

ELECTRONIC CONTRACTS IN VIETNAM: LEGAL VALIDITY, DIGITAL EVIDENCE AND ENFORCEMENT CHALLENGES

Tống Thị Thu Trang

Department of Law, TNU - University of Sciences, Thai Nguyen, Vietnam

ABSTRACT

Electronic contracting has become an ordinary part of commerce, but its apparent speed can conceal difficult questions about intention, identity, attribution and proof. This article examines the legal architecture governing electronic contracts in Vietnam, with particular attention to the Law on Electronic Transactions 2023, the Civil Code 2015, the Commercial Law 2005 and rules on electronic authentication and evidence. Using doctrinal and functional analysis, it distinguishes the validity of a transaction from the reliability of the digital record used to prove it. The article argues that technological equivalence between electronic and paper communications does not itself resolve problems of automated contracting, unauthorized account use, unilateral changes to platform terms, evidentiary integrity or unequal bargaining power. It proposes a risk-sensitive framework combining intelligible assent, verifiable attribution, tamper-evident records, accessible remedies and interoperable institutional practice. The contribution lies in connecting contract doctrine to evidence governance rather than treating electronic signature technology as a complete solution to contractual accountability.

Keyword: *Electronic contracts; Electronic transactions; Digital evidence; Electronic signatures; Contract formation; Vietnam; Consumer protection.*

1. INTRODUCTION

A contract is often described as a meeting of minds, yet digital commerce frequently reduces that encounter to a click, an automated response or a sequence of machine-generated records. In practice, the decisive question is not whether computers can transmit an offer and acceptance. It is whether the legal system can determine who acted, what information was displayed, which terms were incorporated, when the parties became bound and whether the surviving record accurately reflects the transaction. These questions become acute when the parties transact at a distance, use shared devices or rely on intermediary platforms.

Vietnam's Law on Electronic Transactions 2023 (Law No. 20/2023/QH15), effective from 1 July 2024, supplies a renewed general framework for transactions conducted by electronic means. Its significance is substantial, but it must be read alongside substantive contract rules. Article 1 identifies the law's concern with conducting transactions electronically rather than comprehensively defining the content or conditions of every underlying transaction. This

division of legislative labor is essential: an electronic record may satisfy a writing requirement without making an unlawful bargain enforceable.

This article addresses three questions. First, how should Vietnamese law distinguish technological recognition from substantive consent? Second, what makes a digital record sufficiently reliable in contractual disputes? Third, how should legal institutions allocate the risks of fraud, system design and evidentiary asymmetry? The analysis is doctrinal rather than empirical. It interprets legal instruments and develops normative recommendations; it does not assert results from interviews, case files or surveys.

2. CONCEPTUAL AND LEGAL FOUNDATIONS

Electronic contracts are agreements formed, communicated or preserved through electronic data. Their defining characteristic is the medium of expression, not a different theory of obligation. Freedom of contract, voluntariness, legal capacity, lawful purpose and enforceability remain questions of substantive law. The Civil Code 2015 provides the general framework, while the Commercial Law 2005 and specialized laws may

govern particular commercial relationships. The Electronic Transactions Law addresses how electronic messages and records can perform legally significant functions.

The principle of functional equivalence prevents the legal system from rejecting a transaction simply because it is expressed digitally. It does not imply factual equivalence: a scanned image, a cryptographically signed document, an email and a platform log have different capacities to demonstrate authorship, alteration and timing. Consequently, the appropriate legal question is whether the digital method reliably performs the relevant legal function, such as identifying the actor, demonstrating intention or preserving the content.

This distinction reflects a long-standing comparative insight. The UNCITRAL Model Law on Electronic Commerce 1996 emphasizes non-discrimination and functional equivalence, while the UNCITRAL Model Law on Electronic Signatures 2001 focuses on dependable methods of indicating approval. The United Nations Convention on the Use of Electronic Communications in International Contracts 2005 further addresses cross-border electronic communications. These instruments offer analytical guidance, although they must not be mistaken for rules automatically binding every Vietnamese domestic contract.

The legal significance of electronic contracts is therefore layered. The first layer is substantive validity: parties, consent, object and mandatory protections. The second is communicative validity: the legal treatment of messages and signatures. The third is evidentiary sufficiency: whether records can prove a disputed event. The fourth is institutional enforceability: whether an aggrieved party can obtain disclosure, verification and a timely remedy. A legal system can be advanced at the second layer yet remain fragile at the third and fourth.

2.1. Offer, acceptance and digital assent

Digital contracting changes the visibility of assent. In a conventional negotiation, an offer and acceptance may be reconstructed from letters, discussions and signatures. On a website, the legally relevant sequence can involve a product listing, a shopping basket, a confirmation click, a payment authorization and a later acceptance message. The existence of multiple automated

steps creates uncertainty about which event completes the agreement. The answer depends on the applicable law, the displayed terms and the objectively communicated intention, not solely on the platform's label for a button.

