IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

STUDY OF IT LAWS FOR MONITORING AND REGULATING E-COMMERCE AND ONLINE TRANSACTION

[1]Dr Hussain A Choudhury, [2]Salem Ahmed Barbhuiya

[1]Assistant Professor, [2]District Entrepreneurship Officer,

[1]Dept. of Computer Sc. & Engineering,

[1]Barak Valley Engineering College, Karimganj, India

Abstract: The growth of e-commerce and online transactions has led to a need for new IT laws to monitor and regulate these activities. The Information Technology Act, 2000 (IT Act) is the primary law governing e-commerce in India. The IT Act provides for a number of safeguards for consumers, including the right to privacy, the right to information, and the right to redressal of grievances. The IT Act also sets out penalties for cybercrime, including hacking, phishing, and identity theft. In addition to the IT Act, there are a number of other laws that may apply to e-commerce and online transactions. These include the Consumer Protection Act, 2019, the Payment and Settlement Systems Act, 2007, and the Competition Act, 2002. The Consumer Protection Act provides for consumer protection against unfair trade practices and misleading or false information. The Payment and Settlement Systems Act regulates the operation of payment systems in India. The Competition Act prohibits anti-competitive practices, such as price-fixing and collusion. The paper will examine the various legal issues surrounding e-commerce, such as data protection, online consumer protection, intellectual property rights, and electronic contracts. By analyzing the current legal framework, this paper seeks to provide a comprehensive overview of the legal challenges and opportunities presented by e-commerce and IT laws.

Index Terms **- IT; GDPR;ML;AI.**

I. INTRODUCTION

The emergence of e-commerce has transformed the way businesses operate and has revolutionized the global marketplace. However, the growth of e-commerce has also raised new legal and regulatory challenges. To navigate these challenges, it is essential to understand the laws and regulations that govern e-commerce activities. This paper aims to explore the legal framework for e-commerce, focusing specifically on the IT laws that impact online transactions. With the rapid advancement of technology and the proliferation of the internet, e-commerce has emerged as a dominant force in global trade and economic activities. However, the exponential growth of online transactions has raised various legal and regulatory concerns. The growth of e-commerce and online transactions is a positive development for the Indian economy. However, it also creates new challenges for law enforcement and regulators. By working together, law enforcement, regulators, and the private sector can develop new tools and techniques to monitor and regulate e-commerce and online transactions, and help to ensure a safe and secure environment for consumers.

Firstly, privacy and data protection laws play a crucial role in governing e-commerce activities. These laws safeguard the personal information of consumers and ensure that online businesses handle data responsibly. Regulations, such as the General Data Protection Regulation (GDPR), require businesses to obtain informed consent for data collection, implement appropriate security measures, and provide individuals with the right to access and control their data [1].

Secondly, cybercrime laws are essential for combating online fraud, identity theft, hacking, and other cyber threats. Such laws empower law enforcement agencies to investigate and prosecute cybercriminals, thereby safeguarding the integrity of e-commerce transactions. These laws cover offenses like unauthorized access to computer systems, online financial fraud, and dissemination of malicious software [1-2].

Thirdly, consumer protection laws play a vital role in regulating e-commerce transactions. These laws ensure that consumers have adequate information about the products or services they purchase online and protect them from unfair business practices. Consumer protection regulations address issues like deceptive advertising, product liability, unfair contract terms, and dispute resolution mechanisms.

Additionally, intellectual property laws are crucial in the e-commerce landscape to protect trademarks, copyrights, patents, and trade secrets. These laws prevent unauthorized use or infringement of intellectual property rights, fostering innovation and creativity within the digital economy [2-3].

Lastly, international cooperation and agreements are vital for harmonizing e-commerce regulations across different jurisdictions. Initiatives like the World Trade Organization (WTO) e-commerce negotiations aim to create a framework that promotes fair and open digital trade, while addressing emerging challenges and ensuring a level playing field for businesses.

II. THE MOTIVATION TO STUDY IT LAWS REGARDING E-COMMERCE

The study of IT laws regarding e-commerce is essential in today's digital era. With the increasing use of technology in commerce, it is crucial to understand the legal framework surrounding e-commerce to ensure compliance with laws and regulations. Understanding IT laws will help individuals and organizations avoid legal disputes, penalties, and reputational damage. Moreover, it can also provide an opportunity to leverage legal knowledge to create innovative business models and protect intellectual property rights. By studying IT laws related to e-commerce, individuals can gain an in-depth understanding of online contracts, privacy policies, data protection, consumer protection, and other legal issues that are relevant to the digital marketplace. Ultimately, having a solid understanding of IT laws can help individuals and organizations succeed in the competitive e-commerce landscape.

The growth of e-commerce and online transactions has created a number of new challenges for law enforcement and regulators. These challenges include:

i. The cross-border nature of e-commerce, which makes it difficult to track and prosecute criminals.
ii. The use of encryption and other technologies to make it difficult to access and analyze data.
iii. The anonymity of online transactions, which makes it difficult to identify and prosecute criminals.

In order to address these challenges, law enforcement and regulators are working to develop new tools and techniques to monitor and regulate e-commerce and online transactions. These efforts include:

i. The development of new laws and regulations to address specific challenges, such as the use of encryption and other technologies.
ii. The creation of new partnerships between law enforcement and the private sector to share information and resources.
iii. The development of new training programs for law enforcement and regulators to help them understand the challenges of e-commerce and online transactions.

