

E-COMMERCE

Concept, Salient Features, Advantages, Limitations and Models

1. Introduction: Why E-Commerce Is a Cyber Law Subject

E-commerce is not merely traditional commerce performed more quickly through a website. It is commerce whose legally significant acts are mediated by computer systems and communication networks. A product listing is displayed as digital content; a consumer's selection is recorded through an interface; terms are incorporated by hyperlinks or click-based assent; payment is routed through banks and payment intermediaries; order acceptance and dispatch are communicated by automated messages; and the resulting transaction is proved through logs, emails, invoices and delivery data. The electronic form is therefore not incidental. It affects how consent is expressed, how identity is verified, how risk is allocated and how a dispute is proved.

The preamble to the Information Technology Act, 2000 captures this point with unusual clarity. It refers to legal recognition for transactions carried out through electronic data interchange and other electronic communication, commonly described as electronic commerce, using alternatives to paper-based communication and storage. The Act thus begins from a functional-equivalence principle: where law traditionally relied on paper, writing, signature, dispatch, receipt or retention, an electronic method should not be rejected merely because it is electronic, provided the statutory conditions are satisfied. Sections 4 and 5 recognise electronic records and electronic signatures; section 7 addresses retention; sections 11 to 13 address attribution, acknowledgement, and the time and place of dispatch and receipt; and section 10A confirms the enforceability of contracts formed through electronic means.

This legal perspective also explains why the subject cannot be confined to business efficiency. E-commerce creates recurring questions of consumer deception, online identity, cybersecurity, personal-data processing, cross-border jurisdiction, intermediary responsibility, intellectual property, electronic evidence and algorithmic manipulation. The same technology that makes a market available at all times also makes it possible to transact across territorial boundaries, profile a consumer at scale, automate thousands of decisions and replicate misleading content instantly. The benefits and risks are therefore two sides of the same technological design.

2. Concept and Legal Meaning of E-Commerce

2.1 From electronic exchange to internet-enabled commerce

The historical precursor to modern e-commerce was Electronic Data Interchange (EDI). EDI permits structured commercial documents—such as purchase orders, invoices, shipping notices, price lists and fund-transfer advice—to be transmitted

between the computer systems of trading partners in a standard machine-readable format. In a conventional process, a buyer may create a purchase order, send it by post or fax, and require the supplier to re-enter the same data. In an EDI environment, the buyer's system generates the purchase order, translates it into the agreed standard and transmits it directly to the supplier's system, where it can be processed with reduced manual intervention. Vakul Sharma's treatment of EDI rightly places it at the beginning of the development of electronic commerce because it converted commercial documentation from paper-based communication into system-to-system exchange.

EDI was, however, usually organised through proprietary or closed networks among identified trading partners. Internet-enabled e-commerce expanded the model. It made the network accessible to a much wider class of buyers and sellers, permitted public product discovery, enabled online negotiation and payment, and supported marketplaces in which the platform itself might not own the goods. Modern e-commerce therefore includes both highly structured B2B exchange and open, consumer-facing platform commerce. The essential continuity is that commercial information is represented, transmitted and acted upon electronically.

2.2 Government of India definition

Statutory definition

The Government of India defines e-commerce as "buying or selling of goods or services including digital products over digital or electronic network". This formulation appears in the FDI policy framework and in section 2(16) of the Consumer Protection Act, 2019.

The definition is concise but legally significant. First, it includes both goods and services. E-commerce therefore covers physical products ordered online, electronically supplied services, and mixed transactions involving digital ordering and physical performance. Secondly, it expressly includes digital products, such as software, e-books, streaming content and other electronically delivered subject matter. Thirdly, the definition focuses on the network over which buying or selling occurs; it does not require every stage of performance to be digital. A physical product ordered through a digital network remains an e-commerce transaction even though warehousing, transportation and delivery occur offline.

The Consumer Protection Act also defines an 'electronic service provider' as a person who provides technologies or processes enabling a product seller to advertise or sell goods or services to a consumer, including an online marketplace or auction site. This is important because e-commerce law regulates more than the seller. It may also regulate the platform that structures the transaction, controls the interface, collects information, displays rankings, facilitates payment or provides grievance mechanisms.

