mandated all member states to honour AI-formed contracts akin to the MLAC, reducing choice-of-law concerns. However, in the European Union, the regulation of contract formation remains primarily within the competence of the Member States. General principles governing the creation of contracts, such as offer, acceptance, intention to create legal relations, and capacity, are rooted in national pri-

vate law traditions and have not been subject to comprehensive harmonisation at the EU level. The EU lacks a general legislative competence over contract law and may only act in this area when it intersects with specific competences conferred by the Treaties, such as consumer protection (art. 169 TFEU) or the functioning of the internal market (art. 114 TFEU). Accordingly, the EU has adopted targeted directives that regulate aspects of contract formation in defined contexts, notably in cross-border consumer contracts and digital transactions, such as the E-Commerce Directive (2000/31/EC) and the Consumer Rights Directive (2011/83/EU).⁷⁶ These instruments harmonise certain elements, like information duties and the right of withdrawal, but leave the broader framework of contract formation untouched. Thus, while EU law influences certain sectors, the foundational rules governing how contracts are formed remain a matter of national legal autonomy. It will be rather interesting to see how this will be dealt with by the Commission after the UNCITRAL's MLAC.

The U.S. approach has already harmonised state law via UETA for domestic purposes. Both approaches are thus aligned on outcome (validity), but Europe's is more proactive and uniform by design, whereas the U.S.'s is uniform by voluntary adoption of a model act and judicial consensus.

Europe is introducing the idea (through ELI/Wendehorst) of aligning AI actions with human intent explicitly. That serves to reassure that even if an AI acts, we conceptually trace it back to a human's intention (at least at the point of deploying the AI or setting parameters). U.S. law similarly uses the fiction of the user's intent being present via programming.⁷⁷ The main difference is that European discussions might lead to an explicit requirement that AI systems be used in a way that honours the intended agreement of the parties, possibly even implying an obligation to avoid or correct outcomes that stray from what the parties actually wanted.⁷⁸ U.S. law would handle that if it rises to the level of mistake or misrepresentation, but not otherwise. So, Europe could see a slightly more subjective bend (protecting actual intent), whereas the U.S. is firmly objective (if the AI manifested assent, that's the contract, regardless of unexpressed intent).

⁷⁶ Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, in OJ L 304, 22.11.2011, 64 ss.

⁷⁷ P. Cramer – J. Mollod – C. Rimmer, *Contract Law in the Age of Agentic AI*, cit.

⁷⁸ Although not a piece of perfection, the European paradigm, underpinned by both the ELI/Prof. Wendehorst touches on embedding explicit legal obligations within AI system design to ensure that automated negotiation tools operate *strictly* in alignment with the parties' intended agreement. The ELI framework operationalises eight high-level principles into 25 enforceable model-rule articles requiring design mandates that not promise to only empower the consumer but build in legal triggers for corrective action where AI-generated terms diverge from agreed intent. Meanwhile, Prof. Wendehorst's principles serve as the policy blueprint, emphasising attribution of digital assistant actions to the deploying user, extension of consumer-law coverage to algorithmic contracts, transparency, no-barrier access, and conflict-of-interest disclosure, all of which underpin an architecture in which deviation is not tolerated and must be corrected. Together, these initiatives suggest a legal regime in which AI systems may indeed bear explicit obligations to honour intent with built-in design controls and enforceable consumer-law mechanisms that mandate detection and correction of any outcome inconsistent with what the parties actually agreed.

Here, Europe leans toward clarity and possibly a bit of new allocation in extreme cases, whereas the U.S. sticks to traditional allocation (user liable) with narrow escape routes. UNCITRAL's default (user of AI is bound) mirrors UETA's rule: both converge on the principle that the person who uses an AI agent bears the consequences of its actions.⁷⁹ So, there is strong transatlantic alignment on the baseline rule of attribution. The difference emerges with Europe's consideration of unexpected outcomes. The UNCITRAL model (with art. 8) explicitly gives the defrauded/erroneously bound party an out if certain conditions are met. ELI and Wendehorst also contemplate fall-back liability rules for unexpected AI behaviour, likely meaning a structured relief maybe shifting liability to the other party or allowing contract avoidance. The U.S. has no statutory equivalent; it would rely on general doctrines and the equitable sense of a judge. In practice, a U.S. court might reach a similar result to an art. 8 scenario by saying there was no meeting of minds or by rescinding for mistake if the other party should have known. But it's not guaranteed – it requires judicial discretion. The European route seeks to ensure legal certainty by defining when an AI-caused contract isn't enforceable, whereas the U.S. leaves it uncertain but flexible.

