CRIMINAL LAW AND ARTIFICIAL INTELLIGENCE, ALGORITHMS & DIGITAL EVIDENCE

Responsible Faculty Instructor:
Neha Singh
neha.singh1@jgu.edu.in
Assistant Professor

Credits: 4
Credits Type: Law
Cross-registration:
Pre-requisites: Bharatiya Nyaya Sanhita (BNS), Bharatiya Nagarik Suraksha Sanhita (BNSS) and Bharatiya Sakshya Adhiniyam (BSA)

COURSE DESCRIPTION (COURSE VISION):

Criminal law is witnessing a seismic shift due to the 'digital realm', driven by the emergence of new forms of cybercrime. It is the need of the hour to critically interrogate and analyse the adequacy of existing doctrines of liability, evidence and justice in a rapidly digitalising world. This elective course explores the transformative impact of emerging technologies on the Indian criminal justice system. It examines whether traditional principles, such as actus reus, mens rea and evidentiary rules, are sufficient to accommodate developments such as deepfakes, cyber terrorism, FinTech crimes and revenge pornography.

The course examines the growing complexity of electronic evidence and the concerns about its admissibility and reliability. It covers and critically engages with themes such as cyber crimes in financial contexts, ransomware and cyberterrorism, and gendered crimes in online spaces. It also engages with critical questions surrounding AI liability, algorithmic bias, privacy, and the role of state and private actors in regulating digital harms. The course engages with these issues within the Indian legal framework, particularly the Bharatiya Nyaya Sanhita (BNS), the Bharatiya Sakshya Adhiniyam (BSA), the Information Technology Act (IT Act) and the Digital Personal Data Protection Act (DPDP).

TEACHING METHODOLOGY:

This course will adopt a multidisciplinary and discussion-driven pedagogy that blends theoretical frameworks with real-world case studies. Classes will be conducted through a mix of interactive lectures and guided debates on contentious issues, fostering a collaborative environment where students defend their interpretations against diverse viewpoints. Short reflective exercises will be integrated to encourage critical engagement with the subject. The discussions and debates will be anchored in readings, case studies and current developments, encouraging students to articulate their views and build independent critical thinking.

INTENDED LEARNING OUTCOMES:

- Students will engage with core criminal statutes along with the IT Act and the DPDP Act to explore how they address technologically driven offences. They will explore how digital evidence is stored and presented in criminal proceedings and will examine issues such as its authenticity

and admissibility. They will learn to reimagine evidentiary doctrines, such as hearsay and best evidence rules, in the context of intangible, complex digital evidence.

- Students will analyse how traditional principles of criminal liability, such as mens rea and actus reus, might apply to AI systems and platform intermediaries. They will critically consider how responsibility should be distributed and whether the existing doctrines are sufficient.
- Students will examine crimes like revenge pornography, cyberstalking and deepfake-based harassment to understand whether they disproportionately affect women or maginalised groups and if existing legal frameworks adequately address them.
- Students will examine whether predictive policing tools may disproportionately target certain groups and affect fairness in the criminal justice system.

READING LIST (upto 10 select readings):

CORE TEXTBOOK:

1. B. Ramaswamy, *An Exclusive Treatise on Cyber Crimes Law and Practice* (1st edn., Delhi Publishing Co., 2026).

RECOMMENDED BOOKS:

1. Santosh Kumar and Gagandeep Kaur, *Cyber Crimes and Laws: A Guide to Cyber laws & The Information Technology Act, Rules, Regulation & Notification* (4th edn., Whitesmann Publishing, 2024).
2. Susan W. Brenner, *Cybercrime: Criminal Threats from Cyberspace* (Praegar Pub Text, 2010).
3. Parvinder Kaur and Asif Iqbal, *From Mens Rea to Machine Rea: Reimagining Criminal Culpability in Digital Age* (Redshine India, 2026).

READING LIST [NOT EXHAUSTIVE]:

1. Kaushik Thinnaneri Ganesan, 'Evolution of Global Digital Forensics Laws and Emergent Challenges' in Gilbert Peterson and Sujeet Shenoi (eds), *Digital Forensics XIX: 19th IFIP WG 11.9 International Conference, Revised Selected Papers* (Springer, 2023) 237–248
2. Majid Yar and Jacqueline Drew, *'Image-Based Abuse, Non-Consensual Pornography, Revenge Porn: A Study of Criminalization and Crime Prevention in Australia and England & Wales'* (2019) 13(2) International Journal of Cyber Criminology 211–227.
3. Clare McGlynn and Erika Rackley, *'Image-based sexual abuse'* (2017) 37(3) Oxford Journal of Legal Studies 534–561
4. Asher Flynn, Jonathan Clough and Tully Cooke, 'Disrupting and Preventing Deepfake Abuse: Exploring Criminal Law Responses to AI-Facilitated Abuse' in Anastasia Powell, Asher Flynn and Lisa Sugiura (eds), *The Palgrave Handbook of Gendered Violence and Technology* (Palgrave Macmillan 2021) 539–559
5. Gargi Sarkar and Sandeep K Shukla, *'Reconceptualizing online offenses: A framework for distinguishing cybercrime, cyberattacks, and cyberterrorism in the Indian legal context'* (2024) 4 Journal of Economic Criminology
6. Renuka and Rohit Raj*, 'When AI Breaks the Law: Rethinking Mens Rea in the Age of Autonomous System'* (2026) Proceedings of the International Conference on Socio Legal Intricacies of Artificial Intelligence (ICSLIAI 2026) 140–145
7. S Arslan, *'The Legal Implications of Predictive Policing Algorithms: Bias, Oversight, and Public Accountability'* (2023) 2(3) Legal Studies in Digital Age 49–63

WEEKLY READING PLAN (WEEKLY OUTLINE):

A weekly plan is provided below:

MODULES	WEEK(S)
MODULE 1: REIMAGINING CRIMINAL LAW IN THE DIGITAL AGE Emerging cyber-crimes: an introduction How crimes happen online? Role of platforms and intermediaries	1 & 2
MODULE 2: DIGITAL EVOLUTION OF EVIDENCE Electronic evidence: admissibility and reliability Hearsay and Best Evidence rule in digital context Computer forensics and chain of custody	3, 4 & 5
MODULE 3: EMERGING CRIMES IN FINTECH FinTech Crimes: Phishing, vishing and money mules Ransomware attacks	6 & 7
MODULE 4: CYBER CRIMES AND DIGITAL VICTIMISATION Deepfakes and the truth crisis Revenge Pornography and Virtual Voyeurism Cyber stalking and online harassment	8, 9 & 10
MODULE 5: INDUSTRIAL ESPIONAGE AND CYBER TERRORISM Industrial Espionage and trade secrets Cyber terrorism and state security	11 & 12
MODULE 6: ARTIFICIAL INTELLIGENCE: LIABILITY AND ETHICS Can AI commit a crime? Facial Recognition Technology (FRT) and predictive policing bias	13 & 14
REVISION WEEK	Week 15