III. MAJOR E-COMMERCE COMPANIES IN INDIA

Here's a general overview of the market share distribution among major players in the Indian e-commerce landscape up to that point ([34]-[37]):

Table 1: Some of the famous E commerce sites in India

E-commerce Company	Products Offered
Amazon India	Electronics, Fashion, Home & Kitchen, Books, Beauty, Grocery
Flipkart	Electronics, Fashion, Home & Furniture, Books, Beauty, Grocery
Snapdeal	Electronics, Fashion, Home & Living, Books, Beauty, Toys
Myntra	Fashion, Footwear, Accessories, Beauty
Paytm Mall	Electronics, Fashion, Home & Kitchen, Mobiles & Accessories
Tata Cliq	Electronics, Fashion, Footwear, Appliances
ShopClues	Electronics, Fashion, Home & Kitchen, Beauty, Toys
Ajio	Fashion, Footwear, Accessories, Beauty
Bigbasket	Grocery, Fresh Produce, Household Essentials
Grofers	Grocery, Fresh Produce, Home & Kitchen
Nykaa	Beauty, Makeup, Skincare, Haircare
FirstCry	Baby & Kids Products, Toys, Clothes
Zomato Market	Grocery, Food Delivery, Restaurants
Swiggy Stores	Grocery, Food Delivery, Restaurants
Urban Ladder	Furniture, Home Decor
Pepperfry	Furniture, Home Decor, Furnishings
Lenskart	Eyewear, Contact Lenses
PharmEasy	Medicines, Healthcare Products
Bewakoof	Fashion, Mobile Covers, Accessories
Infibeam	Infibeam.com employs 942 people and earns $44M in revenue. Online shopping is a speciality of Infibeam.com. An open corporation is Infibeam.com.

Many other e commerce sites include Make-my-trip, Tata Clique, Shopclues, Mesho, ClearTrip, TravelYaari, Oyo, EaseMyTrip, IRCTC, Yatraa etc etc.

IV. DETECTION OF IRREGULARITIES IN E-COMMERCE

Detecting issues in e-commerce involves a combination of technological solutions, industry standards, consumer feedback, and regulatory authorities. Here's an overview of the mechanisms and authorities involved ([4]-[8]):

A. **Mechanisms to Detect Issues:**

i. **Technology**: E-commerce platforms often employ advanced algorithms and AI systems to detect issues such as fraudulent activities, counterfeit products, pricing manipulation, and suspicious user behavior.
ii. **Customer Reviews and Ratings**: Consumers can provide feedback and reviews on products and sellers, which can help identify issues like poor quality, false advertising, or unethical practices.
iii. **Payment Gateways**: Payment processors can identify unusual transaction patterns, potentially indicating fraudulent activities.
iv. **Data Analytics**: Analysis of large-scale data can reveal patterns and anomalies that might indicate problems, such as sudden spikes in returns or customer complaints.
v. **Supply Chain Monitoring:** Tracking products from manufacturer to consumer can help identify issues related to product quality, authenticity, and ethical sourcing.

B. Authorities to Detect and Punish ([5]-[10]):

i. **Consumer Protection Agencies**: Government agencies responsible for consumer protection monitor e-commerce activities and investigate complaints from consumers. They may take actions against e-commerce platforms or sellers who violate consumer rights or engage in deceptive practices.
ii. **Competition Authorities**: Regulatory bodies that oversee fair competition can intervene if e-commerce entities engage in anti-competitive practices, such as monopolistic behavior or price-fixing.
iii. **Law Enforcement Agencies**: Legal authorities can investigate and take action against e-commerce fraud, cybercrime, and other illegal activities that take place online.
iv. **Industry Associations**: These organizations often establish codes of conduct and standards that e-commerce businesses are expected to adhere to. They can play a role in monitoring and addressing violations within their industry.
v. **Customs and Border Protection**: Authorities responsible for customs and border control can detect counterfeit goods and prevent them from entering a country.
vi. **Online Marketplaces**: The platforms themselves can implement rules and policies to monitor and address issues on their platforms. They may suspend or ban sellers engaging in fraudulent or unethical activities.
vii. **Cyber security Firms**: Companies specializing in cyber security can assist in detecting and preventing cyber threats and data breaches that can impact e-commerce platforms and their users.
viii. **International Organizations**: In the case of cross-border e-commerce, international organizations like the World Trade Organization (WTO) and the United Nations Conference on Trade and Development (UNCTAD) can provide guidelines and frameworks for member countries to address e-commerce issues.

It's important to note that the landscape of e-commerce regulation is complex and varies from country to country. Different jurisdictions have different laws and regulatory bodies overseeing e-commerce activities. Additionally, the responsibilities of these authorities might evolve over time as the e-commerce industry and its challenges continue to develop.

V. DETECTION OF ISSUES IN ONLINE TRANSACTION

Detecting issues in online transactions involves a combination of technological solutions, financial institutions, regulatory bodies, and law enforcement agencies. Here's how it generally works:

1. Mechanisms to Detect Issues in Online Transactions([11]-[13]):

i. **Fraud Detection Systems**: Financial institutions and payment processors often use advanced fraud detection systems that analyse transaction patterns, account behaviour, and other data to identify potentially fraudulent transactions. These systems can flag suspicious activities for further review.
ii. **Machine Learning and AI**: AI algorithms can learn from historical transaction data to identify unusual patterns that might indicate fraud or other issues. They can adapt to new fraud tactics as they emerge.
iii. **Two-Factor Authentication (2FA):** Adding an extra layer of verification (e.g., a text message code or biometric verification) can help prevent unauthorized access and transactions.
iv. **Geolocation and IP Analysis**: Monitoring the geographic location and IP addresses associated with transactions can help identify unauthorized or suspicious transactions.
v. **User Behavior Analysis**: Analyzing user behavior can help distinguish between legitimate and fraudulent transactions. Unusual behavior, such as sudden large purchases on a rarely used account, can raise alarms.
vi. **Device Fingerprinting**: This technique tracks unique attributes of a device used for a transaction, helping to identify when a device is being used for fraudulent activities.

