

POST-GRADUATE DIPLOMA IN CYBER LAW & DATA PROTECTION (PGDCLDP)

(SESSION 2025-26 ONWARDS)

**General Rules, Examination, Regulation and
Course**



**Chotanagpur Law College, Ranchi,
Jharkhand**

PG Diploma in Cyber Law and Data Protection

About the Programme:

In an era dominated by digital technology, the intersection of law, cyberspace, and artificial intelligence (AI) has become more critical than ever. The increasing reliance on the internet, intelligent systems, and electronic communication has given rise to complex legal challenges concerning cybersecurity, data breaches, AI-driven decision-making, digital transactions, and online privacy. As cybercrimes and algorithmic surveillance become more sophisticated and frequent, the demand for legal professionals equipped with advanced understanding of both Cyber Law and AI governance is steadily rising.

The Post Graduate Diploma in Cyber Law and Data Protection, offered by Chotanagpur Law College, Ranchi, is a comprehensive and forward-looking academic programme designed to meet these emerging technological and regulatory challenges. This diploma aims to empower students, legal practitioners, IT professionals, AI developers, law enforcement personnel, and policymakers with in-depth knowledge of the legal and policy framework governing cyberspace, data protection, and artificial intelligence.

The programme covers a wide range of subjects including the Information Technology Act, cybercrimes and offences, digital privacy laws, international data protection regulations, cyber forensics, and the legal implications of AI and emerging technologies. Special focus is laid on understanding how AI affects data governance, surveillance practices, algorithmic accountability, and individual rights in a digital society.

The curriculum emphasizes practical learning through real-life case studies, legal drafting exercises, AI and data compliance simulations, and hands-on training in digital evidence handling. The course structure ensures a balanced integration of theoretical concepts, evolving jurisprudence, and applied legal technology, making learners industry-ready and future-proof in an increasingly AI-powered world.

Duration: 1 Year (The program will consist of two semesters comprising six modules with Project, Dissertation or Internship.)

Mode: Online / Offline / Hybrid

Eligibility: Graduation in Law / IT / Management / Equivalent

Objectives:

1. To provide a comprehensive understanding of cyber law and its application.
2. To educate learners about Indian and international data protection regimes.
3. To train students in cybercrime investigation and cyber forensics.
4. To enhance the legal and technical skills of students, professionals, and law enforcement personnel.

Assessment of Students' Performance and Scheme of Examination Pass Percentage & Promotional Criteria:

1. Assessment of student's performance shall consist of 70 marks (End Semester Written Examination) and 30 marks (Internal Assessment).
2. The duration of the End Semester Written Examination shall be three hours for 70 marks.
3. For internal assessment of 30 marks, one Internal Test + Assignment + Presentation + Viva shall be in each course in each semester.
4. Internal assessment of each paper shall be evaluated by a panel of three teachers of the department. For each paper panel is to be formed by Principal accordingly.
5. Dissertation / Project/ Internship will carry 70 marks.
6. Viva-voce exam will carry 30 marks Viva-voce shall be held soon after the Second semester.
7. In each paper 30 marks shall be reserved for award on the bases of continuous internal assessment of the student in the class room. The HOD will notify information regarding each internal assessment at least one week prior of the presentation with consultation to the teacher concern. All awards of marks will be verified by the HOD and will be send to exam controller accordingly.
8. The criteria for Internal assessment for each paper will be as follows – Internal Test- 10 marks
9. Assignment with presentation – 10 marks Class room seminar and viva – 10 marks

Attendance

The student whose attendance is less than 75% will not be allowed to appear in the end semester examination. Principal may permit a student to appear in examination by relaxation of 25% attendance in special conditions such as;

- Participation in NCC/NSS camps duly supported by a certificate from competent authority.
- Participation in College Team (S) Games or Inter State Tournament (S) duly supported a certificate from competent authority.
- Participation in any of the co-curricular activity organized by College duly certified by competent authority.
- Prolonged illness duly certified by superintendent/CMO of government hospital or registered medical practitioners/hospitals.

Note: The Principal shall have power to condone any deficiency of attendance for cogent reasons.

End Semester Examination

There shall be an end semester examination at the end of the I and II semesters. The semester examination will be held every year normally in December and May or on the dates declared in the academic calendar of the College. A student proceeding to appear in the end semester

examination will submit through the Head of the Department his/her application on the prescribed form along with the required examination fee, etc. to the Registrar of the College.

Every student will have to appear in three & two respective theory papers examinations in the I and II, semesters.

In the II semester, every student will be allotted one dissertation work in lieu of Viva-voce Exam.

Allotment of The Dissertation

Allotment of the dissertation will be done by a committee comprising of the Head of the Department. The Proposal for dissertation shall be submitted by candidate through head of department.

Candidate shall be required to submit the Dissertation at least two weeks before the commencement of Second Semester Examination. Prior of submission of dissertation the students shall make a pre-submission seminar in the College. Seminar shall be opened to all faculty members, research scholar and other students of the College.

The candidate shall be required to secure at least 50% marks in the Dissertation to pass the Examination.

The maximum number of students enrolled for dissertation under one teacher will be as follows-
Assistant Professor – 05

Associate Professor – 08

Professor – 10

Full time teacher of the College is authorized for dissertation guidance. If there is non-availability of full time teachers in the College, rest of all student will be supervised by HOD/ principal accordingly.

Viva-Voce Examination:

The Viva Voce Examination shall be conducted by a Board of Examiners.

The Board shall consist of three members; one member shall be a Professor/Associate Professor as external member of any other university or college. The head of the department (H.O.D.) shall be a member of the board and one Professor/Associate professor of the college as internal examiner. The internal examiner shall be appointed for every year by rotation.

The Viva-Voce Examination shall carry 30 marks. The external examiner shall evaluate the candidate out of 20 maximum marks and two examiners shall evaluate out of 10 maximum marks each.

Candidate shall be required to secure at least 50% marks in the Viva-voce to pass the Examination.

Grad Point and SGPA, CGPA Calculations:

Assessment as per college policy relating to implementation of choice-based credit system (CBCS) to all the programs offered at Chotanagpur College.

Rules of Promotion:

A student can not to be promoted to next semester if he/she fails in up to the maximum two courses (papers) in first semester. The paper/papers in which a student fail shall be considered as back paper. In no case a student having back in more than two papers can be promoted to next semester and will be treated to have year back. In case of year back, he/she have to take readmission by paying approved fee in same year after the recommendation of Principal/HOD. After readmission students have following options;

1. He/ She can choose to pass all the papers of the academic year.
2. He/ She can opt to pass the papers in which he/she has failed.
3. Students will have to submit their choices/options at the time of readmission.
4. No repeat attempt is allowed to pass for internal assessment only.
5. He/ She has to repeat complete course i.e. theory and internal assessment both.

Course Modules:

The course is structured into two semesters, covering core concepts and applied aspects of cyber law and data protection.

Programme Learning Outcomes (PLOs):

Upon completion of the PG Diploma in Cyber Law and Data Protection, learners will be able to:

1. Demonstrate a sound understanding of cyber law principles and legal frameworks.
2. Analyze and interpret legal provisions related to IT Act, data protection laws, and cyber offences.
3. Apply cyber forensic methods and tools in real-world scenarios.
4. Advise institutions on data compliance and digital privacy measures.
5. Exhibit legal drafting, investigation, and research skills related to cyber jurisprudence.

Course Learning Outcomes (CLOs):**Semester I:**

- Understand the origin, scope, and importance of cyber law.
- Explain the key provisions of the Information Technology Act, 2000.
- Identify and categorize different types of cybercrimes.
- Evaluate the legal challenges in cyber jurisdiction and intermediary liability.