2.3 A cyber-law conception of e-commerce

For analytical purposes, e-commerce may be understood as a commercial system comprising three interdependent layers. The first is the communication layer: product information, contractual statements, confirmations, notices and instructions move electronically between participants. The second is the data-management layer: customer details, inventory, price, payment status, order history and delivery information are stored and processed in interoperable formats. The third is the trust and security layer: the system must authenticate participants where necessary, preserve integrity, restrict unauthorised access and produce reliable records. The faculty material correctly identifies communication services, data management and security mechanisms as the basic components of e-commerce.

The legal validity of the transaction depends on the interaction of these layers. A technically successful transmission is not necessarily a legally effective acceptance; a platform's order acknowledgement may be informational rather than contractual; an electronic record may exist but still require proof of origin and integrity; and a secure payment may nevertheless arise from a misleading interface. Cyber law therefore asks not only whether information moved, but who caused it to move, what legal meaning the interface assigned to it, whether the recipient could understand the terms, and whether the resulting record can be trusted.

3. Salient Features of E-Commerce and Their Cyber-Law Significance

The commonly stated features of e-commerce—ubiquity, global reach, universal standards, interactivity, information density, richness and personalisation—remain useful. A non-generic treatment, however, must connect each technological feature to a legal consequence. The following features show why the design of e-commerce changes the legal environment of commerce rather than merely its speed.

3.1 Ubiquity and continuous availability

E-commerce is available beyond the physical premises and ordinary business hours of a seller. This reduces the consumer's search and travel costs and permits transactions through computers and mobile devices from almost any connected location. Legally, ubiquity complicates the identification of the place of business, the place of contracting and the territorial forum. A consumer may access a platform in Nagpur, transact with a seller registered in another State, pay through an intermediary located elsewhere and receive an automated confirmation from a server outside India. Sections 12 and 13 of the Information Technology Act therefore matter because acknowledgement, dispatch and receipt of electronic records cannot be analysed solely through the physical movement of paper. Ubiquity also creates a continuing duty to maintain reliable interfaces,

grievance channels and security because an ‘always open’ store may create harm even when no employee is actively supervising it.

3.2 Global reach without universal law

Digital networks allow sellers to reach customers across geographical boundaries at comparatively low communication cost. The potential market is therefore not limited by the physical catchment area of a shop. Yet technical reach must not be confused with legal universality. Contract law, consumer remedies, taxation, data protection, product standards and intellectual-property rules may differ across jurisdictions. A platform accessible worldwide may restrict delivery to particular territories, select a governing law, or localise its terms. Global reach thus enlarges commercial opportunity while creating conflict-of-laws and enforcement problems. It is also incorrect to state broadly that products purchased online are free from customs duties. Physical goods ordered online remain subject to the applicable customs regime; historically, the WTO moratorium concerned customs duties on electronic transmissions, and that multilateral moratorium lapsed on 30 March 2026.

3.3 Common technical standards and interoperability

Internet protocols and common data formats lower the cost of connecting buyers, sellers, payment systems and logistics providers. EDI illustrates the same principle in a more structured setting: standardisation allows one system to interpret a commercial document generated by another. This interoperability reduces re-entry of data and facilitates automation. Legally, however, common technical standards do not by themselves create common contractual or regulatory standards. A technically interoperable transaction may still fail because the seller lacked authority, the terms were not incorporated, a mandatory disclosure was omitted or the product could not lawfully be sold. Technical standards enable communication; law determines the consequences of the communication.

3.4 Interactivity and electronic assent

Unlike one-way mass advertising, an e-commerce interface allows users to search, compare, ask questions, configure products, submit information and communicate acceptance. This interactivity makes the interface part of the contracting process. Button labels, the sequence of screens, the visibility of terms and the distinction between ‘place order’ and ‘confirm purchase’ may affect whether consent is informed and unequivocal. Interactivity can improve disclosure, but it can also be engineered to manipulate choice. The legal issue is therefore not merely whether the consumer clicked, but what the interface communicated at the moment of the click.

