International Insurance Law Review
ISSN: 0968-2090
Vol 34 Issue 1 (2026)
https://lumarpub.com/iilr

The Legal Architecture of Digital Agreements: A Comprehensive Examination of Contracts and Obligations in Electronic Commerce

NOUIRI Samia[1], BOURDIMA Meriem[2]
[1]Associate professor, Class A, University of 8 May 1945- Guelma, Faculty of Law and Political Science, Law Department, Environmental Legal Studies Laboratory (Algeria)
[2]PH.D of Science, specialization Business law
Email: [1]Nouiri.samia@univ-guelma.dz; [2]bourdima.meryem@gmail.com

Abstract:
The digital revolution has fundamentally transformed the landscape of commercial transactions, presenting unprecedented challenges and opportunities for legal systems worldwide. This comprehensive academic intervention provides an in-depth analysis of the legal frameworks governing electronic contracts, with particular emphasis on the formation, validity, enforceability, and performance of digital agreements. Drawing extensively on international instruments including the UNCITRAL Model Law on Electronic Commerce, the E-Sign Act, the Uniform Electronic Transactions Act, and the EU's e-Commerce Directive, this paper examines the rights and obligations of parties in electronic commerce. The intervention also addresses critical issues of consumer protection, comparative legal approaches across jurisdictions, emerging technological challenges including blockchain and artificial intelligence, and identifies significant legal gaps that require urgent legislative attention.
Keywords: Electronic contracts, digital commerce, consumer protection, digital signatures, contract formation, electronic commerce law, functional equivalence, technological neutrality

1. Introduction: The Digital Transformation of Contract Law

The rapid growth of digital technology and electronic commerce has fundamentally changed how business contracts are created and executed. As more transactions move online, traditional contract law faces new challenges including digital signatures, automated agreements, and consumer protection in digital markets. Emerging technologies like blockchain and artificial intelligence add further complexity, creating legal gaps that urgently need new legislation. To address these issues, legal systems are adopting principles of functional equivalence and technological neutrality to ensure that electronic contracts have the same legal validity as paper contracts. This introduction examines how digital transformation is reshaping contract law and the steps being taken to adapt legal frameworks for the modern digital economy.

1.1. The Emergence of Electronic Commerce

The advent of the Internet and digital technologies has fundamentally altered the way in which commercial transactions are conducted.[1]

Electronic commerce, commonly referred to as e-commerce, has evolved from a nascent technology in the 1990s to become a dominant force in the global economy. According to recent estimates, global e-commerce sales exceed three trillion dollars annually, representing a

Citation: NOUIRI Samia & BOURDIMA Meriem. (2026). The Legal Architecture of Digital Agreements: A Comprehensive Examination of Contracts and Obligations in Electronic Commerce. *International Insurance Law Review*, 34 (1), 1-18.

significant portion of total retail transactions. This explosive growth has been driven by numerous factors, including the widespread adoption of the Internet, the proliferation of mobile devices, the development of secure payment systems, and the increasing comfort of consumers with online shopping.

However, this rapid expansion of electronic commerce has outpaced the development of legal frameworks to govern these transactions. Traditional contract law, which has evolved over centuries in the context of face-to-face negotiations and paper-based agreements, has proven inadequate to address the unique challenges posed by digital transactions. Questions about the formation of contracts through automated systems, the validity of electronic signatures, the enforceability of standardized digital agreements, and the protection of consumer rights in the online environment have all emerged as critical legal issues.

1.2. The Importance of Legal Certainty

The development of a clear, predictable, and internationally harmonized legal framework for electronic commerce is essential for several reasons. First, legal certainty is a prerequisite for the continued growth and development of electronic commerce. Businesses and consumers alike need to have confidence that their transactions will be recognized and enforced by the courts. Without such confidence, the trust necessary for the flourishing of digital commerce would be undermined.

Second, the development of a robust legal framework for electronic commerce is necessary to protect the legitimate interests of all parties involved in these transactions. Businesses need assurance that their contracts will be enforceable and that they will not be subject to unexpected legal challenges. Consumers need protection from fraud, deception, and unfair contract terms. Governments need to ensure that electronic commerce does not become a vehicle for illegal activities such as money laundering or the sale of counterfeit goods.

Third, the harmonization of electronic commerce law across jurisdictions is essential for the development of a truly global digital economy. When different countries adopt different legal frameworks for electronic commerce, it creates barriers to cross-border transactions and increases the costs and complexity of doing business internationally. By adopting internationally harmonized standards, countries can facilitate the growth of electronic commerce while maintaining appropriate protections for their citizens.

1.3. Scope and Objectives of This Intervention

This academic intervention provides a comprehensive analysis of the legal frameworks governing electronic contracts and the obligations of parties in electronic commerce. It examines the key principles and rules that have been developed at the international, national, and regional levels to govern electronic transactions. The intervention also explores the critical issue of consumer protection in the digital marketplace, analyzes comparative legal approaches across different jurisdictions, and identifies emerging legal challenges that require urgent attention.

The primary objectives of this intervention are as follows: (1) to provide a comprehensive overview of the legal frameworks governing electronic contracts; (2) to analyze the principles of contract formation, validity, and enforceability in the digital environment; (3) to examine

Citation: NOUIRI Samia & BOURDIMA Meriem. (2026). The Legal Architecture of Digital Agreements: A Comprehensive Examination of Contracts and Obligations in Electronic Commerce. *International Insurance Law Review*, 34 (1), 1-18.

the rights and obligations of sellers and buyers in electronic commerce; (4) to assess the adequacy of current consumer protection mechanisms; (5) to compare legal approaches across different jurisdictions; and (6) to identify emerging legal challenges and propose directions for future legal development.

