


AMIT KUMAR KASHYAP,

MBA, LLM,

Nirma University, Ahmedabad (India),

Institute of Law;

 <https://orcid.org/0000-0002-2716-8482>,

e-mail: amit1law@gmail.com;


MAHIMA CHAUDHARY,

B.Com, LLB, Student Research Fellow,

Nirma University, Ahmedabad (India),

Institute of Law,

Centre for Corporate Law Studies;

 <https://orcid.org/0009-0004-1864-1778>**CYBER SECURITY LAWS AND SAFETY IN E-COMMERCE IN INDIA**

In today's information technology age, the issue of cyber Security is a complicated and fascinating area of law. The phenomenal growth and development of e-commerce in India is astounding. However, with the rising dependence on internet commerce, the dangers of fraud and security and trust problems have become severe impediments. Creating robust legal and regulatory frameworks that meet the growing concerns about online fraud, data security, and intellectual property protection in both local and international business contexts is critical. The e-commerce sector, like any expanding business, confronts various obstacles, primarily due to an inadequate and inefficient legal and regulatory framework that fails to guarantee the rights and duties of all players engaged sufficiently. To protect user data, tackle cyber threats, and maintain customer trust, e-commerce enterprises must comply with legal regulations. In India, cybersecurity governance falls under the Information Technology Act of 2000, regulating e-commerce, electronic contracts, data protection, and cybercrimes. The imminent passage of the Personal Data Protection Bill, 2019, is expected after ongoing review. The Indian Penal Code addresses unauthorized access, hacking, identity theft, phishing, and computer virus dissemination. The Reserve Bank of India oversees online payment and financial security, mandating two-factor authentication, encryption, and secure payment channels. CERT-In coordinates national cybersecurity incidents, while electronic signatures and digital certificates hold legal recognition. Intellectual Property Laws regulate online violations of patents, copyrights, and trademarks. The Indian government also enforces cybersecurity standards for enterprises and organizations, covering IT infrastructure and incident response. Nonetheless, further steps must be taken to improve the efficiency of India's cyber security regulations. This research study uses a doctrinal and analytical approach to examine India's present Cyber Security Laws and Guidelines. It assesses their effectiveness in addressing legal concerns with Security, privacy, and data protection inside the country. It also evaluates the legal structure that governs the link between e-commerce and Cyber Laws in India. This research will provide a thorough overview of the present condition of cyber security regulations in India, setting the way for prospective reforms and progress in this critical area.

Key words: law, safety, cyber security, e-commerce, data protection, information technology.

Original article

INTRODUCTION. In our world, two significant revolutions have taken place. First is Industrialization, and the second is the electronic revolution called "e-commerce". The onset of the 21st century has marked the beginning of a new era, the E-revolution, which connects people across different corners of the globe (Rattan, 2015). India's internet growth is fueled by affordable access and rising consumer awareness, leading to significant expansion in recent years (Nanda, Xu, Zhang, 2021).

Online marketplaces have transformed shopping habits, enabling cross-border e-commerce and affordable access to a broader range of products and services.

Customers now enjoy an advantage in purchasing primarily online due to intensified competition among businesses (Barkatullah, 2018). The business landscape has experienced numerous advancements resulting from collaborations between corporations, between corporations and individuals, and among individuals (Tanimoto,

2012). Many companies now conduct a significant portion of their operations on the Internet, encompassing B2B, B2C, and C2C transactions (Aljifri, Pons, Collins, 2003). The global e-commerce sector has grown substantially, including elements such as e-marketing, electronic funds transfer, inventory management systems, and online transaction processing (Taher, 2021). This trend is also expanding in India (Shanker, 2008). The e-commerce ecosystem in India involves crucial entities like the government, transportation companies (including Indian Rail, airlines, and roadways firms), merchants, manufacturers, and content providers (Vishwakarma, 2019). These companies, along with ISPs, call centres, shipping companies, financial intermediaries, and social media sites, facilitate online transactions. However, the current progress of e-commerce in India lags behind the growth of internet penetration (Singh, Gupta, Vatsa, 2021). In the face of technological advancements, digital crime poses a dangerous challenge, evolving from financial theft to covert operations and corporate data breaches (Ajiji, 2020). It has become a pressing concern today.

India regulates cyber crimes such as website defacement, spam, hacking, and phishing through the Information Technology Act 2000 (I.T. Act). This legislation aims to confer legal validity to electronic transactions and prevent cybercrimes.

The protection of intellectual property (I.P.) is increasingly recognized as vital for digital organizations, encompassing elements such as software copyright, copyrighted ideas, trademarks, and trade secrets (Mejias, Harvey, 2012). Protecting intellectual property (I.P.) rights in cyberspace is essential for businesses to stay competitive and safeguard digital assets. I.P. laws establish ownership, encourage innovation, and deter unauthorized use or infringement (Chudasama, Patel, 2021).

Cybersecurity in digital business protects intellectual property, promoting innovation, fair competition, trust, and Security. Existing intellectual property laws in India are considered adequate to address emerging cybersecurity concerns in the digital medium, despite the unchanged intellectual property rights regime under the I.T. Act (Kethineni, 2020).

PURPOSE AND OBJECTIVE OF THE RESEARCH. This study assesses cyber security legislation and safety in electronic commerce in India. It analyzes deficiencies in the legal framework and obstacles stakeholders face in ensuring cyber safety. The research evaluates measures such as data protection, privacy laws, and penalties for non-compliance. The study will also examine the various regulatory standards, including

the I.T. Act 2000 and other relevant rules and guidelines, to safeguard against cyber threats and cybercrime.