2. Authorities to Detect and Punish[14]:

i. Financial Regulatory Authorities: Government agencies responsible for financial regulation, such as the U.S. Securities and Exchange Commission (SEC) or the Financial Conduct Authority (FCA) in the UK, may oversee online payment systems and financial institutions.
ii. Consumer Protection Agencies: These agencies focus on protecting consumers from fraudulent or deceptive practices. They can investigate and take action against businesses that engage in unethical practices during online transactions.
iii. Law Enforcement Agencies: Local, state, and national law enforcement agencies have jurisdiction over cybercrimes and online fraud. They can investigate and prosecute individuals or groups involved in illegal online activities.

iv. Cyber security Agencies: These organizations work to prevent and investigate cybercrimes, including those related to online transactions. They may offer resources and support to businesses and individuals to safeguard against online threats.
v. Payment Card Networks: Organizations like Visa, Master card, and others have systems in place to detect fraudulent transactions on their networks. They can alert banks and financial institutions about potentially compromised cards.
vi. International Law Enforcement Cooperation: Cross-border online fraud may involve collaboration between law enforcement agencies in different countries to track down and apprehend perpetrators.

3. Online Platforms and Marketplaces[15]-[16]:

i. E-commerce Platforms: Online marketplaces and e-commerce platforms have their own mechanisms to detect and prevent fraudulent transactions and unauthorized access. They may suspend or ban users engaging in fraudulent activities.
ii. Online Payment Platforms: Companies like PayPal, Stripe, and others have security measures to protect both buyers and sellers during online transactions.

Overall, detecting issues in online transactions requires a collaborative effort involving various stakeholders, including financial institutions, regulatory bodies, law enforcement agencies, and Technology providers. As online transaction methods and technologies evolve, so do the mechanisms used to identify and prevent issues?

VI. DIFFERENT IT LAWS FOR E-COMMERCE AND ONLINE TRANSACTION

A Model Law on E-Commerce (MLEC) was first adopted by the United Nations Commission on International Trade and Law (UNCITRAL) in 1996 and later by the United Nations General Assembly [18].

The main goal of MLEC was to establish an international uniform law governing e-commerce and to bring electronic transactions up to parity with paper-based transactions by determining the rights and liabilities of the parties to the transaction in a manner similar to paper-based transactions. The Information Technology Act of 2000 was enacted by India, a signatory to this Model Law. As a result, India passed the Information Technology (Amendment) Act, 2008 to give effect to the UNCITRAL law on E-Signature (MLES), 2001[20].

A. Classification of IT laws regarding e-commerce

E-commerce is a rapidly growing industry that has revolutionized the way businesses operate and interact with their customers. The growth of e-commerce has also led to the development of a wide range of laws and regulations that are designed to protect consumers and businesses engaged in online transactions. These laws are collectively known as IT laws, and they cover a broad range of topics related to e-commerce, such as data protection, online contracts, electronic signatures, and intellectual property rights. The classification of IT laws regarding e-commerce can be done based on several factors such as the type of law, jurisdiction, and scope. In this note, we will discuss the most common classification based on the type of law [22]-[25].

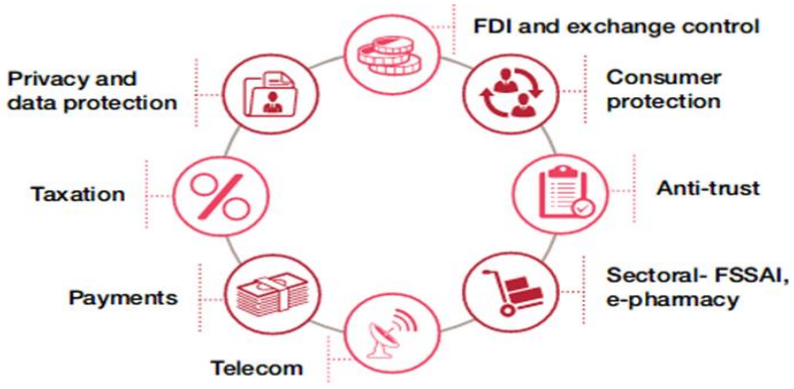

Fig 1: Factors for classification of IT laws

1. **Privacy and data protection laws:** These laws govern the collection, storage, use, and disclosure of personal information collected through e-commerce platforms. The most well-known data protection law is the General Data Protection Regulation (GDPR) which is a European Union law that regulates the processing of personal data of EU residents.
2. **Intellectual property laws**: These laws govern the protection of intellectual property rights (IPR) such as patents, trademarks, copyrights, and trade secrets. E-commerce platforms must respect these rights and not infringe them. For instance, the Digital Millennium Copyright Act (DMCA) is a US law that addresses copyright infringement and other issues related to intellectual property in the digital world.