3.5 Information density, comparison and information overload

E-commerce increases the volume, accuracy and timeliness of information available to market participants. A consumer may compare specifications, prices, delivery terms and reviews within seconds. The same density can reduce

information asymmetry and make misleading claims easier to detect. At the same time, excessive or strategically arranged information can conceal material facts. Sponsored rankings may appear organic; crucial exclusions may be buried in expandable text; and large numbers of reviews may include fabricated or incentivised content. Information density is therefore both an advantage and a regulatory challenge. Consumer law requires material information to be clear, accurate and accessible rather than merely present somewhere on the screen.

3.6 Richness and multimedia representation

Digital commerce can combine text, images, audio, video, live demonstrations, augmented visualisation and user reviews. This 'richness' improves the consumer's understanding of a product and allows a seller to communicate complex attributes. It also broadens the evidentiary record and the scope of potential misrepresentation. A manipulated image, edited demonstration, undisclosed influencer endorsement or false environmental claim may be more persuasive than ordinary text. Because digital content can be copied and redistributed rapidly, a misleading representation can produce mass harm before corrective action is taken.

3.7 Personalisation, profiling and datafication

Personalisation enables a platform to tailor recommendations, advertisements, prices or interfaces by using a customer's identity, location, browsing behaviour and purchase history. It can reduce search costs and improve relevance. From a cyber-law perspective, however, personalisation is built upon the collection and processing of personal data. It raises questions of notice, consent, purpose limitation, security, profiling, discrimination and sharing with third parties. The legal concern is not personalisation as such, but opaque or excessive data use, especially where the platform's knowledge of the consumer is used to exploit vulnerability or to make cancellation and refusal more difficult.

3.8 Automation and algorithmic execution

E-commerce systems routinely automate inventory checks, price updates, fraud detection, order routing, customer support and communication. EDI showed the efficiency of automated business workflows; platform commerce extends automation to consumer-facing decisions. Automation reduces delay and human error, but it also raises issues of attribution and accountability. Who is responsible when an algorithm displays an incorrect price, rejects a legitimate transaction, suppresses a seller's listing or repeatedly charges a subscription? Cyber law must connect automated output to the person or entity that designed, deployed or controlled the system rather than treat the system as an independent actor.

3.9 Network effects and platformisation

Many e-commerce markets become more valuable as more sellers, buyers, reviewers and service providers join them. This network effect favours platforms that aggregate demand and data. It can improve convenience and trust by centralising search, payment and ratings, but it can also produce dependence

and unequal bargaining power. A platform may influence visibility through ranking, impose standard terms, control access to transaction data and determine the practical availability of remedies. This feature explains why the legal classification of a marketplace cannot rest solely on its description of itself as a neutral intermediary; the degree of operational control is relevant.

3.10 Persistence, replicability and traceability of electronic records

Electronic transactions produce logs, confirmations, invoices, payment references, chats and delivery records. These records may improve traceability and reduce disputes about whether a communication was sent. They are also easy to duplicate, alter or remove unless protected by appropriate controls. Digital signatures, hash functions, access controls and audit trails help establish authenticity and integrity. Vakul Sharma's explanation of digital signatures is particularly relevant: asymmetric cryptography and hash functions allow the recipient to verify that a message is associated with the signer and has not been altered after signing. The legal value of traceability therefore depends on the reliability of the system that created and preserved the record.

3.11 Disintermediation and re-intermediation

E-commerce may remove some traditional intermediaries by enabling direct sale from producer to consumer. Yet it usually creates new intermediaries: marketplaces, payment gateways, cloud providers, advertising networks, fulfilment centres and logistics aggregators. The claim that e-commerce simply eliminates the middleman is therefore incomplete. It changes the identity and function of intermediaries. The cyber-law question becomes how responsibility is distributed among entities that jointly create the consumer's transaction experience.

Table 1. Cyber-law implications of principal e-commerce features

Feature	Principal legal consequence
Ubiquity	Jurisdiction, place of contracting, continuous system responsibility
Global reach	Applicable law, cross-border enforcement, product and data regulation
Interactivity	Electronic assent, incorporation of terms, interface fairness
Information density	Disclosure, misleading claims, rankings and reviews
Personalisation	Data protection, profiling and discriminatory or exploitative design
Automation	Attribution, error allocation and algorithmic accountability
Platformisation	Intermediary status, control, dependency and allocation of liability

Feature	Principal legal consequence
Persistence of records	Authenticity, integrity, retention and electronic evidence

4. Models of E-Commerce

E-commerce models can be classified in two different ways. The first classification identifies the participants in the transaction—business, consumer or government. The second examines the operational and legal role of the e-commerce entity—whether it owns the inventory, merely provides a marketplace, aggregates services or distributes digital content. The second classification is especially important in cyber law because entities with the same B2C customer relationship may bear very different legal responsibilities.