Semester II:

- Analyze data protection frameworks including Indian and international laws.
- Apply legal principles in solving privacy-related issues.
- Develop expertise in collecting and preserving digital evidence.
- Understand intellectual property rights in the online domain.
- Conduct legal research and prepare cyber investigation case reports.

Semester I: Foundations of Cyber Law and Regulation

S.No.	Course Code	Course Name	L-IA-P	Total Credit
1.	PGDCLDP 101	Introduction and International Comparison of Cyber Law and Legal Framework	5-2-0	7
2.	PGDCLDP 102	Information Technology Act, 2000 (with Amendments) & Cyber Crimes or Offences	5-2-0	7
3.	PGDCLDP 103	Digital Surveillance, Encryption, Cyber Ethics, Policy And Regulatory Authorities	5-2-0	7
Total Credit in Semester I				21

Semester II: Data Protection, Privacy, and AI

S.No.	Course Code	Course Name	L-IA-P	Total Credit
1.	PGDCLDP 201	Data Protection & Privacy Laws and Intellectual Property Rights In The Digital Space	5-2-0	7
3.	PGDCLDP 202	AI with Emerging Tech in Cyber Law & AI with Data Governance in a Digital World	5-2-0	7
4.	PGDCLDP 203	Project / Dissertation / Internship & Viva	5-2-0	7
Total Credit in Semester II				21
The PG Diploma programme comprises a total of six papers, three papers in Semester I and three papers in Semester II. Each paper carries 7 credits, making the total credit requirement for the programme 42 credits.				

Semester I

Paper I- PGDCLDP 101

INTRODUCTION TO CYBER LAW AND LEGAL FRAMEWORK

Duration: 40 hours (including lectures, seminars, and assessments)

Credits: 7

Introduction:

In the era of digital transformation, legal professionals must be well-versed in the evolving dimensions of cyberspace. This paper introduces the foundational aspects of Cyber Law, the regulatory framework governing cyberspace, and emerging legal issues such as jurisdiction, liability, and digital evidence. It provides students with a thorough understanding of the Information Technology Act, legal recognition of electronic records, and the challenges posed by cybercrimes.

Course Outcomes (C.O.):

1. To understand the origin, scope, and relevance of cyber law in the digital age.
2. To comprehend the key provisions and legal implications under the Information Technology Act, 2000.
3. To analyze cybercrime typologies and legal mechanisms for redressal.
4. To apply cyber law principles to case studies involving digital transactions, evidence, and liabilities.

Program Outcomes:

1. To equip students with legal tools for understanding and handling cyber law issues.
2. To develop practical understanding of statutory compliance and legal responsibility in online platforms.
3. To build awareness about legal frameworks for electronic governance, contracts, and offenses.
4. To prepare learners for careers in cyber regulation, consulting, and policy development.

Syllabus:

Unit I: Evolution of Cyber Law and Jurisprudence

- Growth of the Internet and its legal implications
- Historical development of cyber law across jurisdictions
- Cyber jurisprudence: nature, scope, and challenges
- Emergence of digital societies and the need for regulation
- Cyberspace as a legal construct
- Theories of jurisdiction: territorial, effects-based, and universal
- Contractual and tortious liabilities in cyberspace
- Role of intermediaries and their legal responsibilities

Suggested Readings:

Books:

- Kumar, S. – *Cyber Law: Emerging Trends* (Universal Law Publishing), 2023.
- Terry J. Ilardi – *Cyber Law and Jurisprudence: A Comparative Perspective*, Thomson Reuter, 2015.
- Solove, Daniel J. – *The Digital Person: Technology and Privacy in the Information Age*, New York University Press (2004).

Articles:

- Jack L. Goldsmith, “*Jurisdiction in Cyberspace: A Theory of Reasonableness*”, Yale Law Journal, 105(5), 1058–1132, (1996).
- David R. Johnson and David G. Post, “*The Role of Law in Governing the Internet*”, Stanford Law Review, 48, 1367–1402, (1996).

Case Laws:

- Yahoo! Inc. v. La Ligue Contre Le Racisme et l’Antisémitisme, 169 F. Supp. 2d 1181 (2001)
- Reno v. ACLU, 521 U.S. 844 (1997)
- Shreya Singhal v. Union of India, AIR 2015 SC 1523 – Section 66A struck down

Unit II: Indian Legal Context and Framework to understanding Cyberspace and its Challenges

- Unique features of cyberspace (borderless, anonymous, decentralized)
- Attribution, traceability, and identification in cyber incidents
- Enforcement challenges in digital crimes
- Cyber governance and multi-stakeholder models: ICANN, IGF, ITU
- Constitutional rights in the digital age:
 - a. Article 19(1)(a): Freedom of speech
 - b. Article 21: Right to privacy
- Overview of the IT Act, 2000 and its relevance
- Role of Indian judiciary in shaping cyber jurisprudence
- Related legislations: Bharatiya Nyaya Sanhita, 2023, Bharatiya Sakshya Adhiniyam, 2023, Data Protection Bill

Suggested Readings:**Books:**

- Sharma, Vakul, Information Technology Law and Practice 6th ed., Universal Law Publishing, 2022.
- Gupta, Apar, Internet Law and Policy in India: Cases and Materials, LexisNexis, 2014.

Articles:

- Eichensehr, K. E., “Challenges in Attribution of Cyber Attacks”, UCLA Law Review, 67(3), 520–600, 2020.
- Tripathi, H., “Constitutional Rights in the Digital Age”, NUJS Law Review 2024.

Case Laws:

- Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 — landmark judgment affirming Right to Privacy as a fundamental right

- Avnish Bajaj v. State (NCT of Delhi), 150 (2008) DLT 769 — early Indian case on intermediary liability under IT Act
- Google India Pvt. Ltd. v. Visakha Industries, AIR 2020 SC 510 — clarified safe harbor under Section 79 of the IT Act

Unit III: International Legal Instruments and Models

- Budapest Convention on Cybercrime
- OECD Guidelines on the Protection of Privacy
- WTO principles and e-commerce
- Regional legal frameworks:
 - a. EU's GDPR
 - b. US Cybersecurity Framework
 - c. China's Cybersecurity Law
- Role of United Nations in digital norms and security
- Legal responses to AI, Blockchain, and the Metaverse
- Data localization and digital sovereignty
- Role of ethics and digital constitutionalism
- Challenges in regulating decentralized technologies
- Future of cyber governance and cyber peace

Suggested Readings:

Books:

- Schmitt, Michael, Tallinn Manual on the International Law Applicable to Cyber Warfare, 2.0 (Cambridge Univ. Press) 2017.