This study evaluates the effectiveness of current cybersecurity legislation in addressing evolving risks in electronic commerce. The article analyses the legal and regulatory framework for cyber Security in e-commerce and proposes policy reforms to strengthen transaction security in India.

METHODOLOGY. The methodology is based on the doctrinal method. A doctrinal study of cyber law analyzes rules and principles governing cyber safety and Security in e-commerce. A qualitative approach is used, focusing on external sources and secondary data sources. The article examines regulatory changes in cybersecurity, data protection, and e-commerce in India using a literature review, source analysis, and case study, focusing on secondary sources and concluding. The author has referred to critical pieces of cybersecurity legislation in India, such as:

- Information Technology Act 2000;
- Information Technology Amendment Act 2008;
- Companies Act of 2013;
- Indian Penal Code (IPC) 1980;
- Consumer Protection Act, 2019;
- Indian Contract Act, 1887;
- Constitution of India, 1950;
- The Indian Telegraph Act, 1885;
- Indian Evidence Act, 1872;
- Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013;
- Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011;
- The Information Technology (Information Security Practices and Procedures for Protected System) Rules 2018;
- The Information Technology (Intermediaries Guidelines) Rules, 2011;
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021;
- Companies (Management and Administration) Act 2014, as Amended occasionally.

To conduct a comprehensive and compelling study of cyber law, researchers can use various online legal databases such as Manupatra, Westlaw, LexisNexis, and academic search engines like Dimensions, Google Scholar, and others. Moreover, Electronic research databases like SCOPUS, Elsevier, Hein Online, and SSC Online have been used to collect secondary data to analyze the legal provisions in context.

RESULT AND DISCUSSION

The interplay between Cyber-crime and e-commerce

The Oxford Reference Online describes “*digital wrongdoing*” as wrongdoing submitted over the Web. The term “Cybercrime”, as defined in the “Cybercrime Treaty of the Council of Europe”, encompasses offences such as copyright infringement and crimes against information (Popko, 2021). Digital or computer-based wrongdoing involves using Information Communication Technology (ICT) components to cause harm to individuals, businesses, governments, and ICT infrastructure (Krishna, Karlapalem, Chiu, 2004). Rising online business activities attract cybercriminals, posing risks to data and financial Security. India faces e-commerce fraud challenges, necessitating a balance between development and Security.

Validity of the E-Contracts in E-commerce

The “*Indian Contract Act of 1887*” (ICA 1887) shall govern the administration of all online contracts. Before making any online purchases, the terms and conditions must be acknowledged for a contract to be implied between the buyer and the seller. Some contracts, such as those created by tapping an “*I acknowledge*” tab, are known as “*click-wrap*” contracts (Gholap, 2018). “*Peruse wrap*” is likewise a perceived type of a suggested agreement made by the little perusing of a site (Kidd, Daughtrey, 2000). Along these lines, all standards of agreement law would apply to web-based business exchange. For a contract to be valid, it must fulfil all the prerequisites outlined in the ICA.

All parties must agree to construct a legally enforceable e-commerce contract. Age, mental ability, and assistance affect online agreements. Whether “*click wrapping*” or “*shrinkwrapping*”, an e-contract’s terms and conditions must conform with the ICA (Bhachawat, 2021). These aspects gain significance in an e-commerce contract when disputes arise.

E-contracts lacking negotiation alternatives may be intrinsically unfair or oppressive (Schwartz, Scott, 2003). This prompts the query of whether courts can reject excessive standard-form contracts in e-commerce. In the U.S., such agreements often face case-specific scrutiny for fairness. In India, the fairness of standard Internet agreements lacks a definitive rule, but the ICA 1887 addresses contracts conflicting with public policy. Indian e-commerce laws offer limited guidance, necessitating further development and clarification.

Privacy & Data Protection in E-commerce

Gathering customer personal information is nearly unavoidable in online transactions involv-

ing financial status, personal characteristics, and other relevant details (Singh, 2011). E-commerce systems also collect users’ interests, habits, search history, and more in addition to the necessary information. Under “Section 79” of the “Information Technology (Amendment) Act of 2008”, an intermediary is not liable for the content of any information, data, or communication link he makes accessible or provides on behalf of a third party (Halder, Jaishankar, 2021). “Clause 43A” compensates customers whose personal data may have been compromised by a firm, clarifying the company’s data protection responsibilities. In violation of a legal contract, “Section 72A” makes disclosure illegal (Duraiswami, 2017). Private personal information disclosure can lead to fines of 5 million or three years imprisonment for unauthorized commercial dealings. National security offences were monitored by tightening Section 69. Updated and divided malware and pornographic material sections 66 and 67 increased cybercrime penalties. It prevents the illegal acquisition, distribution, or transfer of intimate body pictures in contexts where women reasonably anticipate privacy (Agarwal, 2012). This crime carries a 3-year sentence and a 2 lakh rupee fine.

Section 43A of the I.T. Act establishes guidelines for safeguarding personal and sensitive data to be followed by body corporates (Determann, Gupta, 2019). This places the responsibility on e-commerce businesses and platforms to establish secure systems and protocols to comply with the law.