2. The International Legal Framework for Electronic Commerce

2.1. The UNCITRAL Model Law on Electronic Commerce: A Foundational Text

The United Nations Commission on International Trade Law (UNCITRAL) has played a pivotal role in the development of international standards for electronic commerce. In 1996, UNCITRAL adopted the Model Law on Electronic Commerce (MLEC), which has become one of the most influential legal instruments in the field.[2]

The Model Law was developed in response to the recognition that the rapid growth of electronic commerce was creating legal obstacles that needed to be addressed at the international level.

The MLEC is based on three fundamental principles that have become cornerstones of modern electronic commerce law: non-discrimination, technological neutrality, and functional equivalence. The principle of non-discrimination provides that a document or record shall not be denied legal effect, validity, or enforceability solely on the grounds that it is in electronic form. This principle was revolutionary at the time of the Model Law's adoption, as it directly challenged the long-standing legal requirement that certain types of documents be in paper form.

The principle of technological neutrality mandates that legal rules governing electronic commerce should be neutral with respect to the particular technology used. This principle is crucial because it ensures that legal rules do not become obsolete as technology evolves. By adopting technology-neutral rules, legislators can ensure that their legal frameworks will remain relevant even as new technologies emerge and replace older ones.

The principle of functional equivalence provides that electronic communications and records should be given the same legal effect as their paper-based counterparts when they serve the same function. This principle is particularly important in the context of electronic signatures, where the law must determine when an electronic signature can serve the same function as a handwritten signature. The MLEC establishes specific criteria that electronic communications must meet in order to be considered functionally equivalent to paper-based communications.

2.2. Key Provisions of the UNCITRAL Model Law

The MLEC contains a number of key provisions that have been adopted by numerous countries around the world. These provisions address several critical issues in electronic commerce law, including the legal recognition of data messages, the formation and validity of contracts concluded by electronic means, the attribution of data messages, the acknowledgement of receipt, and the determination of the time and place of dispatch and receipt of data messages.

One of the most important provisions of the MLEC is Article 11, which addresses the formation of contracts by electronic means. This article provides that a contract need not be concluded or evidenced in any particular form, and that the use of electronic means to form a contract does

Citation: NOUIRI Samia & BOURDIMA Meriem. (2026). The Legal Architecture of Digital Agreements: A Comprehensive Examination of Contracts and Obligations in Electronic Commerce. *International Insurance Law Review*, 34 (1), 1-18.

not render the contract invalid or unenforceable. This provision is significant because it removes legal barriers to the formation of contracts through electronic means and establishes the principle that electronic contracts are entitled to the same legal recognition as paper-based contracts.

Another critical provision is Article 13, which addresses the attribution of data messages. This article establishes rules for determining when a data message is to be attributed to a particular person. Under this provision, a data message is attributed to the originator if it was sent by the originator or by a person authorized to act on behalf of the originator. This provision is important because it establishes clear rules for determining the legal responsibility for electronic communications.

2.3. The UNCITRAL Model Law on Electronic Signatures

In 2001, UNCITRAL adopted the Model Law on Electronic Signatures (MLES) to complement the MLEC.[3]

The MLES provides additional rules specifically addressing the use of electronic signatures in electronic commerce. The Model Law establishes a framework for the legal recognition of electronic signatures and provides guidance on the requirements that electronic signatures must meet in order to be legally valid.

The MLES distinguishes between different types of electronic signatures, including advanced electronic signatures and qualified electronic signatures. An advanced electronic signature is defined as an electronic signature that meets certain technical requirements, including being uniquely linked to the signatory, being capable of identifying the signatory, being created using means that the signatory can maintain under their sole control, and being linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

2.4. The UN Convention on Electronic Communications in International Contracts

In 2005, the United Nations adopted the Convention on the Use of Electronic Communications in International Contracts. This convention extends the principles established in the MLEC and MLES to the specific context of international contracts. The convention provides that electronic communications may be used in the formation and performance of international contracts, and that such communications shall be given legal recognition and effect.

3. The Formation of Electronic Contracts: Principles and Challenges

Electronic contracts must follow the same basic rules as traditional contracts—there must be an offer, acceptance, consideration, and agreement between parties—but applying these principles to online transactions creates new challenges because digital communications happen instantly, parties are often unknown to each other, and it is difficult to determine exactly when and where a contract is formed.

3.1. Traditional Contract Formation Principles and Their Application to Electronic Transactions

The formation of a contract has traditionally required the existence of several essential elements: an offer, an acceptance, consideration (or in civil law jurisdictions, cause or reason for the obligation), and the mutual intent of the parties to be bound.[4]

Citation: NOUIRI Samia & BOURDIMA Meriem. (2026). The Legal Architecture of Digital Agreements: A Comprehensive Examination of Contracts and Obligations in Electronic Commerce. *International Insurance Law Review*, 34 (1), 1-18.

These principles, which have been refined through centuries of common law development and civil law codification, continue to apply to electronic contracts. However, the application of these traditional principles to the unique context of electronic transactions has raised a number of novel legal questions.

An offer is a manifestation of willingness to enter into a bargain, made so as to justify another person in understanding that his assent to that bargain is invited and will conclude it. In the context of electronic commerce, the question of whether a merchant's display of goods on a website constitutes an offer or merely an invitation to make an offer has been a subject of considerable debate. Most courts have held that the display of goods on a website is merely an invitation to make an offer, and that the offer is made by the customer when they place an item in their shopping cart or click the "purchase" button. The merchant then has the right to accept or reject this offer.