4.1 Participant-based models

4.1.1 Business-to-Consumer (B2C)

In B2C commerce, a business offers goods or services to individual consumers through a digital or electronic network. The business may sell through its own website or through a third-party marketplace. The central legal issues are clear disclosure of the seller's identity, accurate product information, incorporation of terms, payment security, delivery, return and refund obligations, grievance redressal and protection against unfair trade practices. B2C is therefore not a single operational model: an inventory-owning retailer and a marketplace seller both transact with consumers, but the platform's responsibility differs according to its role and control.

4.1.2 Business-to-Business (B2B)

B2B e-commerce consists of electronic transactions between commercial entities, such as manufacturer and supplier, wholesaler and retailer, or enterprise and service provider. It commonly involves procurement portals, EDI, electronic invoices, supply-chain integration and repeat transactions governed by negotiated contracts. The parties are usually more sophisticated than consumers, but the legal stakes may be higher because automated errors can affect large volumes. Issues include authority of employees, standard-form purchase conditions, integration of electronic records, cybersecurity obligations, confidentiality, intellectual property and allocation of loss where a system transmits an unauthorised or erroneous order.

4.1.3 Consumer-to-Consumer (C2C)

C2C platforms facilitate transactions between individuals, commonly through classified listings, auctions or resale marketplaces. The platform may provide identity tools, messaging, payment protection or ratings. A key legal difficulty is that an individual seller may not always be a 'business' or 'product seller' in the same sense as a professional trader. The availability of consumer-law remedies may therefore depend on the facts, while fraud, stolen goods, counterfeit

products and unsafe payment arrangements remain significant risks. Platform rules and verification systems become central to trust.

4.1.4 Consumer-to-Business (C2B)

In C2B transactions, individuals supply value to businesses. Examples include freelance services, photographs, software, user-generated content, product-testing feedback, influencer promotion and reverse-auction models in which individuals propose a price. The cyber-law issues include ownership and licensing of content, disclosure of endorsements, personal-data use, standard platform terms, payment, taxation and the distinction between independent service provision and employment-like control.

4.1.5 Business-to-Government and Government-to-Business (B2G/G2B)

B2G and G2B models include e-procurement, tender portals, licence applications, tax interfaces and electronic regulatory filings. Their significance lies in formal authentication, auditability and procedural fairness. Digital signatures and Public Key Infrastructure are especially relevant because the system must verify the authorised signatory, preserve document integrity and create a reliable audit trail. E-procurement also requires equal access, transparent conditions and secure submission so that electronic convenience does not compromise public-law standards.

4.2 Operational and regulatory models

Core regulatory distinction

Participant labels such as B2C describe who transacts. Inventory and marketplace labels describe what the e-commerce entity actually does. The latter distinction is often more important for allocating responsibility.

4.2.1 Inventory-based model

Under the Government of India formulation reproduced and discussed by Vakul Sharma, an inventory-based model is one in which the inventory of goods or services is owned by the e-commerce entity and sold directly to consumers. The entity is not merely a digital venue. It is the seller or principal supplier and normally controls sourcing, price, description, invoicing, fulfilment and returns. Consumer responsibility is correspondingly direct. Defective goods, misleading descriptions or failure to deliver cannot ordinarily be shifted to an independent marketplace seller because the e-commerce entity itself owns or supplies the inventory.

4.2.2 Marketplace-based model

A marketplace model provides an information-technology platform on a digital or electronic network to facilitate transactions between buyers and sellers. The platform may list products, rank results, provide search, collect payment, arrange logistics and operate grievance channels without owning the goods. Its legal position depends on its actual functions. A genuinely facilitative marketplace is different from an entity that controls inventory or presents itself as the seller. Consumer Protection (E-Commerce) Rules, 2020 impose specific duties on

marketplace entities and require them to obtain and display prescribed information from sellers. The platform cannot rely only on contractual labels if its design and conduct create a different commercial reality.