Another point: Europe's discussions include developer liability or third-party liability in the context of AI contracting. While contract law itself in Europe will likely not impose contract liability on developers (privity remains between contracting parties), the EU is concurrently exploring AI liability in tort (the proposed and withdrawn AI Liability Directive and revised Product Liability Directive). This means Europe is thinking more holistically: if an AI defect causes contractual damage, perhaps the developer can be held accountable through those instruments. The U.S. similarly would use product liability tort to handle developer fault. So, both see that as outside contract law but relevant for overall liability.

One more subtle distinction: agency law vs. sui generis rules. The U.S. could apply agency concepts (like apparent authority) if, for example, someone's AI makes a deal, and a third party reasonably believes it was authorised. Europe might incorporate a similar idea. UNCITRAL allows parties to define attribution rules contractually, but by writing explicit rules, they might supersede or supplement traditional agency doctrine. A European regulation might say that the operator of the AI is deemed to have given it authority up to X, leaving less ambiguity. In the U.S., a scenario where a rogue AI did something arguably unauthorised could become a factual agency dispute (with potential outcomes of binding or not).

This is a notable divergence. European initiatives strongly emphasise transparency obligations, e.g., ELI's principles on pre-contractual information and disclosure duties.⁸⁰ The EU tends to impose duties to inform in consumer law (consider the extensive information requirements in consumer rights directives). It is likely that any EU approach to AI contracting will require at least that consumers are informed when they are interacting

⁷⁹ P. Cramer – J. Mollod – C. Rimmer, *Contract Law in the Age of Agentic AI*, cit.

⁸⁰ European Law Institute (ELI), *Interim Report: EU Consumer Law and Automated Decision-Making (ADM)*, Vienna, December 2023, available at europeanlawinstitute.eu

with an AI (complementing the AI Act's general transparency rule) and possibly that businesses disclose certain algorithmic practices. This is seen as necessary to ensure informed consent and trust in AI-mediated deals. The U.S., valuing freedom of contract and minimal interference, has not required such disclosure (except in niche state laws).

As a result, if a European and an American company each deploy an AI negotiator, the European one might be legally required to tell its counterpart that you are dealing with an AI agent, whereas the American one wouldn't unless California BOT law applied or it was in a context that triggers AI Act transparency to EU users. Over time, this could mean European consumers will expect to be told about AI involvement and can object or ask for human oversight, whereas American consumers might not even know. The practical effect is that Europe's approach could enhance fairness and autonomy; humans can decide to continue or ask for a human agent, but it may introduce overhead and potential friction in automated processes. The U.S. approach allows seamless AI-to-human or AI-to-AI interactions without mandated interruptions, arguably fostering efficiency.

Another aspect of transparency is explainability or disclosing AI parameters. The ELI principle 7 about determination/disclosure of parameters hints that Europe might require companies to disclose key factors or constraints of their AI systems in consumer contracts.⁸¹ For example, if an AI car-buying service only searches certain dealerships or won't consider cars above a certain mileage, maybe the consumer should know that. U.S. law would consider that purely the user's responsibility or the service's voluntary feature, no law compels such detail.

Ultimately, Europe appears poised to bake transparency and disclosure obligations directly into the contracting framework (or at least strongly encourage them via model rules), whereas the U.S. relies on general anti-fraud and market forces for transparency. This reflects the broader regulatory philosophies: the EU tends to impose positive duties on businesses for consumer protection, while the U.S. often relies on policing fraud and letting the rest be governed by contract and competition.