Acceptance is the manifestation of assent to the terms of an offer made by the offeree in a manner invited or required by the offer. In the context of electronic commerce, acceptance typically occurs when the customer clicks a button indicating their agreement to purchase the goods or services. However, the question of whether the customer has actually read and understood the terms of the contract has been a subject of considerable controversy.

3.2. The Challenge of Standardized Digital Agreements

One of the most significant developments in the formation of electronic contracts has been the emergence of standardized digital agreements, which are often presented to consumers on a take-it-or-leave-it basis.[5]

These agreements, which include click-wrap agreements, browse-wrap agreements, and shrink-wrap agreements, have raised important questions about the nature of consent and the enforceability of their terms.

Click-wrap agreements are agreements where the user must affirmatively click a button or checkbox to indicate their assent to the terms of the agreement. These agreements typically appear on a website and require the user to scroll through the terms and then click a button indicating that they agree to the terms before they can proceed with their transaction. Courts have generally held that click-wrap agreements are enforceable, provided that the terms are reasonably communicated to the user and the user is given a clear opportunity to assent to those terms.

Browse-wrap agreements are agreements where the terms are merely posted on a website and the user is deemed to have accepted them by simply using the site. These agreements typically include a notice that states something like "By using this website, you agree to be bound by the terms of service" or similar language. Browse-wrap agreements have been met with greater skepticism by the courts, and many courts have held that such agreements are not enforceable because the user may not have had actual notice of the terms.

Shrink-wrap agreements are agreements that are enclosed within the packaging of a product and become binding when the user opens the package or uses the product. These agreements have been recognized as enforceable by courts in some jurisdictions, particularly where the

Citation: NOUIRI Samia & BOURDIMA Meriem. (2026). The Legal Architecture of Digital Agreements: A Comprehensive Examination of Contracts and Obligations in Electronic Commerce. *International Insurance Law Review*, 34 (1), 1-18.

user has had an opportunity to review the terms before opening the package and has the right to return the product if they do not agree to the terms.

3.3. The Principle of Functional Equivalence in Contract Formation

The principle of functional equivalence plays a crucial role in the formation of electronic contracts. This principle holds that electronic records and signatures should be given the same legal effect as their paper-based counterparts when they serve the same function. In the context of contract formation, this principle means that electronic communications that serve the same function as traditional written offers and acceptances should be given the same legal effect.

The application of the principle of functional equivalence to electronic contracts has required courts and legislators to carefully consider what functions are served by traditional paper-based contracts and how electronic communications can serve those same functions. For example, one function served by a written contract is to provide evidence of the agreement between the parties. Electronic records can serve this function by creating a permanent record of the transaction that can be stored and retrieved. Another function served by a written contract is to ensure that both parties have the same understanding of the terms of the agreement. Electronic contracts can serve this function by presenting the terms in a clear and accessible manner.

4. The Validity and Enforceability of Electronic Contracts

For electronic contracts to be useful in commerce, they must be recognized as valid and legally binding, and parties must be able to enforce them in court if disputes arise, which requires legal systems to confirm that digital agreements have the same legal status as paper contracts and that electronic signatures and digital evidence are acceptable proof of agreement.

4.1. Legal Recognition of Electronic Contracts

The legal validity and enforceability of electronic contracts is a fundamental issue in electronic commerce law. In order for electronic commerce to flourish, businesses and consumers need to have confidence that contracts formed through electronic means will be recognized and enforced by the courts. To address this concern, many jurisdictions have adopted legislation explicitly recognizing the legal validity of electronic contracts.

In the United States, the Electronic Signatures in Global and National Commerce Act (E-Sign Act), adopted in 2000, provides that a contract or signature may not be denied legal effect or enforceability solely because it is in electronic form.[6]

The E-Sign Act applies to transactions affecting interstate or foreign commerce and provides a uniform federal standard for the legal recognition of electronic records and signatures. The Act defines an electronic record as "a contract or other record created, generated, sent, communicated, received, or stored by electronic means" and an electronic signature as "an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record."

Similarly, the Uniform Electronic Transactions Act (UETA), which has been adopted by all fifty states and the District of Columbia, provides that a record or signature may not be denied legal effect or enforceability solely because it is in electronic form. The UETA defines an electronic record as "a record created, generated, sent, communicated, received, or stored by

Citation: NOUIRI Samia & BOURDIMA Meriem. (2026). The Legal Architecture of Digital Agreements: A Comprehensive Examination of Contracts and Obligations in Electronic Commerce. *International Insurance Law Review*, 34 (1), 1-18.

electronic means" and an electronic signature as "an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record."

4.2. The Role of Digital Signatures in Contract Enforceability

Digital signatures play a crucial role in ensuring the validity and enforceability of electronic contracts.[7]

A digital signature is an electronic means of authentication that uses cryptographic technology to verify the identity of the signer and to ensure the integrity of the signed document. Unlike a handwritten signature, which is a visual representation of a person's name, a digital signature is a mathematical algorithm that is unique to each individual and cannot be forged or altered without detection.

The law recognizes different types of electronic signatures, with varying levels of security and legal weight. A simple electronic signature might be as basic as typing one's name in an email or clicking an "I agree" button on a website. An advanced electronic signature is an electronic signature that meets certain technical requirements, including being uniquely linked to the signatory, being capable of identifying the signatory, being created using means that the signatory can maintain under their sole control, and being linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

A qualified electronic signature is an advanced electronic signature that is created by a qualified electronic signature creation device and is based on a qualified certificate for electronic signatures. In the European Union, a qualified electronic signature is given the same legal effect as a handwritten signature. This means that a qualified electronic signature provides strong evidence of the identity of the signer and the integrity of the signed document.