3. **Consumer protection laws**: These laws are designed to protect consumers from unfair or deceptive trade practices by e-commerce platforms. These laws cover areas such as advertising, marketing, and sales practices. The Consumer Protection Act (CPA) is an example of such laws that govern online transactions in India.
4. **Electronic transaction laws**: These laws govern the formation and validity of electronic contracts, the use of electronic signatures, and the admissibility of electronic records in legal proceedings. The Electronic Transactions Act (ETA) is an example of such laws that provide a legal framework for electronic transactions in Singapore. Another such law is Payment and Settlement Systems Act, 2007 which governs India's payment and settlement systems
5. **Cybercrime laws**: These laws address criminal activities in the digital world such as hacking, identity theft, and online fraud. The Computer Fraud and Abuse Act (CFAA) is an example of such laws that prohibit unauthorized access to computer systems. Also Information Technology Act, 2000 - This is the primary law governing e-commerce in India. It provides legal recognition to electronic transactions and digital signatures, and outlines penalties for cybercrimes such as hacking, identity theft, and cyber stalking
6. **Taxation laws**: These laws govern the taxation of e-commerce transactions. They cover areas such as sales tax, value-added tax (VAT), and customs duties. For example, the GST (Goods and Services Tax) law in India applies to e-commerce transactions.
7. **Electronic Contracts and Signatures Laws**: These laws establish the legal validity and enforceability of electronic contracts and digital signatures. They ensure that contracts entered into electronically have the same legal standing as traditional paper-based contracts. These laws often incorporate the use of cryptographic techniques and electronic signature standards to verify authenticity and integrity.
8. **Online Dispute Resolution (ODR):** ODR laws provide mechanisms for resolving disputes arising from e-commerce transactions through online platforms. These laws promote alternative methods of dispute resolution, such as mediation or arbitration, conducted entirely online. ODR laws aim to provide efficient and cost-effective solutions for resolving disputes without resorting to traditional court proceedings.
9. **International and Cross-Border Regulations**: Given the global nature of e-commerce, there are efforts to establish international cooperation and agreements to harmonize regulations. Organizations like the World Trade Organization (WTO) and regional bodies work towards creating frameworks that facilitate cross-border e-commerce while addressing legal and regulatory challenges.
10. **Regulations Pertaining to Labelling and Packaging**
    The Legal Metrology Act of 2009, the Food Safety and Standards Act of 2006, the Drugs and Cosmetics Act of 1940, and other pertinent regulations' labelling and packaging specifications must be followed and met by an e-commerce company. The online platform is expected to offer the appropriate information about the items being presented in compliance with the Legal Metrology Act, 2009 read with the Legal Metrology (Packaged Commodity) Rules, 2011. They must mention details like size, weight, and other characteristics on the product page itself.

B. Applicable Laws & Regulations in E-Commerce

1. DIPP's FDI regulations for online shopping

Guidelines for Foreign Direct Investment (FDI) in e-commerce have been released by the Department of Industrial Policy & Promotion (DIPP). Although no FDI was previously allowed in B2C (business to consumer) e-commerce, up to 100% FDI is now allowed in B2B (business to business) e-commerce in India. The marketplace concept for e-commerce is legalised for 100% FDI under the new FDI regulations—under the automatic route. However, the inventory-based model forbids FDI. The sector in recent times has even become an essential part of various multilateral negotiations such as WTO, BRICS, Regional Comprehensive Economic Partnership (RCEP), etc. Ministry of Electronics & Information Technology is at the forefront of such demark negotiations on e-commerce on behalf of India.

Table 2 : **Laws & Regulations in E-Commerce**

Regulatory	**Technology & Data Protection**
1. **Foreign Direct Investment** Policy 2. Further, the Foreign Exchange Management Act, 1999 Companies Act, 2013 3. Payment and Settlement Act, 2007 and other RBI regulations on payment mechanisms 4. Labelling and Packaging 5. **Legal Metrology Act**, 2009 read with Legal Metrology (Packaged Commodity) Rules, 2011 6. Sales, Shipping, Refunds and Returns 7. Moreover, Regulations prescribed by the relevant ministry/state regulations	1. Information Technology Act, 2000 2. Additionally, Information Technology (Intermediaries Guidelines) Rules, 2011 3. Information Technology Act, 2000 (IT Act) and General Data Protection Regulations (GDPR). 4. **Information Technology (Amendment) Act, 2008** 5. Consumer Protection Act, 1986
Tax	**Legal**
1. Income Tax Act, 1961 2. Double Taxation Avoidance Agreement 3. Good and Services Tax	**a.** Indian Contract Act, 1872 **b.** Indian Copyright Act, 1957 **c.** The Patents Act, 1970 **d.** Intellectual Property Issues **e.** **Labour laws**

2. Overview of some IT laws regarding e-commerce and online transactions in India:

i. **Information Technology Act, 2000 (IT Act):**

The Information Technology (IT) Act 2000 was the first e-commerce law ever passed by the Government of India. It was enacted to put the 1996 UNCITRAL Model Law on Electronic Commerce into effect. On January 30, 1997, the General Assembly of the United Nations passed a resolution endorsing the Model Law on Electronic Commerce for consideration as a Model Law by the Member States when they enact or revise their laws, in light of the requirement for uniformity of the law governing alternatives to paper-based methods of communication and information storage.