Articles / Reports

- “The Budapest Convention and Its Global Reach”, Journal of International Cybersecurity Law 2021; <https://www.coe.int/en/web/cybercrime/the-budapest-convention>
- OECD Privacy Guidelines, foundational standards for cross-border flow of personal data, 2013; https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

Unit VI: Unit I: Introduction to Comparative Cyber Law

- Nature and Scope of Comparative Cyber Law
- Need for International Cooperation in Cyber Law
- Methodologies for Comparing Legal Systems
- International Jurisdiction Issues in Cyber Law
- Overview of Internet Governance and Global Actors (ICANN, ITU, IGF)
- Cybercrime Definitions: A Comparative Study
- Comparative Review of National Cybercrime Laws:
 - a. USA (Computer Fraud and Abuse Act)
 - b. EU (Cybercrime Directive)
 - c. India (IT Act, 2000)
 - d. China (Cyber security Law)
- Investigation and Admissibility of Electronic Evidence: A Comparative Perspective
- Cross-Border Cybercrime and Mutual Legal Assistance Treaties (MLATs)

- Role of Interpol and Europol in Cybercrime Prevention

Suggested Readings:

Books:

- Brenner, Susan W., *Cybercrime and the Law: Challenges, Issues, and Outcomes*, Northeastern University Press / Wiley 2012; <https://www.upne.com/1555537933.html>
- Greenleaf, Graham, *Global Data Privacy Laws: 89 National Jurisdictions, 2019 Update* (Oxford Univ. Press); https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3381593

Articles:

- Orla Lynskey, “Comparative Approaches to Data Protection Law”, *Oxford Journal of Legal Studies* vol. 34, no. 2, 2014, pp. 256–282. <https://academic.oup.com/ojls/article/34/2/256/1500844>
- Jack L. Goldsmith, “International Jurisdiction and Cyberspace”, *Duke Law Journal* vol. 65, no. 3, 1998, pp. 477–505.

Cases:

- *U.S. v. Ivanov*, 175 F. Supp. 2d 367 (2001) — cross-border hacking liability
- *Google Spain v. AEPD & Mario Costeja González*, Case C-131/12 (2014) — EU Right-to-be-forgotten case

Unit V: International Legal Instruments on Cyber Law

- Budapest Convention on Cybercrime
- OECD Guidelines on the Protection of Privacy
- Tallinn Manual on International Law Applicable to Cyber Warfare
- UN Resolutions on Cyber security and ICTs
- Role of WTO and WIPO in Digital Trade and IPR
- Cyber Sovereignty vs. Internet Freedom
- Digital Borders and Surveillance Laws
- Artificial Intelligence, Quantum Computing, and Legal Gaps
- Cryptocurrency Regulation and Cross-border Financial Crimes
- Towards a Global Treaty on Cyberspace: Possibilities and Pitfalls

Suggested Readings:

Books:

- Lucian Nehauser, *International Cyber Law: A Practical Framework* (Routledge, 2016)

Articles / Reports:

- WTO E-Commerce Work Programme—analyses on digital trade laws
- Chatham House Report on Digital Sovereignty vs. Internet Freedom

Recommendations:

1. Pavan Duggal, *Cyber Law: The Indian Perspective*, 3rd Edition (LexisNexis / Universal Law Publishing, 2023)
2. Talat Fatima, *Cyber Crimes*, 3rd Edition (Eastern Book Company, 2021)
3. Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2010)

4. Susan W. Brenner, *Cybercrime and the Law: Challenges, Issues, and Outcomes* (Wiley, 2010)
5. UNODC – Manual on Cybercrime Investigation and Cyber Law; <https://www.unodc.org/e4j/en/tertiary/cybercrime.html>; https://www.unodc.org/documents/organized-crime/tools_and_publications/Digest_of_Cyber_Organized_Crime_2nd_edition_English.pdf
6. Budapest Convention on Cybercrime (Council of Europe, 2001); <https://www.coe.int/en/web/cybercrime/the-budapest-convention>
7. General Data Protection Regulation (GDPR), Regulation (EU) 2016/679; <https://gdpr-info.eu>; <https://gdpr.eu>
8. Digital Personal Data Protection Act, 2023 (Government of India); <https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf>; https://en.wikipedia.org/wiki/Digital_Personal_Data_Protection_Act,_2023
9. Tallinn Manual 2.0 on International Law Applicable to Cyber Operations; <https://ccdcoe.org/research/tallinn-manual>; <https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/foreword/F4671348E3478C643AEB9E940044B937>
10. WTO and WIPO Resources on Digital Trade and IP; https://www.wto.org/english/tratop_e/trips_e/intel6_e.htm; https://www.wipo.int/global_health/en/trilateral_cooperation.html
11. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data; <https://legalinstruments.oecd.org/public/doc/114/114.en.pdf>; <https://www.oecd.org/sti/ieconomy/privacy.htm>
12. UN Cybersecurity Norms – UN GGE / OEWG Report; <https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf>; <https://digitallibrary.un.org/record/799853>
13. ICANN and ITU – Internet Governance Resource; <https://www.icann.org/en/policy>; <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx>
14. K.D. Gaur's *Criminal Law (adapted for BNS 2023)* Universal Law Publishing
15. Ratanlal & Dhirajlal's *The Indian Penal Code (Adapted to BNS 2023)* LexisNexis
16. *Information Technology Act, 2000*
17. Batuk Lal's *The Law of Evidence (Adapted to BSA 2023)* Central Law Agency

Evaluation Scheme:

- Internal Assessment (30 Marks):
2 written assignments (10 marks), 1 presentation (10 marks) and Class participation/seminar (10 marks)
- End Semester Examination (70 Marks):
Section A: Short answer questions (30 marks)
Section B: Analytical/Essay-type questions (40 marks)

Paper II- PGDCLDP 102

INFORMATION TECHNOLOGY ACT, 2000 (WITH AMENDMENTS) & CYBER CRIMES AND OFFENCES

Duration: 40 hours (including lectures, seminars, and assessments)

Credits: 7

Introduction:

The Information Technology Act, 2000 is the cornerstone of India's cyber law regime. Enacted to provide legal recognition to electronic commerce and to prevent cybercrime, the Act has evolved through amendments to address the rapid growth of digital technologies. This paper aims to provide a comprehensive understanding of the IT Act's provisions, its enforcement mechanisms, and its intersection with data protection, electronic governance, cybercrime, and digital evidence.

Course Outcomes (C.O.):

1. To understand the legislative intent, structure, and scope of the IT Act, 2000.
2. To analyze the statutory provisions regarding electronic records, signatures, contracts, and governance.
3. To interpret legal protections against cybercrime under the Act and its amendments.
4. To apply the IT Act in practical scenarios involving corporate, civil, and criminal liability in cyberspace.

Program Outcomes:

1. To develop the ability to analyze the structure and legal effect of the IT Act and related rules.
2. To enable understanding of compliance requirements for electronic governance and cyber regulations.
3. To evaluate the liability and responsibilities of intermediaries, companies, and government authorities under the IT Act.
4. To prepare for careers in law, compliance, policy, and digital regulation through strong conceptual grounding.

Syllabus:

Unit I: Structure and Electronic Governance of the IT Act

- Genesis and Need for the IT Act
- Legislative Framework and Definitions under the Act
- Applicability and Non-applicability of the Act
- Amendments to the IT Act: 2008 and post-2011 Developments
- The Digital Personal Data Protection Act, 2023 – Key Points of Convergence
- Legal Recognition of Electronic Records and Digital Signatures
- E-Governance: Legal Provisions, Validity of E-Contracts, Filing and Retention of Electronic Records

- Attribution, Acknowledgment, and Dispatch of Electronic Records
- Secure Digital Signatures and Legal Presumptions
- Case Studies on E-Governance Implementation in India

Suggested Readings:**Books:**

- Pavan Duggal, *Cyber Law: The Indian Perspective*, Saakshar Law Publications, (6th ed. 2023)
- Justice Yatindra Singh, *Cyber Laws*, Universal Law Publishing, (5th ed. 2012)

Articles:

- Anirudh Rastogi, "Legal Recognition of Digital Signatures in India," *NUJS Law Review*, Vol. 2, Issue 3 (2009), pp. 495–510.
- R. Ramakumar, "E-Governance and the Indian Legal Framework," *Economic and Political Weekly*, Vol. 42, No. 50 (Dec. 15-21, 2007), pp. 91–97.