4.3. The Challenge of Proving Consent and Authentication

One of the most significant challenges in the context of electronic contracts is proving that the parties have knowingly and voluntarily consented to the terms of the agreement. This is particularly true in the case of standardized contracts, where consumers may not have the time or inclination to read lengthy and complex legal terms. To address this issue, the law requires that the terms of an electronic contract be reasonably communicated to the user, and that the user be given a clear opportunity to assent to those terms.

The concept of "reasonable communication" has been interpreted by courts to mean that the terms must be presented in a manner that is likely to come to the attention of the user. This typically requires that the terms be clearly visible on the screen, that the user be required to scroll through the terms in order to proceed, and that the user be required to affirmatively indicate their assent to the terms by clicking a button or checkbox.

The authentication of electronic signatures is another critical issue in ensuring the validity and enforceability of electronic contracts. Authentication refers to the process of verifying the identity of the signer and ensuring that the signature has not been forged or altered. Various technological solutions have been developed to address this issue, including public key infrastructure (PKI), which uses a system of digital certificates to verify the identity of signers.

Citation: NOUIRI Samia & BOURDIMA Meriem. (2026). The Legal Architecture of Digital Agreements: A Comprehensive Examination of Contracts and Obligations in Electronic Commerce. *International Insurance Law Review*, 34 (1), 1-18.

5. The Obligations of Parties in Electronic Commerce: A Detailed Analysis

5.1. The Seller's Obligations in Electronic Transactions

The seller in an electronic transaction bears a number of important obligations, which are designed to ensure that the transaction is conducted fairly and transparently, and that the buyer receives the goods or services that were promised.[8]

These obligations can be divided into several categories: pre-contractual obligations, obligations regarding the provision of information, obligations regarding the performance of the contract, and post-contractual obligations.

5.1.1. Pre-Contractual Obligations

Before entering into a contract with a consumer, the seller has an obligation to provide the consumer with certain information about the goods or services being offered. This information typically includes the identity of the seller, the main characteristics of the goods or services, the total price including all taxes and fees, information about payment and delivery methods, and information about any applicable consumer protection laws or guarantees.

The purpose of these pre-contractual obligations is to ensure that the consumer has sufficient information to make an informed decision about whether to purchase the goods or services. This is particularly important in the context of electronic commerce, where the consumer cannot physically inspect the goods before purchase and must rely on the information provided by the seller.

5.1.2. Information Provision Obligations

The seller has an ongoing obligation to provide the buyer with clear and accurate information about the goods or services being offered. This obligation extends beyond the initial sale and includes providing information about any changes to the goods or services, any recalls or safety issues, and any other information that might affect the buyer's satisfaction with the purchase.

In the European Union, the e-Commerce Directive requires that online service providers provide consumers with certain mandatory information, including the identity of the service provider, the address where the service provider is established, the email address and telephone number of the service provider, information about the professional registers in which the service provider is listed, and information about any professional qualifications or memberships.[9]

5.1.3. Performance Obligations

The seller has an obligation to perform the contract in accordance with its terms. This typically involves delivering the goods or providing the services within the agreed timeframe and in the condition promised. The seller must also ensure that the goods or services conform to the description provided and meet any applicable quality standards.

In the event that the goods or services do not conform to the contract, the buyer typically has the right to reject the goods or services, to require the seller to repair or replace them, or to seek damages from the seller. The specific remedies available to the buyer will depend on the applicable law and the terms of the contract.

Citation: NOUIRI Samia & BOURDIMA Meriem. (2026). The Legal Architecture of Digital Agreements: A Comprehensive Examination of Contracts and Obligations in Electronic Commerce. *International Insurance Law Review*, 34 (1), 1-18.

5.1.4. Post-Contractual Obligations

After the sale has been completed, the seller may have certain post-contractual obligations, such as providing warranty coverage, handling returns and exchanges, and addressing customer complaints. These obligations are designed to ensure that the buyer is satisfied with the purchase and that any problems that arise after the sale are resolved in a fair and timely manner.

5.2. The Buyer's Obligations in Electronic Transactions

The buyer in an electronic transaction also has a number of important obligations, which are designed to ensure that the transaction is conducted fairly and that the seller receives payment for the goods or services provided.[10]

These obligations include the duty to read and understand the terms of the contract, the duty to provide accurate information to the seller, and the duty to pay for the goods or services in a timely manner.

5.2.1. The Duty to Read and Understand Contract Terms

While the law recognizes that consumers may not always read the fine print of lengthy and complex legal agreements, it also expects them to take reasonable steps to inform themselves about the terms of the agreement. This is particularly true when the terms are clearly presented and the consumer is given a clear opportunity to review them before agreeing to the contract.

However, there is considerable debate about the extent to which consumers can be held responsible for failing to read contract terms. Some legal scholars argue that the principle of "caveat emptor" (let the buyer beware) has been superseded by modern consumer protection law, which places greater responsibility on sellers to ensure that consumers understand the terms of the contract. Others argue that consumers have a responsibility to protect their own interests by carefully reading contract terms before agreeing to them.

5.2.2. The Duty to Provide Accurate Information

The buyer has an obligation to provide the seller with accurate information necessary to complete the transaction. This typically includes the buyer's name, address, email address, and payment information. The buyer also has an obligation to provide accurate information about the goods or services being purchased, such as the quantity and specifications of the items.

Providing false or misleading information to the seller can constitute fraud and may result in the buyer being held liable for damages. In some cases, providing false information may also constitute a criminal offense.