4.2.3 Aggregator or managed-platform model

An aggregator brings together service providers—such as transport, accommodation, food delivery or professional services—under a common interface. It may standardise prices, allocate requests, collect payment, set performance standards and use ratings. Although described as an intermediary, a highly managed aggregator may exercise substantial control over the transaction. The legal analysis should therefore examine who determines the essential terms, who communicates with the consumer, who handles refunds, and whose brand creates reliance.

4.2.4 Direct-to-Consumer (D2C) model

D2C is a distribution strategy in which a producer or brand sells directly to consumers through its own digital channel. It may reduce dependence on wholesalers and marketplaces and give the business direct access to consumer data. Legally, the business assumes the complete consumer-facing responsibility of a seller, including product claims, data collection, payments, delivery and grievance redressal. D2C therefore illustrates that disintermediation may improve accountability while simultaneously increasing the seller's data-protection and cybersecurity obligations.

4.2.5 Subscription and digital-content model

Subscription services provide continuing access in exchange for recurring payment. Digital-content models may supply software, media, cloud capacity or access licences rather than ownership of a physical product. The legal issues include the duration and scope of the licence, automatic renewal, cancellation, post-termination access, interoperability, digital rights management and recurring-payment consent. A subscription interface becomes problematic when enrolment is easy but cancellation is obscured or deliberately burdensome.

4.2.6 Social and mobile commerce

Social commerce uses social-media feeds, messaging applications, influencers or live streams to promote and conclude transactions. Mobile commerce refers to transactions optimised for smartphones and app-based interfaces. These modes are commercially important but should not be treated as entirely new legal categories; they are channels layered over B2C, C2C or marketplace relationships. Their distinctive risks are compressed disclosures, blurred lines between content and advertising, informal seller identity, app permissions, location tracking and impulsive design.

Table 2. Distinguishing participant and operational classifications

Classification	What it answers	Examples
Participant-based	Who is transacting with whom?	B2B, B2C, C2C, C2B, B2G

Classification	What it answers	Examples
Operational/regulatory	What role does the e-commerce entity perform?	Inventory, marketplace, aggregator, D2C, subscription
Channel-based	Through which interface is the transaction conducted?	Website, mobile app, social media, messaging service

5. Advantages of E-Commerce

The advantages of e-commerce are often divided between consumers and businesses. That division is useful, but the benefits should be stated with appropriate legal qualifications. E-commerce does not automatically guarantee lower prices, faster delivery or wider choice; rather, its architecture can reduce particular transaction costs and make those outcomes more likely when markets remain competitive and systems are reliable.

5.1 Advantages to consumers

Convenience and continuous access. Consumers can search, compare and transact without travelling to a physical market and outside normal business hours. This is especially valuable for persons with mobility constraints or those located far from specialist suppliers. The benefit depends on accessible design, reliable connectivity and transparent delivery coverage.

Greater search capacity and comparison. Digital catalogues allow comparison of price, specifications, ratings and delivery terms across sellers. Search tools can reduce information costs. However, the comparison is meaningful only when sponsored placement, total price and material conditions are clearly disclosed.

Wider product and service availability. E-commerce can connect consumers with products that are unavailable locally, including specialised books, medicines where lawfully supplied, educational services and digital content. Geographic reach expands practical choice, although product-specific law and territorial restrictions continue to apply.

Transaction records and traceability. Order histories, invoices, payment references and communication records provide a documentary trail that may assist in refunds and disputes. The advantage is stronger than in cash-only informal trade, provided records remain accessible and have not been manipulated.

Potential price and delivery efficiency. Direct distribution, automated inventory and competition among sellers may lower costs. Digital goods may be delivered immediately. Yet platform commissions, surge pricing, personalised pricing and logistics charges may offset the savings; the proper advantage is reduced process cost, not a universal promise of low price.

Improved access to reviews and post-sale communication. Consumers can learn from prior purchasers and communicate through platform grievance systems. This can improve accountability, but fake reviews, suppressed complaints and automated responses may distort the apparent benefit.