Case Laws:

- *State of Maharashtra v. Dr. Praful B. Desai*, AIR 2003 SC 2053
- *Karnataka High Court v. Ashok Kini*, 2012 SCC OnLine Kar 2678

Unit II: Certifying Authorities , Cyber Regulations , Amendments, Allied Laws and Landmark Cases

- Establishment, Functions, and Duties of the Controller
- Regulation of Certifying Authorities (CAs)
- Licensing Process and Digital Signature Certificates
- Cyber Appellate Tribunal: Powers, Jurisdiction, and Functions
- Role of the Indian Computer Emergency Response Team (CERT-IN)
- IT Amendment Act, 2008 – Overview and Impact
- Relevant Provisions from *Bharatiya Nyaya Sanhita*, 2023, *Bharatiya Nagarik Suraksha Sanhita*, 2023, and *Bharatiya Sakshya Adhiniyam*, 2023
- *Shreya Singhal v. Union of India and the Striking Down of Section 66A*
- Jurisdictional and Procedural Challenges in Enforcement
- Interface of IT Act with Data Protection and Privacy Laws

Suggested Readings:**Books:**

- Rodney D. Ryder, *Guide to Cyber Laws* (, Wadhwa & Co.)4th ed. 2011.

Articles:

- Indian Constitutional Law Review. Section 66A and freedom of speech: *Shreya Singhal v. Union of India*. *Indian Constitutional Law Review*, 1, 55–65, (2016).
- NALSAR Tech Law Forum. (2018, April). Regulation of certifying authorities in India. Retrieved from <https://techlawforum.nalsar.ac.in>

Case Laws:

- *Shreya Singhal v. Union of India*, (2015) 5 SCC 1
- *Avnish Bajaj v. State (NCT of Delhi)*, 116 (2005) DLT 427

Unit III: Introduction to Cyber Crimes

- Relevant Sections of the IT Act (Sections 43–66, 66F, 67–72)
- Bharatiya Nyaya Sanhita (BNS), 2023 Provisions Related to Cybercrime (e.g., Sections 303, 318, 336–339, 340–341)
- International Legal Instruments: Budapest Convention, Tallinn Manual
- Cyber Law Enforcement Agencies in India: Cyber Crime Police Stations, CBI, CERT-IN
- Cyber Crime Cells: Functions and Case Filing Procedure

Suggested Readings:

Books:

- Susan W. Brenner, *Cybercrime and the Law: Challenges, Issues and Outcomes* (Northeastern Univ. Press 2012).

Articles:

- Centre for Communication Governance, *Emerging Cybercrime Trends in India*, CCG Blog (May 2021), <https://ccgdelhi.org>.
- (2020). *Budapest Convention: Global standard for cybercrime legislation*. *Journal of Cyber Policy*, 5(1), 45–59. <https://doi.org/10.1080/23738871.2020.1737356>

Case Laws:

- *Ritu Kohli v. Unknown*, Delhi, 2001 (First cyberstalking case in India)

Unit IV: Offenses, Penalties and Adjudication Mechanisms

- Computer-Related Offenses and Punishments (Section 43–45, 66–75 of IT Act)
- Hacking, Data Theft, Cyberterrorism, Phishing, Spoofing, Identity Theft
- Corporate Responsibility and Intermediary Liability (Section 79 of IT Act)
- Adjudication Process, Powers of Adjudicating Officers
- Compensation and Penalty Mechanisms under the Act
- Financial Frauds: Online Banking, Credit Card, Cryptocurrency Fraud
- Cyber Terrorism and National Security Offences
- Child Pornography, Cyberstalking, and Harassment
- Deepfakes, Revenge Porn, and Gender-Based Cyber Violence

Suggested Readings:

Books:

- Kerr, O. S., *Computer crime law* West Academic Publishing, 4th ed., (2017).

Articles:

- *Adjudication and Compensation under the IT Act*, *Indian Bar Review*, 41, 65–80 (2014).
- Internet Democracy Project, *Intermediary Liability in India: Section 79 of the IT Act*, (2012), <https://internetdemocracy.in>.

Case Laws:

- *Google India Pvt. Ltd. v. Visaka Industries*, (2011) 6 ALD 578 (AP HC).
- *Myspace Inc. v. Super Cassettes Industries Ltd.*, (2011) 48 PTC 49 (Del. HC).

Unit V: Investigation, Evidence, Forensics and Case Studies

- Reporting and FIR Registration in Cyber Cases
- Search, Seizure and Jurisdiction Issues in Cyber Investigations
- Collection and Preservation of Digital Evidence
- Role of Cyber Forensics and Expert Testimony
- Corporate Cybercrime and Insider Threats
- Cross-border Cybercrime and Extradition Challenges
- Legal Challenges in Metaverse, AI, and Virtual Reality Crimes
- Role of Media, Ethics, and Public Awareness in Cybercrime Prevention
- Admissibility of Electronic Evidence under Bharatiya Sakshya Adhiniyam, 2023
- Landmark Indian Case: Shreya Singhal v. Union of India, Avnish Bajaj (Bazee.com)

Suggested Readings:

Books:

- K.S. Park, *Legal Framework of Cybersecurity* (Springer 2014).
- Nandan Kamath, *Law Relating to Computers, Internet & E-Commerce*, Universal Law Publishing (5th ed. 2012).

Articles:

- Apar Gupta, Digital evidence and legal admissibility in India. *Indian Journal of Law and Technology*, 9, 1–15, (2013).

Case Laws:

- Shreya Singhal v. Union of India, (2015) 5 Supreme Court Cases 1.
- State v. Mohd. Afzal Guru and Others – (Parliament Attack Case) 107 Delhi Law Times 385.

Recommendations:

1. Bare Act: The Information Technology Act, 2000 (as amended)
2. Karnika Seth, *Computers, Internet and New Technology Laws* (2nd ed. 2013).
3. Justice Yatindra Singh, *Cyber Laws*, Universal Law Publishing. (5th ed. 2012).
4. *Bharatiya Nyaya Sanhita*, 2023 (With Comparative Table of IPC, 1860)" Universal Law Publishing / LexisNexis (Sections relevant to cybercrime)
5. Avtar Singh, *Law of Evidence (Adapted for BSA 2023)* Central Law Publications.
6. Government Reports and Guidelines (CERT-IN, MeitY Guidelines on Intermediary Rules); <https://www.cert-in.org.in>; <https://www.meity.gov.in>
7. Criminal Procedure (BNSS 2023 Updated)" Prof. N.V. Paranjape (Central Law Publications)
8. *Information Technology Act*, 2000
9. *Digital Personal Data Protection Act*, 2023
10. *General Data Protection Regulation (GDPR)*, EU <https://eur-lex.europa.eu>
11. *California Consumer Privacy Act (CCPA)* <https://oag.ca.gov/privacy/ccpa>
12. Agarwal, R., *Data Privacy and Protection in India*, Bloomsbury (2021).
13. Paul Lambert, *Understanding the New EU Data Protection Rules*, Routledge (2015).
14. Graham Greenleaf, *Global Data Privacy Laws*, Oxford University Press (2014).

15. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data;
<https://www.oecd.org/sti/ieconomy/privacy.htm>
16. Justice B.N. Srikrishna, Report of the Committee of Experts on Data Protection Framework for India (2018).; <https://www.meity.gov.in/data-protection-framework>
17. Reports and Publications of Internet Freedom Foundation (IFF) and CIS India. IFF: <https://internetfreedom.in>; CIS India: <https://cis-india.org>

Evaluation Scheme:

- Internal Assessment (30 Marks):
2 written assignments (10 marks), 1 presentation (10 marks) and Class participation/ seminar (10 marks)
- End Semester Examination (70 Marks):
Section A: Short answer questions (30 marks)
Section B: Analytical/Essay-type questions (40 marks)

Paper III-PGDCLDP 103

DIGITAL SURVEILLANCE, ENCRYPTION, CYBER ETHICS, POLICY AND REGULATORY AUTHORITIES

Duration: 40 hours (including lectures, seminars, and assessments)

Credits: 5

Introduction:

As the digital world expands, the lines between personal privacy and national security continue to blur. Governments increasingly rely on digital surveillance and interception tools to tackle crime, terrorism, and cyber threats, while civil society raises concerns about overreach and abuse. This paper explores the legal, ethical, and technological dimensions of surveillance practices, the role of encryption in digital privacy and security, and the balance of rights in democratic societies. It also examines global best practices, comparative frameworks, and constitutional safeguards related to state surveillance and data interception.

Course Outcomes (C.O.):

1. To understand the evolution and scope of digital surveillance in national and international contexts.
2. To examine the legal mechanisms governing surveillance, interception, and encryption in India.
3. To evaluate the balance between individual rights and national security in the context of surveillance laws.
4. To analyze emerging legal and policy challenges arising from encryption technologies, surveillance capitalism, and state control.

Program Outcomes:

1. To impart critical legal insight into the digital surveillance ecosystem.
2. To understand encryption as a legal and technological safeguard.
3. To explore constitutional dimensions of privacy, liberty, and state power.
4. To prepare learners for roles in cybersecurity policy, digital rights advocacy, and national legal systems.

Syllabus:

Unit I: Introduction to Surveillance and Constitutional Framework

- Meaning and Types of Surveillance (Physical, Digital, Mass, Targeted)
- Constitutional Limits to State Surveillance – Article 21 and Right to Privacy
- Distinction between Surveillance for Security and for Control
- Towards a Legal Framework for Ethical Surveillance in India
- European Court of Human Rights on Surveillance (Liberty v. UK)
- China's Cybersecurity and Surveillance Model
- UN Reports and Human Rights Watch Guidelines on Surveillance and Privacy

Suggested Readings:

Books:

- Shoshana Zuboff, *The Age of Surveillance Capitalism* (Public Affairs, 2019)

Articles & Reports:

- Surveillance vs. Security in India, *Economic and Political Weekly*, 54(10) (2019).
- The Right to Privacy in the Digital Age, United Nations Human Rights Council (A/HRC/27/37, 2014) Updated Reports: A/HRC/39/29 (2018), A/HRC/51/17 (2022)
- Human Rights Watch: “India’s Surveillance Industrial Complex”; (2021) <https://www.hrw.org>

Case Laws:

- *Liberty and Others v. The United Kingdom*, App no. 58243/00 (ECtHR, 2008) European surveillance case
- Supreme Court of India. (2017). Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

Unit II: Encryption – Law and Technology

- Basics of Encryption – End-to-End, Hashing, SSL/TLS
- Legal Status of Encryption in India and Global Standards
- Law Enforcement vs. Strong Encryption – Backdoors Debate
- Draft Encryption Policy of India (2015) – Analysis and Criticism
- Platform Liability and Intermediary Guidelines 2021 – Traceability Clause
- Role of Judiciary and Judicial Oversight Mechanisms
- Indian Telegraph Act, 1885 – Section 5(2)
- Information Technology Act, 2000 – Sections 69 and 69B
- Interception Rules, 2009 & Data Retention Policies
- Monitoring Tools – CMS, NATGRID, NETRA, and CCTNS

Suggested Readings:**Books:**

- Matthew Green, *Crypto-Trade Secrets* (MIT Press, 2019)
- Paul Rosenzweig, *Cyber Warfare & Encryption Policy*, Hoover Institution Press (2017).

Articles & Reports

- Raghavan, V. Decrypting the draft: Encryption policy and its implications. *Indian Journal of Law and Technology*, 12, 45, (2016).
- Susan Landau, “The Backdoor Dilemma: Encryption vs. Law Enforcement”, Brookings Institution Report (2016). <https://www.brookings.edu>
- Anja Kovac, “Intermediary Guidelines Traceability Clauses Analysis”, Internet Democracy Project (2021) <https://internetdemocracy.in>

Case Laws:

- Interception Rules, 2009 (India) — Supreme Court judgments interpreting these provisions in *People’s Union for Civil Liberties (PUCL) v. Union of India*, (1997) 1 SCC 301.

Unit III: Foundations and Ethical Issues in Technology Use

- Meaning and Scope of Cyber Ethics
- Philosophical Foundations – Utilitarianism, Deontology, Virtue Ethics in Cyberspace
- Ethics vs. Law in Cyberspace
- Netiquette, Digital Footprint, and Responsible Digital Citizenship
- Cyber Bullying, Hate Speech, and Online Abuse – Ethical Concerns
- Ethics in Artificial Intelligence, Machine Learning & Automation
- Ethical Challenges in Data Mining and Big Data Analytics
- Online Anonymity and Identity Theft – Ethical Implications
- Ethics in Online Journalism, Misinformation & Deepfakes
- Cyber security Ethics – Hacking, Penetration Testing, and Insider Threats

Suggested Readings:

Books:

- Michael J. Quinn, Ethics for the Information Age (Pearson, 2011)
- Joseph Migga Kizza, Ethical and Social Issues in the Information Age (Springer, 2013)

Articles & Reports

- Latanya Sweeney et al., Algorithmic Bias and the Ethical Challenges of AI, Harvard Kennedy School Research Paper No. RWP20-034 (2020).
- Karen Hao, The Ethical Crisis of Deepfakes and Fake News, MIT Tech. Rev. (2021).
- Rsvi Sharma, Digital footprints and identity theft: Emerging ethical concerns, Journal of Cyber Policy, 7(2), 89–105(2022).

Case Laws

- Lalita Kumari v. Govt. of U.P., (2014) 2 SCC 1.– clarifications on online harassment FIR registration
- Janhita B. Case K.S. Puttaswamy (Retd.) v. Union of India, (2019) 1 SCC 1 [Aadhaar Judgment]. (Puttaswamy II) – ethical surveillance implications

Unit IV: Cyber Policy Framework and Cyber Regulatory Authorities in India

- National Cyber Security Policy (NCSP) – 2013 & Proposed 2020 Draft
- Role of CERT-In (Indian Computer Emergency Response Team)
- Indian Cyber Crime Coordination Centre (I4C)
- National Critical Information Infrastructure Protection Centre (NCIIPC)
- Policy Challenges in Digital India and Cyber security Preparedness Role of Ministry of Electronics and Information Technology (MeitY)
- Telecom Regulatory Authority of India (TRAI) and Internet Regulation
- Reserve Bank of India (RBI) – Cyber security in Digital Payments
- Data Protection Authority under the Digital Personal Data Protection Act, 2023
- Adjudicating Officers, CERT-In and Sectorial Regulators

Suggested Readings:

Books:

- Vakul Sharma, India's Cyber Legislation Landscape (Universal Law Publishing), 2021.