5.2.3. The Duty to Pay

The buyer has an obligation to pay for the goods or services in accordance with the terms of the contract. This typically involves paying the agreed price within the agreed timeframe using the agreed payment method. Failure to pay constitutes a breach of contract and may result in the seller pursuing legal action to recover the unpaid amount.

Citation: NOUIRI Samia & BOURDIMA Meriem. (2026). The Legal Architecture of Digital Agreements: A Comprehensive Examination of Contracts and Obligations in Electronic Commerce. *International Insurance Law Review*, 34 (1), 1-18.

6. Performance, Breach, and Remedies in Electronic Commerce

6.1. Performance of Electronic Contracts

The performance of an electronic contract involves the fulfillment of the parties' respective obligations under the contract. The specific nature of performance will depend on the type of transaction involved. In the case of the sale of goods, performance typically involves the delivery of the goods to the buyer. In the case of the provision of services, performance typically involves the provision of the services in accordance with the agreed terms.

6.1.1. Delivery of Goods in Electronic Commerce

The delivery of goods in electronic commerce presents unique challenges compared to traditional retail transactions. In many cases, the buyer and seller are located in different geographical locations and may never meet in person. The goods must be shipped from the seller's location to the buyer's location, which may take several days or weeks.

The seller has an obligation to ensure that the goods are delivered in a timely manner and in the condition promised. This typically involves packaging the goods securely to prevent damage during shipping, selecting an appropriate shipping method, and providing the buyer with tracking information so that they can monitor the delivery of the goods.

6.1.2. Delivery of Digital Goods and Services

The delivery of digital goods and services, such as software, music, or cloud computing services, presents different challenges than the delivery of physical goods. In many cases, digital goods and services are delivered instantaneously over the Internet, and there is no physical shipping involved.

The seller has an obligation to ensure that the digital goods or services are delivered in a timely manner and in the condition promised. This may involve ensuring that the software is free from defects, that the music files are in the correct format, or that the cloud computing services are available and functioning properly.

6.2. Breach of Electronic Contracts

A breach of an electronic contract occurs when one party fails to perform its obligations under the contract without a valid legal excuse.[11]

The failure to perform may be total or partial, and may be material or immaterial. A material breach is one that goes to the heart of the contract and substantially deprives the non-breaching party of the benefit of the bargain. An immaterial breach is one that does not substantially affect the value of the contract to the non-breaching party.

6.2.1. Types of Breach

There are several types of breach that may occur in electronic commerce transactions. A seller may be in breach of contract if it fails to deliver the goods or services in a timely manner, if the goods or services are not of the quality that was promised, if the goods or services do not conform to the description provided, or if the seller fails to provide the information or services that were promised.

Citation: NOUIRI Samia & BOURDIMA Meriem. (2026). The Legal Architecture of Digital Agreements: A Comprehensive Examination of Contracts and Obligations in Electronic Commerce. *International Insurance Law Review*, 34 (1), 1-18.

A buyer may be in breach of contract if it fails to pay for the goods or services, if it uses the goods or services in a manner that is not permitted by the contract, or if it fails to provide the information necessary to complete the transaction.

6.2.2. Remedies for Breach

In the event of a breach of contract, the non-breaching party may be entitled to a number of remedies, including damages, specific performance, termination of the contract, and in some cases, restitution.

Damages are a monetary award that is designed to compensate the non-breaching party for the losses that it has suffered as a result of the breach. Damages may include direct damages (the difference between the value of the goods or services as promised and the value of the goods or services actually received) and consequential damages (losses that result from the breach but are not directly caused by it).

Specific performance is a court order that requires the breaching party to perform its obligations under the contract. This remedy is typically available only when damages would be an inadequate remedy, such as in the case of the sale of unique goods or the provision of unique services.

Termination of the contract allows the non-breaching party to be released from its own obligations under the contract. This remedy is typically available only when the breach is material and substantially deprives the non-breaching party of the benefit of the bargain.

Restitution is a remedy that requires the breaching party to return any benefits that it has received from the non-breaching party. This remedy is typically used when the contract has been terminated and the parties need to be restored to their original positions.

7. Consumer Protection in Electronic Commerce: A Critical Analysis

7.1. The Vulnerability of Online Consumers

Online consumers face a number of unique vulnerabilities that are not present in traditional retail transactions.[12]

First, online consumers are often at an information disadvantage compared to online merchants. The merchant has detailed information about the goods or services being offered, while the consumer may have only limited information based on product descriptions and photographs.

Second, online consumers are often presented with complex and lengthy terms and conditions that they may not fully understand. Many consumers do not read these terms carefully, and even those who do may not fully comprehend their legal implications.

Third, online consumers are vulnerable to fraud and deception. Unscrupulous merchants may misrepresent the quality or characteristics of goods or services, may fail to deliver goods or services that have been paid for, or may use the consumer's personal and financial information for fraudulent purposes.

Fourth, online consumers may lack effective remedies when problems arise. If a consumer purchases goods from a merchant located in a different country, it may be difficult or impossible for the consumer to pursue legal action against the merchant.

Citation: NOUIRI Samia & BOURDIMA Meriem. (2026). The Legal Architecture of Digital Agreements: A Comprehensive Examination of Contracts and Obligations in Electronic Commerce. *International Insurance Law Review*, 34 (1), 1-18.

7.2. Legal Protections for Online Consumers

Recognizing the vulnerabilities of online consumers, many jurisdictions have adopted legislation specifically designed to protect consumer rights in electronic commerce.[13]

These protections typically address issues such as the provision of information, the right to withdraw from a contract, the prohibition of unfair contract terms, and dispute resolution mechanisms.