5.2 Advantages to businesses and institutions

Lower entry and communication costs. A business can establish a digital presence without maintaining retail premises in every market. Online catalogues and targeted communication may be less expensive than repeated physical distribution of information. The business must nevertheless invest in secure systems, legal compliance and customer support.

Scalability and wider market access. A digital storefront can serve customers across regions and process high transaction volumes. Automated ordering and inventory systems allow growth without a proportionate increase in manual processing. Scalability also magnifies the consequences of error, making governance and testing essential.

Supply-chain and procurement efficiency. B2B portals and EDI reduce duplicate data entry, shorten procurement cycles and improve inventory visibility. Standard purchase orders and electronic invoices support audit and reconciliation. The efficiency depends on agreed standards and secure integration between systems.

Data-supported decision-making. Businesses can analyse demand, product performance, return rates and customer behaviour. This improves forecasting and service design, but creates corresponding duties concerning lawful data processing, security and retention.

Direct customer relationship. D2C commerce enables a producer to receive feedback and control brand presentation without relying entirely on retail intermediaries. It also makes the producer directly responsible for consumer communication, data protection and fulfilment.

Continuity and resilience. Digital channels may allow business to continue when physical access is disrupted. Cloud infrastructure, remote processing and distributed fulfilment can increase resilience, although dependence on networks and service providers creates new points of failure.

5.3 Legal and administrative advantages

E-commerce also offers advantages that are specifically legal or administrative. Electronic records can be searched, timestamped and audited; electronic signatures can establish authenticity and integrity; automated compliance checks can prevent incomplete submissions; and digital grievance systems can record the sequence of a complaint. B2G procurement and regulatory filing demonstrate how the same architecture can improve transparency and reduce paper-based delay. These benefits are strongest where the system preserves records in an intelligible form and allows authorised access throughout the required retention period, consistent with section 7 of the Information Technology Act.

6. Limitations and Risks of E-Commerce

The limitations of e-commerce are not confined to low bandwidth or the inability to touch a product. They arise from the dependence of commerce on code, networks, data and platform governance. A useful legal classification separates

technological limitations, cybersecurity and privacy risks, consumer-protection concerns, jurisdictional problems, evidentiary difficulties and structural market risks.

6.1 Cybersecurity and payment risk

E-commerce systems are attractive targets for phishing, account takeover, payment fraud, credential theft, malware, unauthorised access and manipulation of transaction data. A consumer may interact with a counterfeit website or be induced to disclose an OTP. A business may suffer compromise of an administrator account or supply-chain integration. Security failure damages trust and may expose personal and financial information. The limitation is not that online payment is inherently unsafe; it is that the system's risk is distributed across the consumer, seller, platform, bank and technical providers, while the consumer may not know which entity failed.

6.2 Privacy, surveillance and profiling

E-commerce requires data for account creation, payment, delivery and customer support, but many platforms collect substantially more through cookies, device identifiers, location, search history and behavioural analytics. Persistent tracking can reveal preferences, habits and vulnerabilities. Personalisation may become surveillance, and data collected for fulfilment may be reused for advertising or shared within an ecosystem. The Digital Personal Data Protection Act, 2023 establishes a framework for lawful processing of digital personal data, notice, consent and obligations of data fiduciaries, with commencement being implemented in stages. Privacy is therefore not a separate issue from e-commerce design; it is embedded in the business model.

6.3 Information asymmetry and misleading presentation

A consumer cannot physically inspect many products and must rely on photographs, descriptions, ratings and claims selected by the seller or platform. Images may conceal scale or quality; reviews may be fabricated; and total cost may appear only at the final stage. Digital richness can thus create a false sense of certainty. Product-specific disclosure requirements remain applicable even when sale occurs online. Vakul Sharma's discussion of Legal Metrology requirements illustrates that marketplace facilitation does not eliminate mandatory declarations concerning packaged commodities.

6.4 Dark patterns and distorted consent

Interface design can deliberately subvert consumer choice. The Guidelines for Prevention and Regulation of Dark Patterns, 2023 identify practices such as false urgency, basket sneaking, confirm shaming, forced action, subscription traps, interface interference, bait and switch and disguised advertisements. These practices show why formal clicking is not always evidence of meaningful consent. E-commerce can make a transaction frictionless for purchase while adding friction to refusal, cancellation or refund. The limitation is therefore behavioural and architectural, not merely informational.