The design of the interface also matters. A user may click 'continue' without realizing that the action incorporates renewal terms, arbitration arrangements or an additional charge. Where the drafter controls the interface, reliance on formal clicks alone risks substituting technical activity for informed agreement. Courts and regulators should examine the prominence, accessibility and timing of material terms. Terms available only after payment or concealed behind ambiguous links raise a different problem from terms clearly presented before acceptance.

Automated transactions add another complexity. Software may generate communications without a natural person reviewing each output. This does not necessarily defeat contractual formation: parties can deliberately authorize automated systems to transact within predefined parameters. But allocation of responsibility becomes difficult where an automated system makes an obvious error, exceeds preset limits or interacts with another automated service. Sound analysis separates an authorized automated act from unauthorized account access, programming mistakes and deceptive manipulation.

A practical contract-design standard would require a clear final confirmation step, a durable summary of essential terms and an accessible correction opportunity for obvious input errors before the agreement is finalized. In transactions with vulnerable consumers, higher-value commitments or recurring charges, additional confirmation may be proportionate. The objective is not to slow down all electronic commerce but to ensure that friction is introduced where the risk of misunderstood consent is highest.

2.2. Electronic signatures, identity and attribution

An electronic signature can indicate approval and link a person to a document, but the probative strength of a particular method depends on its design and deployment. A typed name at the foot of an email, a one-time password, a device-based signature and a certificate-backed digital signature do not provide identical assurances. Even strong cryptographic authentication does

not prove that the account holder freely agreed; a credential may have been compromised, delegated or used under coercion.

Attribution must therefore be examined through a combination of factors. Relevant indicators may include credential issuance, control of the device, authentication history, transaction context, payment trail, contemporaneous communications and unusual behavior. No single indicator should be mechanically decisive. The stronger the potential consequence for the party whose assent is alleged, the greater the need for a coherent explanation of the signature process and relevant safeguards.

The Law on Electronic Transactions 2023 modernizes the framework for electronic records, signatures and trust services. Its application should be coordinated with rules on cybersecurity, data protection and specialized transaction forms. A general rule recognizing electronic signatures does not eliminate special procedures where another law imposes notarization, registration or an additional mandatory formality. Parties should verify the legal regime for the transaction type instead of assuming that every electronic signature is interchangeable with every required handwritten signature.

Organizations should preserve audit information in a privacy-conscious manner. A well-designed authentication record identifies the method used, the document version, the date and time of completion and the integrity checks available. It should not collect unlimited personal data merely because storage is inexpensive. Verification protocols must be explainable to ordinary users and capable of scrutiny by courts and experts.

2.3. Digital evidence and record integrity

The most important evidentiary distinction is between admissibility and weight. A record may be admissible as evidence yet carry little weight because its origin, completeness or integrity cannot be established. Conversely, the absence of a sophisticated digital signature should not automatically make an otherwise corroborated contractual communication worthless. Evaluating evidence requires an assessment of reliability in the circumstances.

Digital evidence is particularly vulnerable to selective presentation. A screenshot may omit the

screen that displayed pricing conditions; a platform export may conceal database changes; a timestamp may reflect the operator's clock rather than an independent source; and a conversation may have been altered through deletion or extraction. Forensic integrity requires attention to original data, metadata, logs, preservation procedures and whether independent replication or verification is possible.

Evidence governance should begin before litigation. Businesses should maintain version histories for terms and conditions, retain the exact text displayed to users at relevant times, record meaningful consent events and document system changes. Where a platform relies on a log, it should be able to explain how entries are generated, who can modify them and how alterations are detected. Independent audit or cryptographic hashing may assist in high-risk settings, but it is not a universal legal prerequisite.

Procedural equality also matters. The platform usually possesses the complete technical history, while the customer holds only receipts and screenshots. If litigation assumes equal access to evidence, formal rights may be hollow. Courts should be willing, within procedural rules, to order targeted disclosure, protect confidential information and draw appropriate inferences from unexplained nonproduction of material records. Proportionate preservation obligations can discourage strategic deletion without imposing indefinite retention.

2.4. platform intermediation and cross-border risks

The identity of the contracting party can be obscured in online marketplaces. A website may collect payment, advertise goods, determine return procedures and communicate with customers while characterizing itself only as an intermediary. Parties should distinguish the platform operator from the underlying seller and from payment or delivery service providers. Responsibility should track actual functions, representations and the applicable legal classification rather than formal disclaimers alone.