The EU has a more paternalistic tradition in consumer contracts, unfair terms control, mandatory rights, etc., and this will extend to AI. EU consumer law is being reviewed for ADM-readiness, as ELI did, ensuring that if an AI contract might circumvent some consumer rights, the law is adjusted. The ELI interim report found the directives mostly adequate with minor tweaks.⁸² One can foresee explicit clarification that, for instance, a consumer using an AI does not lose their 14-day withdrawal right for distance contracts; the AI cannot waive it. Or that if an AI agrees to an arbitration clause, it's only binding if it meets normal validity requirements in EU law and may be subject to unfair terms scrutiny. The Unfair Contract Terms Directive will surely apply to AI-generated terms the same as any; if a term is unfair, causes a significant imbalance, and is not individually negotiated in B2C, it won't bind the consumer, even if an AI accepted it. Perhaps new guidance will note that the fact that a consumer's own AI

⁸¹ ELI, *Interim Report on EU Consumer Law and ADM*, cit.

⁸² *Ibid.*

negotiated a term doesn't count as individually negotiated if the consumer didn't truly understand or have influence over it. This would maintain consumer protections.

In the U.S., enforceability of terms is broad; the unconscionability doctrine exists but is narrower than EU unfair terms law. So, a potentially interesting divergence: an AI might agree to something a human consumer wouldn't, and in the EU, that term might get struck as unfair, whereas in the U.S., it might stand unless it's extreme enough to be unconscionable or illegal. This means European consumers could end up more shielded from certain exploitative outcomes of AI contracting.

A lawyer counselling a multinational company would note that in Europe, they may need to build in compliance for transparency and accountability and possibly adjust contract terms to comply with any new rules on AI-caused mistakes, whereas in the U.S. they have more freedom but also more uncertainty as to how a court might treat a weird AI scenario. The European regime (once finalised) could offer more predictability; companies know the rules of the road for automated contracts, at least within the EU single market. The U.S. regime is predictable to the extent it's just standard contract law but unpredictable in novel situations lacking precedent. Businesses favour certainty in enforceability, so many might welcome clear rules (hence support for UNCITRAL's model by global companies).

The U.S. flexibility arguably encourages faster adoption of AI, for contracting companies can experiment without needing to fulfil new legal requirements first. This favourable environment for AI-driven ventures is noted in the U.S., which may be seen as a favourable environment for AI-driven corporate ventures due to its legal flexibility. Europe's approach might impose some compliance costs or slow certain fully autonomous implementations (if, say, mandatory disclosures or human oversight are required in some cases). But Europe's aim is to ensure trust and uptake in AI by having safeguards. In the long run, both seek to promote AI in commerce, but Europe is more comfortable doing so with guardrails. The U.S. might adjust if real problems emerge; e.g., if consumers start being harmed by unseen AI negotiation tactics, political pressure could lead to targeted regulation or at least FTC guidelines (the U.S. FTC has hinted at scrutinising AI practices under its broad consumer protection mandate).

In conclusion, European and U.S. approaches are convergent in acknowledging AI contracts as valid and treating AI as a tool of humans but divergent in prescribing specific duties and remedies. Europe's path, through instruments like the ELI/Wendehorst principles and potential EU laws, strives for at least some level of legal certainty, harmonisation, and integrated consumer protection. The U.S. path relies on the adaptability of common law and existing statutes, favouring minimal intervention until absolutely necessary. For global businesses, this means navigating a possibly stricter regime in the EU with obligations to disclose AI use and handle AI mistakes in prescribed ways versus a more *laissez-faire* regime in the U.S., but with the uncertainty that courts might later impose limits unpredictably.

Both approaches have merits: Europe's provides a limited level of clarity and preventative safeguards, whereas the U.S.'s provides flexibility and

immediate practicality. Over time, we may see some convergence. If the EU model proves workable and beneficial, U.S. legal thought might borrow concepts (for example, the future Restatement of Contracts could mention electronic agents). Conversely, if the U.S. experiences problems, it might accelerate regulatory responses, which could end up looking like what the EU is now contemplating.