The IT Act is the primary law governing e-commerce in India. It provides for a number of safeguards for consumers, including the right to privacy, the right to information, and the right to redressal of grievances. The IT Act also sets out penalties for cybercrime, including hacking, phishing, and identity theft.

ii. **Information Technology (Amendment) Act, 2008**

In order to apply the UNCITRAL Model Law on Electronic Signatures, 2001 in India, the country enacted the Information Technology (Amendment) Act, 2008. In order to make the IT Act of 2000 technology-neutral, electronic signatures were given preference over restrictive digital signatures. The Act brought about a number of changes, including the definition of an intermediary being changed and the idea of an electronic signature being introduced. In addition, the government acquired explicit authority to regulate websites in order to safeguard privacy and prevent potential abuse that could result in tax evasions. It is crucial to note that this act placed a strong emphasis on safe digital transactions and acknowledged for the first time in India the legal validity and enforceability of digital

signatures and electronic records. These adjustments were made in an effort to reduce the frequency of electronic forgeries and to make e-commerce transactions easier.

iii. **Consumer Protection Act, 2019:**
The Consumer Protection Act provides for consumer protection against unfair trade practices and misleading or false information. It also provides for a number of remedies for consumers who have been harmed by unfair trade practices, such as refunds, compensation, and damages.

iv. **Payment and Settlement Systems Act, 2007:**
The Payment and Settlement Systems Act regulates the operation of payment systems in India. It provides for a number of safeguards for consumers, such as the requirement for payment systems to be secure and reliable.

v. **Competition Act, 2002:**
The Competition Act prohibits anti-competitive practices, such as price-fixing and collusion. It also provides for a number of remedies for consumers who have been harmed by anti-competitive practices, such as refunds, compensation, and damages.

vi. **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021:**
These rules govern the conduct of intermediaries (online platforms) in India. They outline guidelines for content removal, user data protection, and cooperation with law enforcement agencies.

vii. **Foreign Exchange Management Act (FEMA):**
FEMA governs foreign exchange transactions in India. It's important for e-commerce businesses engaged in cross-border transactions to comply with FEMA regulations when receiving or sending foreign currency.

viii. **Banking Regulations:**
Online payment systems and e-commerce platforms must comply with the regulations set by the Reserve Bank of India (RBI) regarding electronic payment and funds transfer.

3. **Here are some of the key provisions of the IT Act-2000 that are relevant to e-commerce**:

i. **Section 43A**: This section provides for the protection of consumers from unfair trade practices and misleading or false information.
ii. **Section 43B**: This section provides for the right of consumers to seek redressal of grievances against businesses.
iii. **Section 66C**: This section provides for the punishment for cybercrime, including hacking, phishing, and identity theft.
iv. **Section 67**: This section provides for the punishment for publishing or transmitting obscene material in electronic form.
v. **Section 69A**: This section provides for the interception of electronic communications by law enforcement agencies.

The Consumer Protection Act of 2019's Section 94 addresses steps to stop unfair business practises in e-commerce, direct sales, etc. It specifies that the Central Government may adopt such measures in the prescribed manner for the objectives of avoiding unfair commercial practises in direct selling and e-commerce, as well as to protect the interest and rights of consumers.

In addition to these laws, there are a number of other laws that may apply to e-commerce and online transactions. The related provisions of the Indian Panel Code, 1860, the Indian Evidence Act, 1872, Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934 were also amended to address the related issues of electronic commerce, electronic crimes and evidence, and to enable further regulation as regards electronic fund transfer.

C. E commerce laws in other countries

Comparing e-commerce laws between different countries can be complex due to the variations in legal systems, cultural contexts, and technological advancements. However, I can provide a general overview of how e-commerce laws might differ between India and some other countries, such as the United States and the European Union (EU):

1. **United States:**
   a. **Electronic Signatures:** The United States has the Electronic Signatures in Global and National Commerce Act (ESIGN) and the Uniform Electronic Transactions Act (UETA), which recognize the legal validity of electronic signatures and contracts.
   b. **Consumer Protection:** The U.S. has various federal and state consumer protection laws that apply to e-commerce, such as the Federal Trade Commission Act (FTCA) and the Electronic Fund Transfer Act (EFTA). These laws focus on preventing unfair and deceptive practices, safeguarding consumers' personal information, and regulating online payment systems.
   c. **Privacy:** The U.S. lacks a comprehensive federal data protection law but has sector-specific regulations like the Health Insurance Portability and Accountability Act (HIPAA) for healthcare and the Children's Online Privacy Protection Act (COPPA) for children's data.
   d. **Taxation:** In the U.S., states have varying rules for sales tax collection on online transactions, and the Supreme Court's South Dakota v. Wayfair decision allows states to require out-of-state sellers to collect sales tax.

2. **European Union (EU):**
   a. General Data Protection Regulation (GDPR): The GDPR is a comprehensive data protection regulation that applies to all EU member states and regulates the processing of personal data. It grants individuals more control over their data and imposes strict requirements on businesses handling EU citizens' data.
   b. Consumer Rights Directive: The EU Consumer Rights Directive harmonizes consumer protection laws across EU countries. It addresses issues such as information provision, cancellation rights, and delivery of goods and services in e-commerce transactions.
   c. Digital Single Market Initiatives: The EU is working on initiatives to create a digital single market, including regulations related to geoblocking (restricting online content or services based on location) and cross-border portability of online content services.
   d. **Platform Liability**: The EU has regulations such as the E-Commerce Directive, which establishes liability exemptions for online platforms that act as intermediaries.