6.5 Absence of physical inspection and fulfilment dependence

Consumers may be unable to assess fit, texture, freshness or quality before purchase. Delivery introduces risks of delay, damage, wrong product and failed reverse logistics. Digital products create a different problem: the consumer may receive access rather than ownership and may lose access if a service closes or a licence terminates. Clear descriptions, return policies and durable access to terms are necessary to reduce this uncertainty.

6.6 Digital divide, literacy and accessibility

E-commerce assumes access to a device, network, payment facility and sufficient digital literacy. Rural connectivity, language barriers, disability, age and fear of fraud may exclude users. An interface may technically be available but practically inaccessible because it is not compatible with assistive technology or presents terms only in dense legal language. The claim of universal reach must therefore be qualified by actual inclusion.

6.7 Dependence on infrastructure and third parties

Online commerce depends on hosting, domain-name systems, cloud services, payment gateways, telecommunications and logistics. Outages or termination by a service provider may stop a business immediately. Integration between legacy databases and modern platforms may be difficult and expensive, as the faculty material notes. The business may also be locked into a platform that controls customer access and transaction data.

6.8 Jurisdiction and cross-border enforcement

The seller, platform, consumer, server and payment service may be located in different jurisdictions. Terms may select foreign law or arbitration, while consumer statutes provide mandatory local remedies. Even when a consumer obtains an order, enforcement against an overseas seller may be costly. Global reach therefore increases the number of legal systems that may claim an interest in the transaction.

6.9 Electronic evidence and attribution

Electronic records are abundant but not automatically self-proving. A party may dispute who controlled an account, whether a screenshot is complete, whether an email was altered, or whether an automated message constituted acceptance. Authentication, metadata, server logs and integrity controls may become decisive. The transition from paper to electronic records reduces some evidentiary uncertainty while creating new technical questions.

6.10 Platform power, ranking and competition

Large platforms may control search visibility, access to customers, fees, reviews and data. Sellers may depend on opaque ranking systems, while consumers may mistake the platform's recommendation for a neutral result. Network effects can concentrate markets and permit self-preferencing or discriminatory treatment. This structural limitation is not captured by the traditional statement that

e-commerce has ‘low barriers to entry’: creating a website may be inexpensive, but obtaining visibility and trust in a platform-dominated market can be costly.

6.11 Corporate exposure and automated scraping

The faculty material refers to extraction of competitive information from websites as ‘web farming’. Contemporary practice includes automated scraping of prices, catalogues, reviews and product data. Public availability does not eliminate issues of database rights, copyright, contractual restrictions, cybersecurity or misuse of confidential information. E-commerce therefore increases transparency to consumers and competitors alike.

6.12 Regulatory fragmentation

An e-commerce transaction may simultaneously engage the Information Technology Act, contract law, consumer law, data-protection law, payment regulation, taxation, Legal Metrology, food or drug regulation and intellectual-property law. Compliance cannot be reduced to publishing terms and conditions. The applicable obligations depend on the product, participants, business model and degree of platform control.

7. Cyber-Law Framework That Enables and Disciplines E-Commerce

Although the principal subject of this article is concept, features, advantages, limitations and models, those topics cannot be understood without the legal framework that gives electronic activity commercial effect. The framework performs two complementary functions: it validates electronic methods and restrains their misuse.

7.1 Information Technology Act, 2000

The Information Technology Act provides the foundational legal recognition of electronic records and signatures. It supports retention of records and determines attribution, acknowledgement, dispatch and receipt. Section 10A makes clear that a contract is not unenforceable solely because proposals, acceptances or revocations were expressed through electronic records. The Act also establishes digital and electronic signature mechanisms and a regulatory structure for Certifying Authorities. Vakul Sharma’s account of public-key infrastructure explains the trust chain: the subscriber signs using a private key; the relying party verifies with the public key; and the Certifying Authority links the certificate to the subscriber’s identity.