5. Conclusion: Policy Considerations and Future Directions

The analysis conducted throughout this article demonstrates that the European legal framework for AI-driven contracting remains fragmented, incomplete, and conceptually unbalanced. While international and European initiatives, such as the UNCITRAL Model Law on Automated Contracting, the ELI Guiding Principles, and Professor Wendehorst's Principles, each provide valuable insights, none alone offers a coherent doctrinal basis capable of reconciling technological autonomy with the foundational requirements of contract law. The resulting legal landscape is characterised by partial harmonisation, inconsistent allocation of liability, and insufficient protection of parties interacting with non-human agents. The proposed hybrid regulatory model therefore seeks to move from this fragmentation toward coherence by integrating and systematising the most robust elements of these instruments within a single European framework.

The model rests on three interdependent pillars. The first concerns validity, affirming that contracts generated by AI systems should not be denied legal effect solely due to the absence of direct human agency, provided that they satisfy the principle of functional equivalence and reflect a traceable manifestation of intent attributable to a human actor. The second pillar addresses liability, establishing a differentiated regime that allocates responsibility according to the role and influence of each actor involved in the AI system's design, deployment, and operation. Accountability can no longer remain confined to the contracting parties alone but must extend, under certain conditions, to developers and intermediaries whose technical or commercial choices materially shape contractual outcomes. The third pillar concerns transparency and human oversight, requiring that parties be informed of the use and operational parameters of AI systems in contractual processes and that meaningful human control be preserved at critical decision points to ensure fairness, predictability, and compliance with European values of autonomy and trust.

From a *de iure condendo* perspective, these three pillars translate into concrete legislative recommendations. The European Union should consider supplementing the AI Act with a dedicated legal instrument, potentially a directive or regulation on automated contracting, clarifying the validity, attribution, and liability of AI-mediated transactions. This instrument should harmonise rules governing digital representation and automated contracting across member states, ensuring cross-border consistency. It should also introduce a layered approach to liability, distinguishing betwe-

en deployers, developers, and users according to their capacity to control the system and foresee its consequences. Finally, transparency and human-oversight obligations should be made mandatory for AI systems capable of autonomously concluding or materially influencing contracts. At the same time, scholarly and industry debates reveal diverging perspectives on the desirability and extent of regulatory intervention. While some scholars maintain that existing European contract law principles grounded in autonomy, consent, and risk allocation are sufficiently flexible to accommodate AI contracting, others contend that specific legislative measures are indispensable to ensure legal certainty and uniform application across the Union. The European Commission's ongoing consultations confirm the importance of balancing regulatory clarity with the interests of businesses, particularly small and medium-sized enterprises, which often express concern about excessive regulatory burdens. In this respect, potential policy directions include the adoption of sector-specific guidelines to address contractual practices in distinct markets, the enhancement of liability-attribution frameworks to ensure fairness in AI-mediated relationships, and the establishment of procedural safeguards for AI-induced contractual errors and misunderstandings.

As AI systems continue to reshape contractual processes, the European legal order must evolve not only to address but also to clarify the challenges raised by automated contracting. Whether through the adaptation of existing frameworks or the adoption of new legislative instruments, achieving regulatory clarity is indispensable for fostering trust, accountability, and innovation in AI-driven contractual relations. The European Commission's forthcoming policy choices will thus play a decisive role in shaping the future of AI contracting in Europe, determining whether the transition from fragmentation to coherence will remain a scholarly aspiration or become a tangible legislative achievement.

Abstract

The increasing use of AI in contract formation challenges EU private-law principles like those of consent, attribution, and liability. Existing efforts like UNCITRAL's Model Law, the ELI Guiding Principles, and the EU AI Act, address aspects of algorithmic contracting but remain fragmented. This article argues for a hybrid EU model: *de iure condito*, recognise AI-generated contracts via functional equivalence; *de iure condendo*, adopt a differentiated liability regime allocating responsibility between deployer and developer. It also calls for mandatory transparency and human oversight to secure accountability and trust. Integrating international and European initiatives, the framework enhances legal certainty, supports innovation, and protects contracting parties in the digital market.

Keywords

automated contracting – AI regulation – UNCITRAL – AI Act – algorithmic governance