Jurisdiction in matters of disputes in cases of privacy breaches in e-commerce

E-commerce relies on order processing, delivery coordination, and electronic payment processing, requiring prompt resolution of challenges to prevent irreversible consequences. Resolving B2C disputes can be challenging (Malik, Choudhury, 2019). Conflicts are decided in the party’s physical jurisdiction, with varying rules in different countries.

Courts in several nations first used the Internet to determine jurisdiction in web-related transactions. U.S. courts noted that a foreign court’s jurisdiction would not immediately be recognized in the original country. Instead, it would need to be evaluated by the local court based on its laws and constitution (Ahmad, 2009). In the U.S., Courts use a website’s interactivity and commercial aspect to determine jurisdiction. They have divided website activities into three categories:

a) fully interactive websites where customers can purchase products or services, exchange information or files, or enter agreements;

b) completely passive sites where information is available for people to view;

c) websites that fall somewhere in between, with limited interactivity.

Unless the administrator specifically denied the transaction or did not target the state, courts favour local jurisdiction over out-of-state logical site administrators. Non-state dormant sites rely less on local legislation. Online commerce scope and authorization laws in India are continually developing (Das, 2000).

The “long arm ward” provision extends local regulations beyond their jurisdiction if they have illegal or unfair effects internationally (Bali, 2007). Section 75 of the I.T. Act applies to offences or violations committed outside India involving a computer, computer system, or network located within India (Dwivedi, 2020). Section 3 of the IPC extends jurisdiction to prosecute individuals for crimes committed abroad, treating them as if committed within India. However, e-commerce jurisdiction remains unaddressed, mainly in Indian statutes.

Financial Transaction & E-commerce

The “Payment and Settlements Systems Act of 2007” defines a “*payment system*” as any mechanism that facilitates funds transfer between a player and a recipient. Stock exchanges are also included, although services for clearing payments or settling trades are not (Singh, Gupta, Vatsa, 2021). A company wishing to accept online payments must demonstrate that they comply with RBI regulations (Tiwari, 2019). Additionally, for an intermediary to accept electronic payments, a Nodal Account must be functional to settle the merchants’ charges on that intermediary’s online e-commerce platform.

In addition, in 2018, the government released a proposed e-commerce policy. This strategy must have been formulated considering domestic and foreign considerations (Dudin et al., 2018). There are a lot of pro-commerce provisions in the proposed policy. For instance, if payment systems follow the advice to create a central KYC registry, they would save money and time on KYC compliance.

Competition & Consumer Protection in E-commerce

Measures to prohibit unfair business practices in e-commerce, direct selling, and other areas are discussed in Section 94 of the “Consumer Protection Act”, which was passed in 2019. The Central Government is empowered to take measures to curb unfair trade practices and protect consumer rights in direct selling and e-commerce.

Regulatory Aspects of Cyber Security and Safety

Ensuring cyber safety and Security in India requires robust enforcement and prosecution mechanisms supported by solid legislation, sector-specific regulations, and coordinated responses to cyber incidents.

Constitution of India

Article 19(2) of the Indian Constitution permits the government to restrict freedom of speech to safeguard national sovereignty, integrity, Security, foreign relations, public order, decency, and morality and prevent defamation, libel, or incitement. Safety and stability take precedence.

The Indian Telegraph Act, 1885 (I.T. Act, 1885)

Section 5(2) of the “Indian Telegraph Act, 1885” authorizes the Central Government, a State Government, or authorized persons nominated by them to legally intercept communications in times of public emergency or for public safety. India’s sovereignty, integrity, state security, good ties with other countries, public order, and prevention of encouragement to commit acts of terrorism are all at stake. Hence this interception is necessary.

Information Technology Act, 2000

The Information Technology Act of 2000 (ITA 2000) is India’s first e-commerce legislation. The “United Nations General Assembly” passed it on January 30, 1997, making law the “UNCITRAL Model Law on Electronic Commerce” from 1996. As an alternative to paper, this Model Law helped member states create uniform legal frameworks for electronic communication and data storage.

The ITA aimed to legally recognize e-commerce, including information exchange and electronic communication, and promote its growth in India. Its provisions, called “Legal Acknowledgment of Electronic Records”, covered digital signatures, accountability for electronic records, authentication, and establishing transmission details. The Act outlines penalties for cybercrimes, focusing on Certification Authorities (C.A.s) and their appointment, licensing, international recognition, and digital signature obligations. It addresses offences like hacking, source code tampering, data dissemination, confidentiality breaches, and fraudulent digital signature use. The Adjudicating Authority and Cyber Regulatory Appellate Tribunal adjudicate cyber disputes and criminal crimes. The Act promotes electronic financial transfers, e-commerce, cybercrime, and digital evidence. The “Indian Penal Code 1860”, the “Indian Evidence Act 1872”, the “Banker’s Book Evidence Act 1891”, and the “Reserve Bank of India Act 1934” were all updated to address the problems with e-commerce and electronic evidence and give more clarity for businesses.

Information Technology (Amendment) Act, 2008

Indian law was changed by adding the “Information Technology (Amendment) Act, 2008” so that the “UNCITRAL Model Law on Electronic Signatures, 2001” could be used. Amendments to the Information Technology Act of 2000 were made to reduce reliance on technology and enable lawful authentication.

The implementation costs were high, but introducing electronic signatures and refined definitions for intermediaries enhanced Security and streamlined online commerce in India.

Safety and Security Regulations

The Regulations Concerning Information and Communications Technology (the I.T. Rules). The focal point of the Information Technology Rules lies in overseeing specific elements related to data collection, transmission, and processing. These rules encompass the following provisions.