7.2 Contract law

Electronic form does not displace the ordinary requirements of contract law. Parties must still possess capacity; consent must be free; consideration and object must be lawful; and terms must be sufficiently certain. Section 10A removes a form-based objection, but it does not validate a transaction that fails substantive contract requirements. Platform design must also distinguish a

product display, an invitation to make an offer, an order acknowledgement and final acceptance according to the governing terms and conduct.

7.3 Consumer Protection Act, 2019 and E-Commerce Rules, 2020

The Consumer Protection Act expressly includes e-commerce and electronic service providers. The Consumer Protection (E-Commerce) Rules, 2020 apply to goods and services bought or sold over digital or electronic networks, including marketplace and inventory models, and impose duties concerning information, grievance redressal and unfair trade practices. This regime recognises that online consumers require protection not only from defective products but also from deficient platform processes and misleading interface practices.

7.4 Product-specific and disclosure regulation

E-commerce does not create a regulatory-free channel. Packaged commodities, food, drugs, financial products and other regulated goods remain subject to their respective legal requirements. The book's examples of Legal Metrology and FSSAI requirements are important because they show that the platform must account for laws governing the underlying product, not only laws governing the network.

7.5 Data protection and cybersecurity

Collection of personal data for search, payment, fulfilment and personalisation must be governed by lawful purpose, appropriate notice and security safeguards. Cybersecurity must be treated as a governance obligation rather than a purely technical function because security failure can affect consumer rights, business continuity and evidence. The DPDP Act provides the contemporary statutory framework for digital personal data in India, subject to its notified commencement schedule.

7.6 Dark patterns and fair interface design

The 2023 Guidelines demonstrate the movement of consumer law from regulating only statements to regulating digital design. A technically accurate disclosure may still be unfair if the interface hides it, creates false urgency or makes cancellation disproportionately difficult. Fair e-commerce therefore requires symmetry of choice: refusal, cancellation and complaint should not be designed as obstacles while purchase is designed as effortless.

8. Analytical Synthesis

The main concepts discussed above can be brought together through one central proposition: the legal character of e-commerce follows the allocation of information and control. The more an entity controls product presentation, ranking, price, payment, fulfilment, data and grievance redressal, the more difficult it becomes to treat that entity as a merely passive technical conduit. Conversely, an entity that only transmits information without selecting, modifying or controlling the transaction may occupy a more limited role. Legal classification

should therefore examine function rather than rely only on contractual terminology.

The same proposition connects the salient features with the advantages and limitations. Ubiquity improves access but complicates jurisdiction. Information density improves comparison but enables overload and manipulation. Personalisation improves relevance but depends on intrusive data processing. Automation reduces cost but concentrates error. Traceability creates evidence but requires secure preservation. Platformisation makes commerce convenient but redistributes power. A cogent cyber-law analysis must preserve both sides of each feature rather than present technology as either inherently liberating or inherently dangerous.

The evolution from EDI to modern marketplaces also shows continuity. EDI standardised the electronic exchange of commercial documents among known partners; internet commerce opened the network to mass participation; platform commerce added data-driven intermediation; and contemporary systems increasingly automate recommendations, pricing and customer interaction. At every stage, the central legal tasks remain authentication, integrity, allocation of responsibility and protection of legitimate expectations.

9. Conclusion

E-commerce is best understood not as a website-based substitute for a physical shop, but as an electronic commercial environment in which law must recognise records, attribute communications, validate consent, protect data and allocate responsibility among multiple actors. Its salient features—ubiquity, global reach, interoperability, interactivity, information density, richness, personalisation, automation, platformisation and traceability—create both efficiency and legal risk. Its models must be classified not only by participants such as B2B or B2C, but also by the actual role of the e-commerce entity, particularly the distinction between inventory and marketplace models.

The advantages of e-commerce include reduced search and documentation costs, continuous access, broader markets, automation and improved traceability. Its limitations include cybersecurity threats, privacy loss, information asymmetry, dark patterns, digital exclusion, infrastructure dependence, cross-border enforcement, evidentiary complexity and platform concentration. The Indian cyber-law framework responds through the Information Technology Act, contract law, consumer-protection legislation, data-protection law and product-specific regulation. The governing principle is functional accountability: electronic form should enable commerce, but technological design should not be used to obscure consent, identity, responsibility or remedy.