However, the Digital Services Act (DSA) and Digital Markets Act (DMA) are proposed regulations aiming to update the legal framework for online platforms, including addressing issues of content moderation, competition, and fairness.

3. **Comparison**
   a. While each country has its own unique legal framework for e-commerce, some common themes include consumer protection, electronic signatures, data privacy, and taxation. However, the nuances in the laws, enforcement mechanisms, and cultural considerations can differ significantly.
   b. Key differences might include the level of data protection regulation (GDPR vs. India's proposed data protection bill), the approach to platform liability, and the specifics of taxation rules for e-commerce transactions.
   c. It's important to note that laws can change, and specific circumstances can greatly impact how these laws are applied. Businesses engaging in e-commerce across different jurisdictions should seek legal advice to ensure compliance with relevant laws and regulations.

4. Issues in laws pertaining to e-commerce and online transaction([23]-[28])

Laws pertaining to e-commerce and online transactions are complex and evolving rapidly as technology advances and new challenges arise. Here are some key issues and challenges that often arise in this domain:

a. Jurisdiction and Applicable Laws: E-commerce transactions often cross national boundaries, making it difficult to determine which laws apply. Conflicts can arise when different countries have varying regulations regarding consumer protection, intellectual property rights, and taxation.

b. Consumer Protection: Ensuring consumer rights in e-commerce is crucial. Issues can range from misrepresentation of products or services, fraud, privacy violations, and the quality of goods received. Building effective mechanisms for resolving disputes and enforcing consumer protection laws online is a challenge.

c. Data Privacy and Security: E-commerce involves the collection, storage, and transfer of personal and financial data. Laws such as the General Data Protection Regulation (GDPR) in the European Union aim to protect individuals' privacy rights. Implementing strong data security measures to prevent breaches and unauthorized access is critical.

d. Cyber security and Fraud: Online transactions are vulnerable to hacking, identity theft, and payment fraud. E-commerce platforms must invest in robust cyber security measures to protect their users' data and financial information.

e. Intellectual Property (IP) Rights: E-commerce platforms facilitate the distribution of digital goods, leading to concerns about copyright infringement, trademark violations, and the sale of counterfeit products. Striking a balance between protecting IP rights and enabling legitimate commerce is essential.

f. Taxation: Determining the appropriate taxation for online transactions can be challenging due to the global nature of e-commerce. Questions arise about where sales tax should be applied, particularly for cross-border sales, digital goods, and services.

g. Electronic Signatures and Contracts: The validity of electronic signatures and contracts is a legal issue that can impact the enforceability of agreements made online. Laws like the Electronic Signatures in Global and National Commerce Act (ESIGN) in the U.S. provide a framework for recognizing electronic signatures.

h. Competition and Antitrust: E-commerce platforms can dominate markets and stifle competition. Antitrust concerns may arise if a platform engages in anti-competitive practices, such as favoring their own products or excluding competitors from their platform.

i. Domain Names and Trademarks: Disputes over domain names and trademarks can arise in the e-commerce context. Businesses might face challenges when their trademarks are used in domain names that could lead to consumer confusion.

j. Cross-Border Legal Challenges: Differences in legal systems, languages, and cultural norms can complicate cross-border e-commerce. Businesses need to navigate these complexities to ensure compliance with various regulations.

k. Digital Accessibility: E-commerce websites and platforms must adhere to accessibility standards to ensure that people with disabilities can access and use their services. Failure to comply with accessibility laws can result in legal action.

l. Platform Liability: E-commerce platforms often host third-party sellers. Determining the extent of liability for counterfeit or faulty products, as well as user-generated content, can be legally complex.

m. Regulatory Compliance: E-commerce businesses must adhere to a variety of regulations, including export controls, product safety standards, and advertising regulations, depending on the nature of the products they sell.

VII. TYPES OF FRAUDS AND ISSUES IN E-COMMERCE AND THEIR PUNISHMENT UNDER INDIAN LAWS

Table 3 : Different E commerce laws and their punishments in India

E-commerce Fraud/Issue	Description	Related Laws	Potential Punishments
Payment Fraud	Unauthorized use of payment information for fraudulent purchases	Information Technology Act, 2000; Indian Penal Code (IPC)	Imprisonment, fines under IPC sections such as 420 (cheating), 468 (forgery), 471 (using forged documents) and other sections
Phishing	Deceptive emails/websites to trick users into revealing personal information	Information Technology Act, 2000; IPC	Imprisonment, fines under IPC sections such as 419 (cheating by personation), 420 (cheating), and relevant sections of the IT Act.
Identity Theft	Stealing personal information to make unauthorized transactions	Information Technology Act, 2000; IPC	Imprisonment, fines under IPC sections such as 419 (cheating by personation), 420 (cheating), and relevant sections of the IT Act
Cyberbullying	Harassment, threats, or humiliation through online platforms	Information Technology Act, 2000; IPC	Imprisonment, fines under IPC sections such as 509 (word, gesture, or act intended to insult the modesty of a woman), 354D (stalking), and relevant sections.
Online Scams	Various fraudulent schemes to deceive users	IPC; Consumer Protection Act, 2019, SEBI Act (for securities and investment fraud).	Imprisonment, fines under SEBI Act, IPC sections like 420 (cheating), 406 (criminal breach of trust), and relevant sections of the IT Act, & other Acts.
Counterfeit Goods	Selling fake products as genuine	Trade Marks Act, 1999; Copyright Act, 1957	Imprisonment, fines
Data Breaches & Hacking	Unauthorized access and theft of personal data	Information Technology Act, 2000	Imprisonment, fines Imprisonment and/or fine under IPC sections like 379 (theft), 406 (criminal breach of trust), and relevant sections
Online Defamation	False statements damaging a person's reputation	IPC; Information Technology Act, 2000	Imprisonment, fines
Digital Payment Frauds	Fraudulent transactions using digital payment methods	Information Technology Act, 2000; Payment and Settlement Systems Act, 2007	Imprisonment, fines
Vendor Fraud	Misrepresentation by e-commerce vendors	Consumer Protection Act, 2019	Fines, legal action