- Following the “*Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013*”, Computer Emergency Response Team (CERT-In), the central agency, collects, analyzes, and shares cyber incident information. It implements emergency measures, handles incidents, and addresses emergencies, ensuring efficient response and mitigation.

- The “*Information Technology (Information Security Practices and Procedures for Protected System) Rules 2018*” mandates implementing specific information security measures.

- The “*Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011*”, also known as SPDI Rules, outline security practices for personal and sensitive data collection and processing, available on the department’s website. Intermediaries must report cybersecurity vulnerabilities to CERT-In. The SPDI Rules also acknowledge the “International Standard ISO/IEC 27001 on Information Technology” – Security techniques – Information security management systems – Requirements as an acceptable security standard that corporate entities can adopt to protect personal information.

- The “*Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021*” prohibit hosting certain types of content on the Internet and regulate the role of intermediaries, including social media intermediaries, in safeguarding the personal data of their users during online activities.

- The “*Information Technology (Guidelines for Cyber Cafe) Rules 2011*” require cybercafés to register with a designated agency and maintain a log of users’ identities and internet usage.

- The “*Information Technology (Electronic Service Delivery) Rules 2011*” empower the gov-

ernment to designate certain services, such as applications, certificates, and licenses, to be delivered electronically.

- The Indian Companies Act of 2013 grants the “*Serious Frauds Investigation Office*” (SFIO) the authority to file criminal charges against Indian corporations and their directors. The Companies Inspection, Investment, and Inquiry Rules of 2014 strengthen SFIOs’ role in cyber forensics, electronic discovery, and cybersecurity due diligence. The “*Companies (Management and Administration) Rules, 2014*” outline cybersecurity obligations for business directors and executives, requiring them to ensure the Security of electronic records against unauthorized access and tampering.

- The “*Indian Penal Code 1860*” also contains provisions to punish offences, including those committed in cyberspace, such as defamation, cheating, criminal intimidation, and obscenity.

Role of Government and Policy Reforms in E-Commerce Safety and Security

Various regulatory bodies, such as the “*Reserve Bank of India*” (RBI), the “*Insurance Regulatory and Development Authority of India*”, the “*Department of Telecommunication*” (DOT), and the “*Securities Exchange Board of India*” (SEBI), have issued circulars mandating their regulated entities to comply with cybersecurity standards.

The RBI released the “*Guidelines on Regulation of Payment Aggregators and Payment Gateways*” in March 2020, which necessitates payment aggregators to store data only in India for unrestricted supervisory access by the RBI.

The Ministry of Communication and Information Technology introduced the “*National Cyber Security Policy*” in 2013, promoting a secure online environment, strengthening laws and early warning systems for cyberattacks, and aligning with organizational objectives and international standards.

Governance through CERT-In

CERT-In has been operational since January 2004, and its primary constituency is the Indian Cyber Community. CERT-In is a vital agency in India’s e-commerce governance, providing cybersecurity services and coordinating incident response activities (Patil, 2022).

CERT-In monitors cyberspace for cyberattacks. It gathers, analyses, and shares e-commerce cyber occurrences (Kumar et al., 2016). CERT-In publishes recommendations, advisories, vulnerability notes, information security practises, procedures, incident prevention, response, and reporting to secure Indian e-commerce. It warns stakeholders, anticipates cybersecurity, and organises incident response (Singh, Gupta, Kumar, 2016). As per its constitution under I.T. Act, CERT-In performs the following functions:

- they are collecting, analyzing, and disseminating information about cyber incidents;
- issuing cybersecurity incident forecasts and alerts;
- responding immediately to cybersecurity incidents;
- coordinating activities related to responding to cyber incidents;
- publishing guidelines, advisories, vulnerability notes, whitepapers, and other materials on information security practices, protocols, and the prevention, response, and reporting of cyber incidents;
- undertaking any additional tasks related to cybersecurity that may be necessary.

Digital India and Aadhar

At the core of “*Digital India*” is the Aadhaar identity program, which provides every citizen of the country with a unique identity number or Aadhaar number (Jain M., 2019).

Aadhaar, the world’s most extensive biometric I.D. system, promotes inclusive governance, public sector reforms, and budgetary management. It ensures accountability, efficiency, and inclusive development through secure authentication and unique identity elimination.

Intellectual property

The I.T. Act and related laws equally apply to cyber threats involving intellectual property and grant similar protection. In 1999, the government enacted crucial legislation to protect intellectual property rights, which drew from global best practices. The legislation included the following:

- “*The Patents (Amendment) Act, 1999*” introduced a mailbox system for patent filings and granted exclusive marketing rights for five years;
- “*The Trademarks Bill, 1999*”;
- “*The Copyright (Amendment) Act, 1999*”;
- “*The Geographical Indications of Goods (Registration and Protection) Bill, 1999*”.

The biggest hurdle in cyberspace is the violation of intellectual property (I.P.) and the existing legal framework’s insufficiency, which includes the Copyright Act of 1957, I.T. Act, and Trademark Act of 1999. Surprisingly, the Information Technology Act of 2000 doesn’t address intellectual property protection, even though I.P. infringement is a significant challenge in cyberspace.

Copyright and domain name infringement are standard on the Internet, but the Copyright Act of 1957 and the Trademark Act of 1999 are mute, despite dealing with related problems (Austin, 1999). As a result, we lack enforcement machinery to safeguard domain names online (Jain I., 2023). It is time for the government to enact new legislation to ensure intellectual property in cyberspace.