Policy Reports

- India's National Cyber Security Policy, 2013; Proposed 2020 review (MeitY) <https://www.meity.gov.in>
- "NCSP Implementation Review", ITU and MeitY evaluation reports. ITU, India: NCSP Implementation Review Report (2021). https://unidir.org/wp-content/uploads/2023/05/UNIDIR_India_International_Cyber_Operations.pdf?utm_source=chatgpt.com
- TRAI Consultations on Net Neutrality & OTT Regulation https://www.trai.gov.in/sites/default/files/2024-11/Sridhar-Prasad_30-05-2016.pdf?utm_source=chatgpt.com

Unit V: International Institutions and Frameworks

- Budapest Convention on Cybercrime
- Internet Governance Forums (IGF) and ICANN
- United Nations and ITU Cybersecurity Initiatives
- European Union's GDPR – Ethics, Compliance and Enforcement
- Role of Interpol and Europol in Cybercrime Regulation Accountability Mechanisms and Limitations US Surveillance Framework – FISA, PRISM, and the Snowden Revelations
- UK Investigatory Powers Act, 2016

Suggested Readings:**Books:**

- Michael Schmitt (ed.), Tallinn Manual 2.0 on International Law Applicable to Cyber Operations (Cambridge University Press, 2017)
- Graham Greenleaf, Global Data Privacy Laws: 89 National Jurisdictions, 2019 Update (Oxford, 2019)

Articles:

- Laura K. Donohue, Section 702 and the Collection of International Telephone and Internet Content, Harvard Journal of Cybersecurity, Pol'y 117 (2014); https://harvardlpr.com/wp-content/uploads/sites/20/2014/07/Donohue_Symposium.pdf
- Lorna Woods, "UK Investigatory Powers Act, 2016 Review", European Data Protection Law Review, 3. (2017)

Case Law:

- R (Privacy International) v. Investigatory Powers Tribunal, [2019] UKSC 22.

Recommendations:

1. Information Technology Act, 2000, Sections 69, 69B
2. Indian Telegraph Act, 1885, Section 5(2)
3. Raman Jit Singh Chima & Udbhav Tiwari, *Surveillance in India: A Legal & Regulatory Overview*, 2013.
4. Srikrishna Committee Report on Data Protection and Surveillance (Official Documents: Justice B.N. Srikrishna Committee Report and Personal Data Protection Bill, 2018)
5. Snowden, Edward, *Permanent Record*, Metropolitan Books, 2019

6. Report of the UN Special Rapporteur on the Right to Privacy by the Secretariat-
<https://www.ohchr.org/en/special-procedures/sr-privacy>.
7. Liberty v. United Kingdom, ECHR, 2008
8. CIS India Reports on Encryption and Surveillance; <https://cis-india.org/internet-governance/blog/state-of-cyber-security-and-surveillance-in-india.pdf/view>
9. Intermediary Guidelines & Digital Media Ethics Code, 2021
10. Digital Personal Data Protection Act, 2023
11. National Cyber Security Policy, 2013
12. Budapest Convention on Cybercrime; <https://www.coe.int/en/web/cybercrime/the-budapest-convention>
13. Kizza, Joseph Migga, *Ethical and Social Issues in the Information Age*
14. UN GGE Reports on Cyber Norms and State Behaviour
15. CERT-In Guidelines & Advisories; <https://www.cert-in.org.in/s2cMainServlet?pageid=GUIDLNVIEW02&refcode=CISG-2024-01>
16. Internet Governance Forum Reports; <https://www.intgovforum.org/en/igf-2023-reports>
17. RBI Cyber Security Framework for Banks; <https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=10435>
18. TRAI Recommendations on Net Neutrality and OTT Regulation; https://traigov.in/sites/default/files/2024-09/Recommendation_14092020.pdf
19. Indian Cyber Crime Coordination Centre (I4C) Guidelines
20. ICANN Policy Briefs on Internet Infrastructure Governance; <https://www.icann.org/resources/pages/internet-governance-2013-06-14-en>

Evaluation Scheme:

- Internal Assessment (30 Marks):
2 written assignments (10 marks), 1 presentation (10 marks) and Class participation/ seminar (10 marks)
- End Semester Examination (70 Marks):
Section A: Short answer questions (30 marks)
Section B: Analytical/Essay-type questions (40 marks)

Semester II

Paper I- PGDCLDP 201

DATA PROTECTION & PRIVACY LAWS AND INTELLECTUAL PROPERTY RIGHTS IN THE DIGITAL SPACE

Duration: 40 hours (including lectures, seminars, and assessments)

Credits: 7

Introduction:

The digital age has revolutionized the way intellectual property (IP) is created, used, shared, and infringed. This paper examines how traditional IP law principles apply to digital environments, such as websites, software, online content, and domain names. It explores the legal mechanisms and challenges involved in protecting copyright, trademarks, and patents in cyberspace, along with international treaties and enforcement mechanisms. It also addresses current controversies like digital piracy, online licensing, and open-source software governance.

Course Outcomes (C.O.):

1. To understand the relevance and transformation of intellectual property rights in digital domains.
2. To examine the application of copyright, trademark, and patent laws in the context of digital content and technologies.
3. To analyze emerging legal issues such as domain name disputes, digital piracy, and online licensing models.
4. To evaluate the effectiveness of Indian and international mechanisms for protecting digital IPRs.

Program Outcomes:

1. To develop an in-depth understanding of IP law in the context of technology and cyberspace.
2. To empower students to advise on IP protection, enforcement, and litigation in digital platforms.
3. To sensitize learners to the need for balancing innovation, fair use, and IP enforcement in the digital economy.
4. To prepare learners for academic or professional roles in IP consultancy, digital law practice, and IP management.

Syllabus:

Unit I: Fundamentals of Data Protection and Privacy

- Understanding Privacy – Legal and Philosophical Dimensions
- Right to Privacy as a Fundamental Right – Puttaswamy Judgment
- Types of Data: Personal, Sensitive, Biometric, Financial
- Legal Definition and Components of Data Protection

- Evolution of Data Privacy Laws in India
- The Information Technology Act, 2000 – Sections 43A, 72, 72A
- Rules Relating to Reasonable Security Practices (SPDI Rules, 2011)
- Digital Personal Data Protection Act, 2023 – Key Provisions
- Rights of Data Principals, Obligations of Data Fiduciaries
- Role and Powers of the Data Protection Board of India

Suggested Readings:**Books:**

- Aparna Chandra, Farrah Ahmed, Siddharth Narrain – Privacy and the Constitution of India (Oxford University Press, 2022)
- Daniel J. Solove – Understanding Privacy (Harvard University Press, 2008)

Articles & Reports

- “Justice K. S. Puttaswamy v. Union of India: The Right to Privacy Judgment” – Economic and Political Weekly, Vol. 52, Issue No. 51, Dec. 23, 2017
- “Reasonable Security Practices under SPDI Rules, 2011: Industry Implementation Analysis” – Journal of Data Protection Law, 2014.

Case Laws:

- Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 – Fundamental Right to Privacy

Unit II: Corporate Responsibilities and Compliance

- Privacy by Design & Default
- Consent and Transparency in Data Processing
- Data Protection Impact Assessment (DPIA)
- Data Breach Notification Requirements
- Sector-Specific Data Compliance (e.g., Fintech, HealthTech, EdTech)
- Government Surveillance, National Security, and Privacy
- Data Localization and Digital Sovereignty
- AI and Big Data – Algorithmic Bias and Ethical Implications
- Facial Recognition, Biometric Data, and Consent
- Towards a Global Data Protection Treaty – Challenges and Prospect

Suggested Readings:**Books:**

- Graham Greenleaf – Global Data Privacy Laws: 89 National Jurisdictions, 2019 Update (Oxford University Press)

Articles & Reports

- “Consent Mechanisms under India’s 2023 Act and GDPR” – Berkeley Technology Law Journal, 36 Berkeley Tech. L.J. 1253 (2021).
- Andrea O’Sullivan, “Algorithmic Bias & Data Fiduciaries: Ethical Dimensions” – Harvard Journal of Law & Technology, Fall 2020.