VIII. FAMOUS CASE LAWS

a. In 2002, a person was convicted for a credit card fraud. It was the nation's first cyber conviction through the CBI (Central Bureau of Investigation), though the Act was not invoked, and the man was convicted under section 418, 419 and 420 of IPC.
b. Shreya Singhal v. Union of India (2015) - This landmark judgment declared Section 66A of the IT Act, which criminalized specific online speech, unconstitutional.
c. Reserve Bank of India v. Jayantilal N. Mistry (2016) - In this case, the Supreme Court held that a bank could not be held liable for unauthorized transactions on a customer's card if the customer had been negligent with their card details.
d. Google India Pvt. Ltd. v. Visaka Industries (2017) - In this case, the Supreme Court held that search engines like Google could be held liable for defamatory content hosted on third-party websites if they failed to remove the content after receiving notice.
e. Amazon Seller Services Pvt. Ltd. v. Amway India Enterprises Pvt. Ltd. (2019) - In this case, the Delhi High Court held that e-commerce platforms like Amazon could not be held liable for the sale of counterfeit products on their platform did not knowledge of the counterfeit nature of the products.
f. WhatsApp Privacy Policy Case (2021) - In this case, the Delhi High Court ordered WhatsApp to suspend its new privacy policy in India, which had been criticized for collecting and sharing user data with Facebook without adequate consent
g. Ram Jethmalani v. Union of India (2013): This case highlighted the issue of unauthorized online transactions and the need for stricter regulations to protect consumers from fraudulent activities. It emphasized the need for user authentication measures and stronger cybersecurity.
h. ICICI Bank v. Raja Ramesh (2010): In this case, the court ruled in favor of the bank, holding the customer liable for online transaction fraud due to negligence in safeguarding their credentials. This case highlighted the importance of customer responsibility in maintaining the security of their online banking details.
i. Axis Bank v. CybizCall International Pvt. Ltd. (2016): This case involved fraudulent transactions where a company's bank account was compromised. The court ruled in favor of the bank, stating that it had fulfilled its obligations to secure the account, and the fraud was a result of the company's own negligence.
j. PayPal Inc. v. State Bank of India (2016): This case revolved around the unauthorized transactions made through the plaintiff's PayPal account. The court ruled in favor of the plaintiff, highlighting the bank's negligence in handling the unauthorized transactions.
k. Ashish Dixit v. Reserve Bank of India (2016): This case questioned the liability of banks and financial institutions in cases of fraudulent online transactions. The court ruled that banks should bear the liability for unauthorized transactions if the customer isn't at fault.
l. In a recent instance, a striptease video featuring a Noida girl has been going viral online. Evidently following the release of the film by her ex-boyfriend, it was widely shared online. Both are B-school students, and since the victim's family hasn't complained about the MMS issue, the police have now filed a case under sections 506 and 507 of the IPC (threat to murder). The case was not filed under the IT Act for what reason? According to the police, no complaints regarding the MMS were filed; nonetheless, the police also believed that the Act's restrictions may use some strengthening.

IX. CONCLUSION

The IT Act is a complex law, and it is important to seek legal advice if you have any questions about how it applies to your business or your online activities. The classification of IT laws regarding e-commerce is important because it helps to ensure that consumers are protected and that businesses are held accountable for their actions. By understanding the different laws that apply to e-commerce, consumers can make informed decisions about their online purchases and businesses can operate in a safe and legal environment

In conclusion, the classification of IT laws regarding e-commerce is essential for businesses and individuals engaged in online transactions. It helps them understand their legal obligations and protect their rights and interests. Businesses must comply with these laws to avoid legal disputes and penalties. As the e-commerce industry continues to grow, new laws and regulations will emerge to address the evolving challenges and opportunities in the digital world.