For any company venturing into the online business world, safeguarding intellectual property

(I.P.) rights is crucial (Bressler, 2014). The Internet’s expansive nature and limited regulations pose challenges in protecting intellectual property rights in e-commerce. India’s established frameworks for physical transactions are ineffective in e-commerce, and domain name disputes remain unresolved.

E-commerce enterprises must register their domain names. Trademark law regulates domain names (Nguyen, 2001). Domain name registries may register similar domain names but not identical ones. Third parties may purchase deceptively similar domain names (Shackelford, 2016). I.P. legislation affects cyber Security, primarily online. Corporations and organisations prioritise rights preservation for competitive advantage and digital asset protection. DRM and watermarks protect cyber Security (Natarajan, Makhdumi, 2009). Software piracy is another significant type of copyright infringement directly affecting computer software (Christensen, Eining, 1991), generally addressed through copyright and patent laws. Two common forms of copyright infringement are framing and linking (Wassom, 1998).

Linking redirects visitors to another website, creating a perceived connection. Cybercriminals exploit the tension between public access and copyright holders’ rights, infringing on copyright.

Framing allows consumers to access content protected by intellectual property rights directly through their web browsers.

Trademark infringement and cybersquatting involve websites using meta tags or keywords to redirect traffic and cause financial harm. Protecting trademarks and domain names is crucial to prevent association with reputable brands. Domain name disputes should follow ICANN guidelines (Davis, 2000).

Safeguarding intellectual property rights is vital for innovation and fair competition. Indian laws lack specific regulations for domain names, requiring comprehensive measures to address e-commerce disputes (Finck, Moscon, 2019).

Prosecution and Enforcement to Ensure Cyber Safety and Security

Prosecution and Enforcement ensure cyber safety in India. Sections of the I.T. Act and IPC are utilized, but comprehensive data protection regulations are lacking.

Prosecution. The I.T. Act, read with IPC and CrPC, provides the power of prosecution in cases of contravention of its provisions or commission of any cybercrime.

- I.T. Act & CrPC: The state may appoint any person as a special public prosecutor for I.T. Act violations under Section 61. The special public prosecutor has the same authority as the Code of Criminal Procedure, 1973 public prosecutor.

- I.T. Act & IPC: Indian authorities use the I.T. Act and IPC to prosecute organizations that violate information security laws. The lack of a comprehensive data protection framework that allocates cybersecurity duties to all relevant businesses should be considered when making such decisions.

- Penalties under the I.T. Act for Cybercrime: Hacking, manipulating computer source code, denial-of-service attacks, phishing, malware attacks, identity fraud, electronic theft, cyberterrorism, privacy violations, and introducing computer contaminants or viruses are punishable by fines and imprisonment under the I.T. Act.

- Powers of Adjudicating Authorities: The adjudicating authorities designated under the I.T. Act possess the authority, similar to a civil court, to request evidence and documentation and summon witnesses for an investigation into any violation under the I.T. Act.

Non-compliance with regulations designed to prevent cybersecurity breaches can result in significant penalties, as follows:

- Section 43 of the I.T. Act: Unauthorized access to computer systems, data extraction, and system disruption can lead to liability for damages under this provision;

- Section 66 of the I.T. Act: Under this section, individuals guilty of fraud or dishonesty can face imprisonment for up to three years or a fine of up to 500,000 rupees;

- Section 66C of the I.T. Act deals with the fraudulent or dishonest use of another person's electronic signature, password, or unique identification feature. Offenders can face imprisonment for up to three years and a fine of up to 100,000 rupees;

- Other Penalties: I.T. Act penalizes entities for non-compliance with CERT-In requests, with potential imprisonment, fines, or both;

- Sector-specific authorities: Regulators like the RBI may also impose penalties for non-compliance with sector-specific cybersecurity standards.

Organizations must comply with cybersecurity regulations and standards to avoid such penalties and safeguard their data and systems against cyber threats.

Enforcement:

The ITA Act 2000 is a comprehensive law that deals with various aspects of electronic communication, electronic governance, and cybercrime in India. The Act grants certain powers of Enforcement to different authorities to ensure compliance with its provisions and tackle cybercrime.

- Section 48 of the I.T. Act empowers the Controller of Certifying Authorities (CCA) to in-

vestigate and audit Certifying Authorities (C.A.) for compliance.

- Section 49 establishes CERT-In as the national agency for cybersecurity incidents, with the authority to investigate and issue guidelines.

- Section 69 permits the government to intercept and monitor computer resources in the interest of national Security.

- Section 66 allows the police to investigate cybercrimes and conduct search and seizure operations without a warrant if there are reasonable grounds to suspect an offence.

Judicial Trends

In the matter of "Jaydeep Vrujlal Depani v State of Gujarat" R/SCRA/5708/2018 Order, the Gujarat High Court defined cybercrime as offences committed to harm an individual's or group's reputation, inflict direct or indirect physical or mental harm or loss on the victim, to utilize modern telecommunication networks such as the Internet (including platforms like chatrooms, emails, noticeboards, and groups) and mobile phones (via Bluetooth/SMS/MMS).

In the case of "Justice K S Puttaswamy (Retd) and Anr v Union of India and Ors" (Writ Petition (Civil) No. 494 of 2012), the Supreme Court of India established the right to privacy as a fundamental right. The court affirmed that the right to privacy is an inherent component of the right to life and personal liberty under Article 21 of the Constitution of India, thereby recognizing it as a fundamental right applicable to all individuals.