Cross-border contracts introduce questions concerning applicable law, jurisdiction, service of process and enforceability of judgments. Digital accessibility in Vietnam does not by itself answer where a contract is made or which country's consumer standards apply. Contractual choice-of-

law clauses may have significance, but mandatory protective rules require separate analysis. The 2005 UN Electronic Communications Convention provides useful conceptual approaches to communication across borders, without replacing domestic private international law.

Dispute-resolution design should reflect transaction size. Low-value claims are rarely litigated if costs exceed the amount at issue. Accessible online complaint systems, independent review and documented refund procedures can therefore be as significant as formal contractual recognition. Such mechanisms require transparency about who decides disputes, how evidence is assessed and when outcomes can be contested.

2.5. limitations and reform directions

A first reform priority is coherent guidance on digital assent. Regulators and professional bodies should produce practical criteria for the presentation of material terms, informed confirmation and correction of input errors. Guidance should distinguish ordinary business-to-business dealings from consumer contracts and especially consequential financial commitments. Standardization must preserve contractual flexibility while preventing deliberate manipulation of user interfaces.

Second, record integrity should be approached as a governance obligation. Platform operators and high-volume contracting businesses should preserve transaction-specific versions of material terms and maintain auditable consent logs. A risk-based standard is preferable to insisting on the same authentication technology for every transaction. Third, dispute procedures should mitigate informational imbalance by facilitating focused requests for transaction records and expert examination where necessary.

Fourth, contract-law analysis should be coordinated with consumer protection, privacy and cybersecurity. Authentication requirements that expose excessive personal data may create new harms. Effective design should collect only the information necessary to establish attribution and safeguard it through controlled access, limited retention and incident response. Finally, training for judges, lawyers and enterprise compliance teams should focus on how systems actually generate evidence rather than relying on labels

such as 'digital' or 'verified' without technical explanation.

These recommendations follow a common principle: legal recognition of electronic form is the starting point of reliability, not its conclusion. A credible regime should make electronic contracts both easy to conclude and possible to contest where assent or integrity is genuinely disputed.

3. CONCLUSION

Vietnam's modern framework for electronic transactions has strengthened the legal foundation of digitally mediated commerce. Nevertheless, the central legal problems are no longer reducible to whether an electronic message can be a contract or an electronic signature can be recognized. The harder questions concern meaningful assent, trustworthy attribution, evidentiary completeness and effective remedies when the record is controlled by one party.

The proposed framework separates substantive validity, communicative recognition, evidentiary reliability and institutional enforceability. Reform should prioritize intelligible interfaces, secure and proportionate authentication, preservation of terms and transaction logs, balanced access to proof and coordination among contract, consumer and data-protection rules. Treating electronic contracting as a problem of accountable systems rather than mere paper replacement would better protect legitimate commerce and reduce disputes.

4. ACKNOWLEDGEMENTS

The author would like to thank TNU- University of Sciences for supporting us to complete this article.

REFERENCES

- [1] National Assembly of Vietnam. (2015). Civil Code No. 91/2015/QH13.
- [2] National Assembly of Vietnam. (2005). Commercial Law No. 36/2005/QH11.
- [3] National Assembly of Vietnam. (2023). Law on Electronic Transactions No. 20/2023/QH15. <https://vanban.chinhphu.vn/?classid=1&docid=208421&pageid=27160&typegroupid=3>
- [4] National Assembly of Vietnam. (2023). Law on Protection of Consumers' Rights No. 19/2023/QH15.

[5] United Nations Commission on International Trade Law. (1996). UNCITRAL Model Law on Electronic Commerce with Guide to Enactment. United Nations.

[6] United Nations Commission on International Trade Law. (2001). UNCITRAL Model Law on Electronic Signatures with Guide to Enactment. United Nations.

[7] United Nations. (2005). United Nations Convention on the Use of Electronic Communications in International Contracts.

[8] United Nations Commission on International Trade Law. (2017). UNCITRAL Model Law on Electronic Transferable Records. United Nations.

[9] United Nations Commission on International Trade Law. (2018). UNCITRAL Model Law on International Commercial Mediation and International Settlement Agreements Resulting from Mediation. United Nations.

[10] Organisation for Economic Co-operation and Development. (2016). Consumer protection in e-commerce: OECD Recommendation. OECD Publishing.

[11] Organisation for Economic Co-operation and Development. (2022). OECD Recommendation on Digital Security of Critical Activities. OECD.

[12] European Parliament and Council. (2014). Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market.

[13] European Parliament and Council. (2024). Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.

[14] Brownsword, R. (2006). Contract Law: Themes for the Twenty-First Century (2nd ed.). Oxford University Press.

[15] Mik, E. (2014). The effectiveness of electronic contracts in Australia. *Journal of Contract Law*, 30, 103–139.

[16] Reed, C. (2004). *Internet Law: Text and Materials* (2nd ed.). Cambridge University Press