- Meltzer, J. P., & Lovelock, P., “Data Localization and Sovereignty: Implications for Cloud Services” Brookings India Report (2018).

Unit III: Emerging Challenges and Future Pathways

- AI Surveillance, Facial Recognition, and Predictive Policing
- Surveillance Capitalism and Corporate Data Exploitation
- Impact of Surveillance on Democracy, Dissent, and Media Freedom
- International Treaties and Frameworks on Cross-Border Data Surveillance

Suggested Readings:

Books:

- Julie E. Cohen – Between Truth and Power: The Legal Construction of Informational Capitalism (Oxford, 2019)

Articles & Reports:

- “Predictive Policing and Bias: Rights Violations in Emerging Technologies” – American Civil Liberties Union (2016).
- “Cross-border Data Surveillance Treaties and their Limitations” – Journal of Cyber Policy.

Unit IV: Overview of Intellectual Property Rights

- Introduction to IPR: Copyright, Trademark, Patent, Design, Trade Secrets
- Philosophical and Economic Justifications of IPRs
- Role of IP in Digital Economy and Innovation
- Interface Between IP Law and Technology
- Key Statutes: Indian Copyright Act, Trade Marks Act, Patents Act
- Copyright Protection of Digital Works: Text, Image, Music, Videos, Software
- Digital Reproduction and Distribution Rights
- Fair Use vs. Infringement: YouTube, E-Libraries, Online Archives
- DRM (Digital Rights Management) and Anti-Circumvention Measures
- Internet Piracy, Torrenting, and Streaming Platforms

Suggested Readings:

Books:

- P. Narayanan, Intellectual Property Law, 4th ed., Eastern Book Company, 2017.
- Elizabeth Verkey, Law of Intellectual Property, 2nd ed., Universal Law Publishing, 2016.

Articles & Reports

- “DRM and Copyright enforcement in India” – NUJS Delhi Journal of IP Rights, Vol. 5, 2021, pp. 45–62.
- “Piracy and E-libraries: Fair Use Limits” – Journal of Copyright Society of India, Vol. 18, No. 2, 2020, pp. 101–115.
- Ann Cavoukian & Jeff Jonas, “Privacy by Design: The 7 Foundational Principles,” Information and Privacy Commissioner of Ontario, 2011.

Case Laws:

- Enforcement action in Zee TV vs. ISPs Delhi High Court, 2017 on infringement and injunctions

Unit V: Software Licensing, Open Source Issues, Trademark and Domain Name Disputes

- Legal Nature of Software: Copyright vs. Patent Protection
- Software Licenses: Proprietary, Freeware, Shareware
- Open Source Licenses: GPL, Apache, MIT – Legal Features and Restrictions
- Issues in Software Piracy and Enforcement
- Software Agreements: EULA and Terms of Use
- Trademark Infringement in Online Platforms
- Keyword Advertising, Meta Tags, and Cybersquatting
- Legal Protection of Domain Names under Indian Law
- WIPO's Uniform Domain Name Dispute Resolution Policy (UDRP)

Suggested Readings:

Books:

- S.P. Singh, Law of Copyright and Trademark in Digital Space, 1st ed., Central Law Publications, 2020.
- K.C. Kailasam & Ramu Vedaraman, Law of Copyright and Industrial Designs, 2nd ed., Eastern Law House, 2012.

Articles:

- “EULA, GPL, and License Risks: What Developers Must Know” – Stanford Technology Law Review, Vol. 14, 2019, pp. 77–94.
- “Keyword Advertising and Unauthorized Meta Tags” – Journal of Competition Law, Vol. 9, No. 1, 2022, pp. 56–73.

Case Law:

Tata Sons Ltd. v. Manu Kosuri & Others 2001 (21) PTC 432 (Del) – Trademark and cybersquatting

Recommendations:

1. N.S. Gopalakrishnan & T.G. Agitha, *Principles of Intellectual Property*
2. K. C. Kailasam & Ramu Vedaraman, *Law of Copyright and Industrial Designs*
3. WIPO Reports, *World Intellectual Property Organization Publications*
4. *Indian Copyright Act, 1957 (with amendments)*
5. *The Trade Marks Act, 1999*
6. *Information Technology Act, 2000*
7. *UDRP Rules and WIPO Arbitration Guidelines*
8. Law Commission Reports and relevant case law on digital IPR

Evaluation Scheme:

- Internal Assessment (30 Marks):
2 written assignments (10 marks), 1 presentation (10 marks) and Class participation/ seminar (10 marks)

- End Semester Examination (70 Marks):
Section A: Short answer questions (30 marks)
Section B: Analytical/Essay-type questions (40 marks)

Paper III- PGDCLDP 203

AI WITH EMERGING TECH IN CYBER LAW & AI WITH DATA GOVERNANCE IN A DIGITAL WORLD

Duration: 40 hours (including lectures, seminars, and assessments)

Credits: 7

Introduction:

Artificial Intelligence (AI) is transforming the legal, technological, and data governance landscapes. This paper explores how AI intersects with emerging technologies such as blockchain, quantum computing, big data, IoT, and surveillance tools, and examines the challenges and frameworks that govern their deployment. It focuses on the evolving role of AI in cyber law, digital governance, privacy regimes, ethical AI, accountability mechanisms, and regulatory frameworks.

Students will develop the ability to analyze, critique, and contribute to the debates and legal developments around AI-driven governance and digital ecosystems.

Course Outcomes (C.O.):

1. To understand the intersection between AI and cyber law in national and international contexts.
2. To analyze the ethical, legal, and regulatory challenges posed by AI, big data, and automation.
3. To critically assess the role of AI in surveillance, digital rights, and algorithmic accountability.
4. To examine emerging legal standards, national strategies, and data governance frameworks regulating AI and new technologies.

Program Outcomes:

1. Ability to link legal theories to practical technological applications such as AI, big data analytics, and smart systems.
2. Understanding of interdisciplinary approaches in regulating data-driven technologies and algorithms.
3. Promotion of responsible AI practices with human rights, privacy, and legal safeguards at the core.
4. Capacity to participate in digital policy-making, legal innovation, and AI governance debates.

Syllabus:

Unit I: Fundamentals of AI & Emerging Tech

- Introduction to Artificial Intelligence, Machine Learning, and Deep Learning
- AI and allied technologies: Blockchain, IoT, Quantum Computing
- Role of algorithms and predictive analytics in law enforcement
- Risks of bias, discrimination, and black-box decision making

- AI and the right to privacy, freedom of expression

Suggested Readings:**Books:**

- Stuart Russell & Peter Norvig, *Artificial Intelligence: A Modern Approach* (4th ed.). Pearson. 2021.
- Melanie Mitchell, *Artificial Intelligence: A Guide for Thinking Humans* (Penguin), 2019.
- Chris Reed & Marcin Biały – *Law, Artificial Intelligence and the Future of Government* (Oxford University Press, 2022)

Articles & Reports:

- “Understanding Artificial Intelligence and the Internet of Things” – NITI Aayog 2018; <https://www.niti.gov.in/ai-national-strategy-india>
- Green, H., “Risks of Black-Box AI: Legal and Ethical Issues” – *Harvard Journal of Law & Technology*, 2020.
- West, D., “AI and Law Enforcement: Predictive Policing and Bias” – Brookings Institution, 2019.; <https://www.brookings.edu/research/algorithmic-bias>

Unit II: AI and Cyber Law

- Legal personality of AI: Can AI be held liable?
- AI and automated legal reasoning systems
- Smart contracts and decentralized justice platforms
- Use of AI in legal research, drafting, and dispute resolution
- Algorithmic decision-making and procedural fairness

Suggested Readings:**Books:**

- Pavan Duggal, *Artificial Intelligence and Law* (Universal Law Publishing) 2022.
- Orin S. Kerr – *Computer Crime Law* (West Academic), 2021.