These two cases hold significant importance in defining cybercrime and acknowledging the right to privacy as a fundamental right. The Gujarat High Court's definition of cybercrime enables the identification of specific types of offences falling within this category, facilitating a clear understanding of what constitutes a cybercrime.

CONCLUSION. The rapid growth of e-commerce has created a need for efficient and effective regulatory mechanisms in India. The absence of a proper regulatory structure and weak digital security laws have been cited as major obstacles hindering the success of e-commerce in India. The Indian government must establish a legal framework that protects consumers' fundamental rights, such as privacy, intellectual property, fraud prevention, and consumer protection, while promoting domestic and international trade.

As technology advances and brings about innovations, adopting stronger legal measures for safeguarding sensitive data, information, and intellectual property online becomes crucial. With the emergence of novel cybercrimes targeting intellectual property, it becomes necessary to establish new laws beyond traditional regulations.

This is because the existing legal framework is inadequate in addressing the unique challenges encountered in protecting and tracing intellectual property infringers in the cyber world.

The Information Technology Act now regulates India's e-commerce sector, while intellectual property protection falls under separate regulations. Legal experts play a crucial role in ensuring compliance with existing laws for e-commerce operations, balancing technology's potential with practical regulatory limitations. However, the absence of specific regulations poses challenges in taxation, data protection, consumer rights, and cross-border trading. To address these issues,

collaboration between the Indian government, industry professionals, solicitors, and stakeholders is necessary.

Creating an appropriate legal framework requires a comprehensive e-commerce policy that fosters inclusivity and sustainability. This policy should be supported by a robust regulatory system that safeguards consumer rights, facilitates domestic and international commerce, and establishes a transparent and predictable business environment for entrepreneurs and investors. By nurturing an enabling environment, India can fully capitalize on the potential of e-commerce as a significant catalyst for economic growth and development.

REFERENCES

1. Agarwal, V. (2012). Privacy and data protection laws in India. *International Journal of Liability and Scientific Enquiry*, 5(3-4), 205-212. <https://doi.org/10.1504/IJLSE.2012.051949>.
2. Ahmad, T. (2009, September 30). *Technology convergence and protection of data privacy: Human rights, democracy issues and judicial responses in USA, European Union and India*. Democracy Issues and Judicial Responses in USA, European Union and India.
3. Ajiji, Y. M. (2020). Internet of thing (IoT): data and information (gadget protection). *Journal of Applied Science, Engineering, Technology, and Education*, 2(2), 194-203. <http://dx.doi.org/10.35877/454RI.asci2253>.
4. Aljifri, H. A., Pons, A., & Collins, D. (2003). Global e-commerce: a framework for understanding and overcoming the trust barrier. *Information Management & Computer Security*, 11(3), 130-138. <https://doi.org/10.1108/09685220310480417>.
5. Austin, G. W. (1999). Domestic Laws and Foreign Rights: Choice of Law in Transnational Copyright Infringement Litigation. *The Columbia Journal of Law & the Arts*, 23(1).
6. Bali, V. (2007). Data privacy and data piracy: can India provide adequate protection for electronically transferred data. *Temple International & Comparative Law Journal*, 21(1), 103-146.
7. Barkatullah, A. H. (2018). Does self-regulation provide legal protection and Security to e-commerce consumers? *Electronic Commerce Research and Applications*, 30, 94-101. <https://doi.org/10.1016/j.elerap.2018.05.008>.
8. Bhachawat, K. (2021). Electronic Contracts in India: Challenges and Complexities. *International Journal of Law Management and Humanities*, 4(3), 3502-3513. <https://doi.org/10.10000/IJLMH.11894>.
9. Bressler, M. S., & Bressler, L. (2014). Protecting your company's intellectual property assets from cyber-espionage. *Journal of Legal, Ethical and Regulatory Issues*, 17(2). https://www.researchgate.net/publication/281034771_Protecting_your_company's_intellectual_property_assets_from_cyber-espionage.
10. Christensen, A. L., & Eining, M. M. (1991). Factors influencing software piracy: Implications for accountants. *Journal of Information systems*, 5(1).
11. Chudasama, D., & Patel, S. (2021). Importance of Intellectual Property Rights. *Journal of Intellectual Property Rights Law*, 4(2), 16-22. <http://doi.org/10.37591/JIPRL>.
12. Das, O. (2000). Cyber laws in india. *International Business Lawyer*, 28(7), 327-329.
13. Davis, B. G. (2000). The New New Thing: Uniform Domain-Name Dispute-Resolution Policy of the Internet Corporation for Assigned Names and Numbers. *The Journal of World Intellectual Property*, 3(4), 525-554.
14. Determann, L., & Gupta, C. (2019). India's personal data protection act, 2018: comparison with the general data protection regulation and the california consumer privacy act of 2018. *Berkeley Journal of International Law*, 37(3), 481-516. <https://doi.org/10.2139/ssrn.3244203>.
15. Dudin, M. N., Zasko, V. N., Frolova, E. E., Pavlova, N. G., & Rusakova, E. P. (2018). Mitigation of cyber risks in the field of electronic payments: organizational and legal measures. *Journal of Advanced Research in Law and Economics*, 9(1), 78-88.
16. Duraiswami, D. R. (2017). Privacy and Data Protection in India. *Journal of Law & Cyber Warfare*, 6(1), 166-186. <http://www.jstor.org/stable/26441284>.
17. Dwivedi, S. (2020). From Privacy to Data Protection in India: Evaluating the Personal Data Protection Bill, 2019. *International Journal of Law Management & Humanities*, 3, 2136-2152.
18. Finck, M., & Moscon, V. (2019). Copyright law on blockchains: between new forms of rights administration and digital rights management 2.0. *IIC-International Review of Intellectual Property and Competition Law*, 50, 77-108. <https://doi.org/10.1007/s40319-018-00776-8>.
19. Gholap, S. (2018). Electronic Contracts in India: An Overview. *International Journal of Research in Humanities, Arts and Literature*, 6(8), 251-260.