7.2.1. The EU's Consumer Rights Framework

The European Union has developed one of the most comprehensive frameworks for consumer protection in electronic commerce.[14]

The Consumer Rights Directive, which was adopted in 2011, provides a high level of protection for online consumers. The Directive gives consumers a right of withdrawal, which allows them to cancel an online contract within 14 days without giving any reason. This right is particularly important in the context of electronic commerce, where consumers cannot physically inspect goods before purchase.

The Directive also requires that sellers provide consumers with clear and comprehensive information about the goods or services being offered, including the main characteristics of the goods or services, the price, the payment method, the delivery method, and information about any applicable guarantees or warranties.

The Directive also prohibits the use of unfair contract terms. An unfair contract term is one that creates a significant imbalance in the parties' rights and obligations under the contract, to the detriment of the consumer. Examples of unfair contract terms include terms that allow the seller to unilaterally modify the price or terms of the contract, terms that allow the seller to avoid liability for defects in the goods or services, and terms that require the consumer to waive important consumer rights.

7.2.2. Consumer Protection in the United States

In the United States, consumer protection in electronic commerce is governed by a combination of federal and state laws.[15]

The Federal Trade Commission (FTC) is the primary federal agency responsible for protecting consumers from unfair and deceptive practices in the marketplace. The FTC has authority under the Federal Trade Commission Act to bring enforcement actions against companies that engage in deceptive or unfair practices in connection with electronic commerce.

The FTC has brought numerous enforcement actions against companies that have engaged in deceptive practices in electronic commerce, such as misrepresenting the characteristics or quality of goods or services, failing to disclose material information, or using misleading advertising. The FTC has also brought enforcement actions against companies that have failed to protect consumer privacy or that have engaged in identity theft.

In addition to federal protections, many states have adopted their own consumer protection laws that apply to electronic commerce. These state laws often provide protections that are similar to those provided by the EU's Consumer Rights Directive, such as the right to withdraw from a contract or the prohibition of unfair contract terms.

Citation: NOUIRI Samia & BOURDIMA Meriem. (2026). The Legal Architecture of Digital Agreements: A Comprehensive Examination of Contracts and Obligations in Electronic Commerce. *International Insurance Law Review*, 34 (1), 1-18.

7.3. The Role of Alternative Dispute Resolution

Given the challenges of pursuing litigation in electronic commerce disputes, many jurisdictions have developed alternative dispute resolution (ADR) mechanisms to help consumers resolve disputes with merchants. These mechanisms include mediation, arbitration, and online dispute resolution (ODR) platforms.

Mediation is a process in which a neutral third party helps the parties to a dispute reach a mutually acceptable resolution. Mediation is typically less formal and less expensive than litigation, and it allows the parties to maintain control over the outcome of the dispute.

Arbitration is a process in which a neutral third party (called an arbitrator) hears evidence from both parties and makes a binding decision about how to resolve the dispute. Arbitration is typically faster and less expensive than litigation, but it may provide fewer procedural protections than litigation.

Online dispute resolution (ODR) platforms use technology to facilitate the resolution of disputes between consumers and merchants. These platforms may use automated systems to help the parties reach a settlement, or they may use human mediators or arbitrators to help resolve the dispute. ODR platforms have the advantage of being accessible to consumers regardless of their geographical location and can often resolve disputes quickly and inexpensively.

8. Comparative Legal Approaches to Electronic Contracts

8.1. Common Law Jurisdictions

In common law jurisdictions, such as the United States, the United Kingdom, Canada, and Australia, electronic contracts are governed by a combination of traditional contract law principles and legislation specifically addressing electronic commerce.[16]

These jurisdictions have generally adopted the approach of applying traditional contract formation principles to electronic transactions, while recognizing that electronic communications may take different forms than traditional paper-based communications.

The E-Sign Act in the United States and the UETA provide a federal and state-level framework for the legal recognition of electronic records and signatures. These statutes establish the principle that electronic records and signatures may not be denied legal effect or enforceability solely because they are in electronic form. However, these statutes also recognize that certain types of contracts may be excluded from their scope, such as contracts relating to wills, trusts, and powers of attorney.

8.2. Civil Law Jurisdictions

In civil law jurisdictions, such as France, Germany, Spain, and many Latin American countries, electronic contracts are governed by civil codes that have been amended to recognize the legal validity of electronic records and signatures.[17]

These jurisdictions have generally adopted the approach of integrating electronic commerce provisions into their existing civil codes, rather than creating separate legislation specifically addressing electronic commerce.

Citation: NOUIRI Samia & BOURDIMA Meriem. (2026). The Legal Architecture of Digital Agreements: A Comprehensive Examination of Contracts and Obligations in Electronic Commerce. *International Insurance Law Review*, 34 (1), 1-18.

Many civil law jurisdictions have adopted the UNCITRAL Model Law on Electronic Commerce as the basis for their electronic commerce legislation. This has helped to promote harmonization of electronic commerce law across different civil law jurisdictions.

8.3. Hybrid Jurisdictions

Some jurisdictions, such as those in the Middle East and North Africa, have legal systems that combine elements of both common law and civil law traditions. These jurisdictions have adopted various approaches to regulating electronic commerce, ranging from the adoption of the UNCITRAL Model Law to the development of indigenous electronic commerce legislation.

9. Emerging Legal Challenges and Future Directions

9.1. Blockchain Technology and Smart Contracts

One of the most significant emerging challenges in electronic commerce law is the development of blockchain technology and smart contracts.[18]

A smart contract is a computer program that automatically executes the terms of a contract when certain conditions are met. Smart contracts are typically stored on a blockchain, which is a distributed ledger that records all transactions in a tamper-proof manner.