Articles:

- “Legal Personhood of AI: A Debate” – *Stanford Technology Law Review*, 2020.
- “Smart Contracts and Legal Enforceability” , *Harvard Law Review Blog*, 2020.
- “AI in Legal Tech and Judicial Systems” *Journal of Law & AI*, 2021

Unit III: AI and Data Governance

- Concept and models of data governance
- Role of AI in personal data processing and surveillance
- Consent, control, and algorithmic transparency
- Data trusts, fiduciary models, and accountability

Suggested Readings:**Books:**

- Cédric Villani Report (France), *For a Meaningful Artificial Intelligence: Towards a French and European Strategy*, 2018.

Articles:

- “Data Trusts as an Alternative Data Governance Model” – MIT Technology Review 2021.
- “Algorithmic Transparency in the Age of AI” – Journal of Cyber Policy
- OECD – Principles on Artificial Intelligence 2019.; <https://oecd.ai/en/>
- Data Governance in the Digital Age – World Economic Forum White Paper, 2021; <https://www.weforum.org/reports/data-governance>

Unit IV: Global Perspectives and Comparative Frameworks

- OECD, UNESCO, and EU AI frameworks (AI Act, GDPR implications)
- India's approach: NITI Aayog's AI strategy, DPDP Act 2023
- Comparative governance: US, China, and UK AI regulations
- Role of multilateral bodies in setting AI norms and ethics
- Explainability, fairness, and non-discrimination in AI systems

Articles & Reports:

- “Comparative AI Regulation: China, EU, USA, and India” – The Regulatory Review (Penn Law) 2021
- “AI Norms and Global Ethics: Role of Multilateral Bodies” – Carnegie Endowment for International Peace, 2020.
- European Commission – Artificial Intelligence Act 2021 (Proposed Regulation 2021/0106) <https://artificialintelligenceact.eu/>
- UNESCO – Recommendation on the Ethics of Artificial Intelligence (2021) <https://unesdoc.unesco.org/ark:/48223/pf0000381137>
- NITI Aayog – National Strategy for Artificial Intelligence 2021 #AIForAll <https://www.niti.gov.in/sites/default/files/2021-07/NationalStrategy-for-AI-Discussion-Paper.pdf>

Unit V: Ethical and Human Rights Challenges

- Sandbox models, risk-based approaches, and AI audits
- Regulation of autonomous systems (drones, self-driving cars, etc.)
- Legal sandbox initiatives in India
- Preparing law students for AI-driven practice
- Facial recognition and surveillance capitalism

Suggested Readings:**Books:**

- Virginia Eubanks – Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor (St. Martin’s Press), 2018.
- Shoshana Zuboff – The Age of Surveillance Capitalism (Public Affairs), 2019.

Articles & Reports:

- “Facial Recognition and Discrimination” – EFF Report on Surveillance, 2021; <https://www.eff.org/issues/surveillance>

- “AI and Human Rights: A Primer” – OHCHR Tech & Human Rights Report 2021; <https://www.ohchr.org/en/press-releases/2021/09/new-un-report-calls-moratorium-use-ai-predictive-policing>

Recommendations:

1. Rajya Sabha Report (2021) – *Ethical AI and Emerging Challenges*
2. UNESCO – *Recommendation on the Ethics of Artificial Intelligence* (2021)
3. Sandra Wachter – *Algorithmic Decision-Making and the Law*
4. Julie E. Cohen – *Between Truth and Power: The Legal Construction of Informational Capitalism*
5. Malgieri, G. – *Right to Explanation and Algorithmic Transparency*
6. Digital Personal Data Protection Act, 2023 (India)
7. Anita Allen, *Unpopular Privacy What Must We Hide?* Oxford University Press, 2011.
8. World Economic Forum. (2021). AI Governance Toolkit. Retrieved from <https://www.weforum.org/projects/ai-governance>
9. OECD. (2020). AI Regulatory Frameworks and Sandbox Models. Retrieved from <https://www.oecd.org/digital/artificial-intelligence/>
10. NASSCOM. (2021). Legal Sandbox Guidelines and AI Startups in India. Retrieved from <https://nasscom.in/knowledge-center/publications>
11. Harvard Journal of Law & Technology. (2021). Risk-Based Regulation of AI: A Comparative Study.
12. Stanford Cyber Policy Center. (2021). AI Auditability and Governance.

Paper III- PGDCLDP 203

Project / Dissertation / Internship

Credits: 7

Introduction:

The culmination of the PG Diploma program is the application of knowledge through a research-based project, dissertation, or practical internship. This paper is designed to foster independent thinking, analytical skills, and domain-specific expertise. Students are encouraged to explore real-world challenges in cyber law, data protection, digital privacy, AI ethics, cybercrime investigation, and policy analysis. The aim is to bridge academic learning with practical legal or regulatory exposure.

Course Outcomes (C.O.):

1. To enable students to apply theoretical knowledge in practical or empirical legal research.
2. To promote critical thinking and original contribution to emerging legal challenges in cyberspace.
3. To provide exposure to legal work environments through internships with law firms, courts, or regulatory agencies.
4. To prepare students for future academic research or professional engagements in cyber and data law fields.

Program Outcomes:

1. Strengthen academic and practical understanding of cyber law and data protection issues.
2. Encourage the development of writing, documentation, and citation skills.
3. Enhance the ability to engage with field-based or doctrinal research methodologies.
4. Promote interface with legal professionals, technology experts, and administrative institutions.

Structure & Guidelines:

Option A: Dissertation/Project

- Topic Selection: Based on areas like cyber law, AI and law, privacy rights, data governance, or cyber forensics.
- Supervisor: Each student will be assigned a faculty supervisor.
- Format: As per university norms (Abstract, Introduction, Literature Review, Methodology, Analysis, Conclusion, References).
- Word Limit: Minimum 10,000 words.
- Submission Date: To be notified by the college.
- Assessment Criteria: Originality (20%), Research Quality (30%), Relevance (20%), Structure & Presentation (20%), Viva (10%).

Option B: Internship

- Duration: Minimum 4 weeks

- Organizations: Cyber law firms, IT companies, government departments (e.g., CERT-In), courts, NGOs, data protection authorities.
- Supervision: Certificate from the host organization and report verified by academic coordinator.
- Internship Report: Minimum 3,000-word report detailing learning outcomes, observations, and contributions.
- Assessment Criteria: Participation (20%), Report Quality (30%), Relevance of Tasks (20%), Evaluation by Mentor (20%), Viva (10%).

Viva Voce Examination

A panel consisting of internal and external examiners will assess the student's presentation and defense of their work (whether dissertation/project or internship). Viva will evaluate clarity, conceptual grasp, articulation, and response to queries.

Suggested Areas for Dissertation/Project:

- Legal analysis of cyberbullying and harassment on social media platforms
- GDPR vs. India's Digital Personal Data Protection Act: A comparative legal study
- Regulation of AI-based surveillance in democratic societies
- Role of forensic tools in cybercrime investigations
- Blockchain and smart contract enforceability under Indian law
- Impact of data localization policies on cross-border trade

Suggested Readings & Resources:

1. ILI Publication, *Legal Research and Methodology*
2. Kothari C.R., *Research Methodology: Methods and Techniques*
3. Legal citation guides: Harvard Bluebook, OSCOLA