20. Halder, D., & Jaishankar, K. (2021). Cyber governance and data protection in India: A critical legal analysis. In *Routledge Companion to Global Cyber-Security Strategy* (pp. 337-348). Routledge.
21. Jain, I. B. (2023). The Significance of Intellectual Property Rights in Cyber Law. *European Economic Letters*, 13(1), 161-167. <https://doi.org/10.52783/eel.v13i1.134>.
22. Jain, M. (2019, May 9). *The Aadhaar card: Cybersecurity issues with India's biometric experiment*. The Henry M. Jackson School of International Studies. <https://jsis.washington.edu/news/the-aadhaar-card-cybersecurity-issues-with-indias-biometric-experiment/>.
23. Kethineni, S. (2020). Cybercrime in India: Laws, regulations, and enforcement mechanisms. In T. J. Holt, & A. M. Bossler (Eds), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 305-326). Palgrave Macmillan Cham. https://doi.org/10.1007/978-3-319-90307-1_7-1.
24. Kidd, D., & Daughtrey, W. (2000). Adapting contract law to accommodate electronic contracts: overview and suggestions. *Rutgers Computer & Technology Law Journal*, 26(2), 215-276.
25. Krishna, P. R., Karlapalem, K., & Chiu, D. K. (2004). An EREC framework for e-contract modeling, enactment and monitoring. *Data & Knowledge Engineering*, 51(1), 31-58.
26. Kumar, S. R., Yadav, S. A., Sharma, S., & Singh, A. (2016, February). *Recommendations for effective cyber security execution* [Conference presentation abstract]. International Conference on Innovation and Challenges in Cyber Security, Greater Noida, India.
27. Malik, J. K., & Choudhury, S. (2019). Privacy and surveillance: the law relating to cyber crimes in India. *Journal of Engineering, Computing and Architecture*, 9(12), 74-98.
28. Mejias, R. J., & Harvey, M. G. (2012). A case for information security awareness (ISA) programmes to protect global information, innovation and knowledge resources. *International Journal of Transitions and Innovation Systems*, 2(3-4), 302-324.
29. Nanda, A., Xu, Y., & Zhang, F. (2021). How would the COVID-19 pandemic reshape retail real estate and high streets through acceleration of E-commerce and digitalization? *Journal of Urban Management*, 10(2), 110-124. <https://doi.org/10.1016/j.jum.2021.04.001>.
30. Natarajan, M., & Makhdumi, G. (2009). Safeguarding the digital contents: Digital watermarking. *Journal of Library & Information Technology*, 29(3), 29-35. <http://doi.org/10.14429/djlit.29.249>.
31. Nguyen, X. T. (2001). Intellectual Property Financing: Security Interests in Domain Names and Web Contents. *Texas Wesleyan Law Review*, 8, 489-512.
32. Patil, S. (2022). India's Cyber Security Landscape. In *Varying Dimensions of India's National Security: Emerging Perspectives* (pp. 75-90). Springer Nature Singapore.
33. Popko, V., & Popko, Y. (2021). Theoretical and Legal Characteristics of Economic Crimes of a Transnational Nature. *Baltic Journal of Economic Studies*, 7(1), 93-101. <https://doi.org/10.30525/2256-0742/2021-7-1-93-101>.
34. Rattan, J. (2015). Law Relating To E-Commerce: International and National Scenario with Special Reference to India. *International Journal of Social Science and Economics Invention*, 1(2). <https://pdfs.semanticscholar.org/424a/8ffdc0de57f1f1be1c3a431652deff3fec094.pdf>.
35. Rizal, M., & Yani, Y. M. (2016). Cybersecurity policy and its implementation in Indonesia. *Journal of ASEAN Studies*, 4(1), 61-78.
36. Schwartz, A., & Scott, R. E. (2003). Contract theory and the limits of contract law. *Yale Law Journal*, 113(3), 541-620.
37. Shackelford, S. J. (2016). Protecting intellectual property and privacy in the digital age: the use of national cybersecurity strategies to mitigate cyber risk. *Chapman Law Review*, 19(2), 445-482.
38. Shanker, D. (2008, May 15-17). *ICT and Tourism: challenges and opportunities* [Conference presentation abstract]. Conference on Tourism in India, Kozhikode, India. <http://115.249.96.25/xmlui/bitstream/handle/2259/185/50-58.pdf?sequence=1&isAllowed=y>.
39. Singh, G., Gupta, R., & Vatsa, V. (2021, November 10-12). *A Framework for Enhancing Cyber Security in Fintech Applications in India* [Conference presentation abstract]. 2021 International Conference on Technological Advancements and Innovations, Tashkent, Uzbekistan.
40. Singh, O., Gupta, P., & Kumar, R. (2016). A Review of Indian Approach towards Cybersecurity. *International Journal of Current Engineering and Technology*, 6(2), 644-648.
41. Singh, S. S. (2011). Privacy and data protection in india: a critical assessment. *Journal of the Indian Law Institute*, 53(4), 663-677. <http://www.jstor.org/stable/45148583>.
42. Taher, G. (2021). E-commerce: advantages and limitations. *International Journal of Academic Research in Accounting Finance and Management Sciences*, 11(1), 153-165. <http://doi.org/10.6007/IJARAFMS/v11-i1/8987>.
43. Tanimoto, K. (2012). The emergent process of social innovation: multi-stakeholders perspective. *International Journal of Innovation and Regional Development*, 4(3-4), 267-280.
44. Tiwari, R. (2019). Contribution of Cyber Banking towards Digital India: A Way Forward. *Khoj: An International Peer Reviewed Journal of Geography*, 6(1), 46-52. <http://doi.org/10.5958/2455-6963.2019.00005.5>.
45. Vishwakarma, M. M. (2019). E-commerce: emerging trend for business management education. *Challenges and Opportunities in Social Sciences, Humanities and Business Management*, 114.