Smart contracts present a number of novel legal challenges. First, there is the question of whether a smart contract can constitute a valid and enforceable contract under existing contract law. Most legal scholars agree that a smart contract can constitute a valid contract if it meets the essential requirements of contract formation, including offer, acceptance, consideration, and mutual intent to be bound. However, there are questions about how these requirements apply in the context of smart contracts, particularly in cases where the contract is executed automatically without human intervention.

Second, there is the question of how to allocate responsibility when a smart contract fails to perform as intended. If a smart contract contains a bug or is hacked, who bears the responsibility for the resulting losses? The answer to this question will depend on the applicable law and the terms of the contract.

Third, there is the question of how to ensure that smart contracts comply with applicable consumer protection laws. Many consumer protection laws require that certain information be provided to consumers before they enter into a contract, and that consumers be given an opportunity to review the terms of the contract before agreeing to it. It may be difficult to satisfy these requirements in the context of smart contracts, particularly when the contract is executed automatically.

9.2. Artificial Intelligence and Automated Decision-Making

Another significant emerging challenge is the use of artificial intelligence (AI) and automated decision-making in electronic commerce.[19]

Many online merchants now use AI systems to make decisions about pricing, inventory management, and customer service. Some merchants also use AI systems to make decisions about whether to accept or reject customer orders or to determine the creditworthiness of customers.

Citation: NOUIRI Samia & BOURDIMA Meriem. (2026). The Legal Architecture of Digital Agreements: A Comprehensive Examination of Contracts and Obligations in Electronic Commerce. *International Insurance Law Review*, 34 (1), 1-18.

The use of AI in electronic commerce raises a number of legal challenges. First, there is the question of whether a contract can be formed through an AI system. If an AI system makes an offer or acceptance on behalf of a merchant, is the merchant bound by that offer or acceptance? Most legal scholars agree that the answer is yes, provided that the AI system was authorized to act on behalf of the merchant.

Second, there is the question of how to ensure that AI systems comply with applicable consumer protection laws. Many consumer protection laws prohibit discrimination based on protected characteristics such as race, gender, or age. However, AI systems may make decisions based on factors that are correlated with protected characteristics, even if the protected characteristics themselves are not explicitly used in the decision-making process. This raises the question of whether the use of such AI systems violates consumer protection laws.

Third, there is the question of how to ensure transparency and accountability in AI decision-making. Many consumers do not understand how AI systems make decisions, and they may not be aware that their transactions are being governed by AI systems. This raises questions about whether consumers are giving informed consent to contracts that are governed by AI systems.

9.3. Data Privacy and Security in Electronic Commerce

Data privacy and security have become increasingly important issues in electronic commerce.[20] When consumers purchase goods or services online, they typically provide the merchant with personal information, such as their name, address, email address, and payment information. This information is valuable to merchants, but it is also vulnerable to theft and misuse.

Many jurisdictions have adopted legislation specifically addressing data privacy and security in electronic commerce. The most comprehensive of these is the European Union's General Data Protection Regulation (GDPR), which provides a comprehensive framework for the protection of personal data. The GDPR requires that merchants obtain informed consent from consumers before collecting their personal data, that merchants use the personal data only for the purposes for which it was collected, and that merchants implement appropriate security measures to protect the personal data from theft and misuse.

9.4. Cross-Border Electronic Commerce and Jurisdictional Issues

As electronic commerce becomes increasingly global, questions about jurisdiction and the applicable law have become more pressing. When a consumer in one country purchases goods or services from a merchant in another country, which country's laws apply? Which country's courts have jurisdiction to hear disputes between the consumer and the merchant?

These questions are particularly important in the context of consumer protection. If a merchant in one country sells goods to a consumer in another country, should the consumer be able to rely on the consumer protection laws of their own country, or should they be subject to the consumer protection laws of the merchant's country?

The European Union has addressed these issues through the Brussels Regulation, which provides rules for determining which courts have jurisdiction in cross-border disputes. The regulation generally provides that a consumer can bring a claim against a merchant in the

Citation: NOUIRI Samia & BOURDIMA Meriem. (2026). The Legal Architecture of Digital Agreements: A Comprehensive Examination of Contracts and Obligations in Electronic Commerce. *International Insurance Law Review*, 34 (1), 1-18.

consumer's own country, even if the merchant is located in another country. This approach is designed to protect consumers by allowing them to pursue claims in their own country without having to travel to the merchant's country.

10. Legal Gaps and Recommendations for Reform

10.1. Inadequate Protection for Vulnerable Consumers

Despite the development of comprehensive consumer protection frameworks in many jurisdictions, there remain significant gaps in the protection afforded to vulnerable consumers. Elderly consumers, consumers with limited education, and consumers with limited access to technology may be particularly vulnerable to fraud and deception in electronic commerce.

There is a need for targeted consumer protection measures that specifically address the needs of vulnerable consumers. These measures might include simplified contract terms, enhanced disclosure requirements, and specialized dispute resolution mechanisms for vulnerable consumers.

10.2. Lack of Harmonization in International Electronic Commerce

While the UNCITRAL Model Law on Electronic Commerce has been adopted by many countries, there remain significant differences in how different jurisdictions regulate electronic commerce. These differences create barriers to cross-border electronic commerce and increase the costs and complexity of doing business internationally.

There is a need for greater harmonization of electronic commerce law across jurisdictions. This might be achieved through the adoption of international conventions or model laws that establish common standards for electronic commerce.

10.3. Inadequate Legal Framework for Emerging Technologies

As discussed above, emerging technologies such as blockchain, smart contracts, and artificial intelligence are creating new legal challenges that are not adequately addressed by existing legal frameworks. There is a need for new legislation and legal doctrines that specifically address these emerging technologies.