REFERENCE

1. Bakos, J.Y. (1991), ''A strategic analysis of electronic marketplaces'', MIS Quarterly, Vol. 15 No. 3,pp. 295-310.
2. Basu, S. and Jones, R. (2002), ''Legal issues affecting e-commerce: a review of Indian Information Technology Act, 2000'', paper presented at the 17th BILETA Annual Conference, 5-6 April, Free University, Amsterdam.
3. Benjamin, R. and Wigand, R. (1995), ''Electronic markets and virtual value chains on the information superhighway'', Sloan Management Review, Vol. 36 No. 2, pp. 62-72.
4. Christersen, C.M., Suarez, F.F. and Utterback, J.M. (1998), ''Strategies for survival in fast-changing industries'', Management Science, Vol. 44 No. 12, pp. S207-20.
5. CII (2001), ''E-commerce in India: how to make it happen?'', Report of the CII National Committee on e-commerce 2000-2001, Confederation of Indian Industry.
6. Dutta, S. (2003), ''Impact of information communication technology on society'', Yojana, Vol. 47 No. 2, p. 24.
7. Gallaugher, J. (2002), ''E-commerce and the undulating distribution channel'', Communications of the Association for Computing Machinery, Vol. 45 No. 7, pp. 89-95.
8. Kaur, K. (2005), ''Consumer protection in e-commerce in Malaysia: an overview'', UNEAC Asia Papers, No. 10.
9. Khatibi, A., Thyagarajan, V. and Seetharaman (2003), ''E-commerce in Malaysia: perceived benefits and barriers'', Vikalpa, Vol. 28 No. 3, pp. 77-81.
10. Kuhn, P. and Skuterud, M. (2000), ''Internet and traditional job search methods, 1994-1999'', paper presented to the IRPP and CERF Conference on Creating Canada's Advantages in an Information Age, May.
11. Light, D.A. (2001), ''Sure, you can trust us'', MIT Sloan Management Review, Vol. 43 No. 1, p. 17.
12. Mitnick, K.D. and William, L.S. (2002), the Art of Deception: Controlling the Human Element of Security, John Wiley and Sons, New York, NY.
13. Neuman, B.C. and Genyady, M. (1998), ''Internet payment services'', in McKnight, L.W. and
14. Bailey, J.P. (Eds), Internet Economics, MIT Press, Cambridge, MA, pp. 401-16.
15. Nicholas, R. and Jerry, F. (2002), ''Electronic customer relationship management: an assessment of research'', International Journal of Electronic Commerce, Vol. 6 No. 3, pp. 59-111.
16. Pastor, R.S. and Alessandro, V. (2004), Evolution and Structure of the Internet: A Statistical Physics Approach, Cambridge University Press, Cambridge.
17. Poon, S. (2000), ''Business environment and internet commerce benefits: a small business Perspective'', Journal of Information System, Vol. 9, pp. 7-81.
18. Rastogi, R. (2002), Country Report on E-Commerce Initiatives, available at: www.unescap.org/tid/ publication/part_three2261_ind.pdf (accessed 4 June 2008).
19. Shapiro, C. and Varian, H. (1999), Information Rules: A Strategic Guide to the Networked Economy, Harvard Business School Press, Boston, MA.
20. Sumanjeet (2002), ''Cyber laws in need of upgrade'', Indian Business Law Journal, Vol. 1 No. 2, pp. 27-9.
21. Sumanjeet (2005), ''E-CRM building the loyal customers in the age of electronic commerce'', Pakistan Management Review, Vol. XLII No. 3, pp. 45-54.
22. Sumanjeet (2008a), ''Electronic commerce in India: the evolution of revolution'', E-Business, July.
23. Sumanjeet (2008b), ''Impact of e-commerce on economic models: little to lose; more to gain'', International Journal of Trade and Global Markets, Vol. 1 No. 3, pp. 319-37.
24. Sumanjeet (2010), ''Digital divide in India: measurement, determinants and policy for addressing the challenges of digital divide'', International Journal of Innovation and Digital Economy (accepted for publication, forthcoming issue).
25. Timmers, P. (1999), Electronic Commerce: Strategy and Models for Business-to-Business Trading, John Wiley, Chichester.
26. Zhu, K., Kenneth, L.K. and Xu, S. (2002), ''A cross-country study of electronic business adoption using the technology-organization-environment framework, paper presented at the ICIS Conference, Barcelona, 15-18 December.
27. Abha Chauhan, "Evolution and Development of Cyber Law - A Study with Special
28. Reference to India," available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2195557 (Visited on June 6, 2016).

29. Dr. Jyoti Rattan, "Law Relating to E-commerce: International and National Scenario with Special Reference to India" 1(2) IJSSEI 7 (2015).
30. ET Bureau, "Don't let regulatory issues hamper ecommerce in India; Constitute an 'informed' empowered committee" The Economic Times Sep. 21, 2014.
31. 4. Jayanth Pattanshetti Associates, "Ecommerce Laws In India: Foreign Investment And Retail Trade" 2-3 available at: Https://Pattanshettiassociates. Wordpress. Com/2015 /01/02/Ecommercelawsinindiaforeigninvestmentandretailtrade/ (Visited on June 3, 2016).
32. K. M. Baharul Isalm, "E-commerce: Laws and Cyber Crimes," available at: https://www.academia.edu/694983/ECOMMERCE_LAWS_AND_CYBER_CRIMES (Visited on June 6, 2016).
33. M.M.K. Sardana, "Evolution of E-Commerce in India: Challenges Ahead (Part 2)" 3 available at: http://www.isid.org.in/pdf/DN1408.pdf (Visited on June 6, 2016).
34. Nishith Desai Associates, "E-commerce in India, Legal, Tax and Regulatory Analysis" available at: http://www.nishithdesai.com /fileadmin /user_upload /pdfs /Research%20Papers /ECommerce_in_India.pdf (Visited on June 6, 2016).
35. Rajendra Madhukar Sarode, "Future of E-Commerce in India Challenges & Opportunities" 1(12) IJAR 646 (2015).
36. Sumanjeet,"E-Commerce Laws in the Indian Perspective" available at: http:// www. smsvaranasi.com/insight/ecommerce_laws_in_the_indian_perspective.pdf (Visited on June 7, 2016) Anderson, E., Day, G.S. and Rangan, V.K. (1997), ''Strategic channel design'', Sloan Management Review, Vol. 38 No. 4, pp. 59-69.

Web resources:
37. https://kanoongurus.com/blog/e-commerce-fraud-in-india/