LL.B PART II

INFORMATION TECHNOLOGY ACT AND CYBER LAWS

(PAPER CODE 302 B & 402 B)

1. INTRODUCTION

Cyber laws regulate the legal aspects of digital transactions, online security, information technology governance, and artificial intelligence applications. This course provides a comprehensive understanding of the Information Technology Act, 2000, addressing electronic commerce, cybersecurity, digital rights, cybercrime laws, and AI-related legal frameworks. Students will explore landmark case laws, international cyber and AI law frameworks, regulatory mechanisms, and the role of law enforcement agencies in cyberspace and AI governance.

2. COURSE OBJECTIVES

This course aims to:

1. Explain the scope and significance of the Information Technology Act, 2000, its amendments, and AI regulations.

2. Analyze cybercrime and AI-related offense classifications, digital evidence, and enforcement mechanisms.

3. Examine the legality of electronic transactions, contracts, intellectual property, and AI applications in cyberspace.

4. Study landmark case laws on cyber and AI regulations and consumer protection.

5. Understand global cyber and AI law frameworks and cross-border jurisdiction issues.

6. Evaluate contemporary challenges such as AI governance, blockchain regulation, data protection, and ethical AI use.

3. COURSE OUTCOMES

Upon successful completion, students will be able to:

1. Define and explain the legal framework of cyber laws and AI regulations in India.

2. Differentiate between civil and criminal cyber and AI-related offenses under the IT Act.

3. Analyze key landmark cases in cyber and AI law jurisprudence.

4. Demonstrate understanding of electronic commerce regulations, digital contract law, and AI-driven transactions.

5. Evaluate data protection mechanisms, cybersecurity policies, and AI ethical frameworks.

4. COURSE STRUCTURE & RECOMMENDED READINGS

SEMESTER-III

(PAPER CODE: 302 B)

Full Marks: 50

(Theory Paper – 40 Marks, Internal Assessment – 10 Marks)

4 Credits [3 Lecture hours+1 Tutorials per week]

Required Lecture Hours: 48 Hours

PART A: CYBER LAW AND AI FRAMEWORK

I. Nature and Evolution of Cyber Law and AI Regulation (5 Marks)

· Definition, scope, and relevance of Cyber Law and AI Regulation

· Development of Information Technology and AI Laws in India

· International perspectives on Cyber Law and AI Governance

Landmark Case Laws:

· Shreya Singhal v. Union of India (2015) – Right to Free Speech Online

· Avnish Bajaj v. State (Delhi High Court, 2008) – Cybercrime Liability

Recommended Readings:

1. Sharma, Vakul. Cyber Law and Information Technology, 4th ed., LexisNexis, 2019.

2. Wachter, Sandra. Artificial Intelligence and the Law, Cambridge University Press, 2023.

II. Information Technology Act, 2000 and Amendments (5 Marks)

· Objectives and key provisions of the IT Act, 2000

· Recognition of electronic records, digital signatures, and AI-generated data

· Amendment of 2008: Cybercrime definitions, AI-related offenses, and increased penalties

Landmark Case Laws:

· Syed Asifuddin & Ors v. State of Andhra Pradesh (2005) – Cybercrime conviction

· Google India Pvt Ltd v. Visakha Industries (2014) – Intermediary Liability

Recommended Readings:

1. Duggal, Pavan. Cyber Law in India, 2nd ed., Saakshar Law Publications, 2020.

2. Kamath, Nandan. Law Relating to Computers, Internet, and E-Commerce, Universal Law Publishing, 2017.

III. Cyber Crimes, AI-Related Offenses, and Digital Evidence (5 Marks)

· Classification of Cyber Crimes and AI-Related Offenses – Data theft, hacking, identity fraud, AI misuse

· Investigation and prosecution of cyber and AI-driven offenses

· Role of CERT-In (Computer Emergency Response Team – India) and AI regulatory bodies

Landmark Case Laws:

· Tamil Nadu v. Suhas Katti (Cyberstalking, 2004)

· Infosys BPO Data Theft Case (2018)

Recommended Readings:

1. Bansal, Vikas. Cyber Crimes and Digital Evidence, Bloomsbury, 2021.

2. Halder, Debarati. Artificial Intelligence and Cybercrime, Routledge, 2024.

SEMESTER-IV

(PAPER CODE: 402 B)

Full Marks: 50

(Theory Paper – 40 Marks, Internal Assessment – 10 Marks)

4 Credits [3 Lecture hours+1 Tutorials per week]

Required Lecture Hours: 48 Hours

PART A: E-COMMERCE, DATA PROTECTION, AND AI GOVERNANCE (25 Marks)

I. Legal Framework for E-Commerce and AI-Driven Transactions (5 Marks)

· Recognition of electronic and AI-generated contracts

· Consumer Protection under the IT Act for AI-driven services

· Jurisdictional issues in online and AI-related fraud

Landmark Case Laws:

· eBay Inc v. Newmark (Cyber Marketplace Disputes)

Recommended Readings:

1. Saxena, Rishi. E-Commerce Laws and Consumer Protection, Eastern Book Company, 2020.

II. Data Protection, Privacy Laws, and AI Ethics (5 Marks)

· Personal Data Protection Bill, 2019 and AI data governance

· GDPR, International Data Privacy, and AI Ethical Regulations

· Case studies on Facebook-Cambridge Analytica, Aadhaar Data Protection, and AI bias

Landmark Case Laws:

· Justice K.S. Puttaswamy v. Union of India (2017) – Right to Privacy

Recommended Readings:

1. Warren, Samuel. Privacy and Technology Law, Oxford University Press, 2020.

2. Floridi, Luciano. The Ethics of Artificial Intelligence, Oxford University Press, 2021.

III. Emerging Challenges in Cyber Law and AI Regulation (5 Marks)

· AI governance, ethical AI frameworks, and blockchain regulations

· Cyber Warfare, AI-driven threats, and International Cooperation

· Social Media Laws, Fake News, and AI-generated misinformation

Landmark Case Laws:

· TikTok Ban Case (India, 2020)

Recommended Readings:

1. Goodman, Marc. Future Crimes: Cyber Threats & Legal Responses, Penguin, 2019.

2. Cath, Corinne. Governing Artificial Intelligence: Ethical, Legal, and Technical Challenges, MIT Press, 2023.

****