10.4. Inadequate Enforcement Mechanisms

Even where comprehensive consumer protection laws exist, enforcement of these laws is often inadequate. Many consumers do not know their rights, and many merchants are not aware of their obligations. There is a need for improved enforcement mechanisms, including consumer education programs, merchant compliance programs, and effective dispute resolution mechanisms.

11. Conclusion: Toward a More Equitable Digital Marketplace

The development of a legal framework for electronic contracts and electronic commerce has been one of the most significant challenges facing legal systems in the digital age. While substantial progress has been made in establishing a framework that recognizes the legal validity of electronic contracts and provides protections for consumers, significant challenges remain.

Citation: NOUIRI Samia & BOURDIMA Meriem. (2026). The Legal Architecture of Digital Agreements: A Comprehensive Examination of Contracts and Obligations in Electronic Commerce. *International Insurance Law Review*, 34 (1), 1-18.

The principles of non-discrimination, technological neutrality, and functional equivalence that are enshrined in the UNCITRAL Model Law on Electronic Commerce have provided a solid foundation for the development of electronic commerce law. These principles have been adopted by many jurisdictions and have helped to promote the growth of electronic commerce while maintaining appropriate protections for consumers.

However, as electronic commerce continues to evolve and new technologies emerge, the legal framework must continue to adapt. The development of blockchain technology, artificial intelligence, and other emerging technologies will require new legal doctrines and principles to ensure that the digital marketplace remains fair and efficient.

Furthermore, there is a need for greater attention to the protection of vulnerable consumers and for improved enforcement of consumer protection laws. The digital marketplace should not be a place where the strong exploit the weak, but rather a place where all participants can engage in fair and honest commerce.

In conclusion, the legal architecture of digital agreements is a complex and multifaceted area of the law that continues to evolve. By understanding the key principles that govern the formation, validity, and enforceability of electronic contracts, and by remaining vigilant in identifying and addressing emerging legal challenges, we can work toward creating a digital marketplace that is fair, efficient, and protective of the legitimate interests of all participants.

References

1. UNCITRAL Model Law on Electronic Commerce (1996) with additional article 5 bis as adopted in 1998. United Nations Commission On International Trade Law. Available at: https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce
2. UNCITRAL Model Law on Electronic Commerce (1996), Articles 1-16, establishing the foundational principles of non-discrimination, technological neutrality, and functional equivalence for electronic transactions.
3. UNCITRAL Model Law on Electronic Signatures (2001). United Nations Commission On International Trade Law. Available at: https://uncitral.un.org/en/texts/esignatures/modellaw
4. Restatement (Second) of Contracts § 24-71 (1981), establishing the fundamental principles of contract formation including offer, acceptance, consideration, and mutual intent.
5. Hillman, R. A., & Rachlinski, J. J. (2002). "Standard-Form Contracting in the Electronic Age." Cornell Law Review, 87, 269-315. Discussing the enforceability of click-wrap, browse-wrap, and shrink-wrap agreements in electronic commerce.
6. Electronic Signatures in Global and National Commerce Act (E-Sign Act), 15 U.S.C. § 7001-7006 (2000), establishing federal recognition of electronic records and signatures in interstate and foreign commerce.
7. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, establishing the legal framework for digital signatures in the European Union.

Citation: NOUIRI Samia & BOURDIMA Meriem. (2026). The Legal Architecture of Digital Agreements: A Comprehensive Examination of Contracts and Obligations in Electronic Commerce. *International Insurance Law Review*, 34 (1), 1-18.

8. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), Articles 5-9, establishing seller obligations and information requirements.
9. Directive 2000/31/EC, Article 5, requiring online service providers to disclose specific information to consumers including identity, address, contact details, and professional qualifications.
10. Uniform Commercial Code § 2-201 et seq., establishing the duties and obligations of buyers and sellers in commercial transactions, including electronic transactions.
11. Restatement (Second) of Contracts § 235-237 (1981), defining breach of contract and distinguishing between material and immaterial breaches.
12. UNCTAD (2019). "Digital Economy Report 2019: Value Creation and Capture: Implications for Developing Countries." United Nations Conference on Trade and Development, addressing vulnerabilities of online consumers in developing markets.
13. Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC and repealing Council Directive 85/577/EEC and Directive 97/7/EC.
14. Directive 2011/83/EU, Articles 5-8, establishing the right of withdrawal, information requirements, and prohibition of unfair contract terms in consumer contracts.
15. Federal Trade Commission Act, 15 U.S.C. § 45 (1914), and various state consumer protection statutes providing legal protections for consumers in electronic commerce.
16. Uniform Electronic Transactions Act (UETA), National Conference of Commissioners on Uniform State Laws, establishing uniform rules for electronic transactions across U.S. states.
17. French Civil Code Articles 1369-1369-14 and German BGB §§ 312-312k, incorporating electronic commerce provisions into civil law frameworks.
18. De Filippi, P., & Wright, A. (2015). "Blockchain and the Law: The Rule of Code." Harvard University Press, discussing legal implications of blockchain technology and smart contracts.
19. Yeung, K. (2018). "'Hypernudges' and Regulation: The Virtues and Vices of AI-Driven Choice Architecture." Journal of European Consumer and Market Law, 7(1), 14-27, addressing legal challenges of AI-driven decision-making in commerce.
20. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation - GDPR), establishing comprehensive data protection requirements for electronic commerce.

Citation: NOUIRI Samia & BOURDIMA Meriem. (2026). The Legal Architecture of Digital Agreements: A Comprehensive Examination of Contracts and Obligations in Electronic Commerce. *International Insurance Law Review*, 34 (1), 1-18.