46. Wassom, B. D. (1998). Copyright implications of unconventional linking on the world wide web: Framing, deep linking and inlining. *Case Western Reserve Law Review*, 49, 181-193.

Received the editorial office: 2 June 2023

Accepted for publication: 25 June 2023

АМІТ КУМАР КАШ'ЯП,

*MBA, магістр права,
Університет Нірма, Ахмедабад (Індія),
Інститут права;
ORCID: <https://orcid.org/0000-0002-2716-8482>,
e-mail: amit1law@gmail.com;*

МАХІМА ЧАУДХАРІ,

*бакалавр комерції, бакалавр права, науковий співробітник,
Університет Нірма, Ахмедабад (Індія),
Інститут права,
Центр досліджень корпоративного права;
ORCID: <https://orcid.org/0009-0004-1864-1778>*

ЗАКОНИ ПРО КІБЕРБЕЗПЕКУ ТА БЕЗПЕКУ ЕЛЕКТРОННОЇ КОМЕРЦІЇ В ІНДІЇ

Сьогодні, в епоху інформаційних технологій, питання кібербезпеки є складною та цікавою галуззю права. Феноменальне зростання та розвиток електронної комерції в Індії вражає. Однак зі зростанням залежності від інтернет-торгівлі небезпека шахрайства та проблеми безпеки і довіри стали серйозними перешкодами. Створення надійної нормативно-правової бази, яка б відповідала зростанню занепокоєння щодо шахрайства в інтернеті, забезпечення безпеки даних і захисту інтелектуальної власності як у місцевому, так і в міжнародному бізнес-контексті мають вирішальне значення. Сектор електронної комерції, як і будь-який бізнес, що розвивається, стикається з різними перешкодами, насамперед через неадекватну та неефективну нормативно-правову базу, яка не гарантує достатнього рівня захисту прав та обов'язків усіх учасників ринку. Щоб захистити дані користувачів, протистояти кіберзагрозам і зберегти довіру клієнтів, підприємства електронної комерції повинні дотримуватися правових норм. В Індії управління кібербезпекою підпадає під дію Закону про інформаційні технології від 2000 року, який регулює електронну комерцію, електронні контракти, захист даних і кіберзлочини. Очікується, що найближчим часом, після доопрацювання, буде ухвалено законопроект про захист персональних даних 2019 року. Кримінальний кодекс Індії передбачає відповідальність за несанкціонований доступ, хакерство, крадіжку персональних даних, фішинг і розповсюдження комп'ютерних вірусів. Резервний банк Індії здійснює контроль за онлайн-платежами та фінансовою безпекою, вимагаючи двофакторної автентифікації, шифрування та захищених платіжних каналів. CERT-In координує інциденти кібербезпеки на національному рівні, а електронні підписи та цифрові сертифікати мають юридичне визнання. Закони про інтелектуальну власність регулюють порушення патентів, авторських прав і торгових марок в інтернеті. Уряд Індії також забезпечує дотримання стандартів кібербезпеки для підприємств та організацій, що охоплюють IT-інфраструктуру та реагування на інциденти. Тим не менш, необхідно вжити подальших заходів для підвищення ефективності індійського законодавства у сфері кібербезпеки. У цьому дослідженні використано доктринальний та аналітичний підходи для вивчення чинних законів і керівних принципів Індії у сфері кібербезпеки. Оцінено їх ефективність у вирішенні правових проблем, пов'язаних із безпекою, конфіденційністю і захистом даних всередині країни, а також правову структуру, яка регулює зв'язок між електронною комерцією та кіберзаконодавством в Індії. Дослідження надало ґрунтовний огляд поточного стану нормативно-правового регулювання кібербезпеки в Індії, прокладаючи шлях для майбутніх реформ і прогресу в цій критично важливій сфері.

Ключові слова: *право, безпека, кібербезпека, електронна комерція, захист даних, інформаційні технології.*

Цитування (ДСТУ 8302:2015): Kashyap A. K., Chaudhary M. Cyber security laws and safety in e-commerce in India. *Law and Safety*. 2023. No. 2 (89). Pp. 207–216. DOI: <https://doi.org/10.32631/pb.2023.2.19>.

Citation (APA): Kashyap, A. K., & Chaudhary, M. (2023). Cyber security laws and safety in e-commerce in India. *Law and Safety*, 2(89), 207–217. <https://doi.org/10.32631/pb.2023.2.19>.