தமிழ்நாடு டாக்டர் அம்பேத்கர் சட்டப் பல்கலைக்கழகம்

The Tamil Nadu Dr.Ambedkar Law University

SCHOOL OF EXCELLENCE IN LAW

LL.M CBCS PATTERN

CURRICULUM

FROM ACADEMIC YEAR 2021 – '23

DEPARTMENT OF CYBERSPACE – LAW & JUSTICE

CYBER SPACE - LAW AND JUSTICE

The Department of Cyber Space - Law and Justice of The TamilNadu, Dr. Ambedkar Law University, School of Excellence, Chennai has been newly launched as an updated and unique specialization in the University.

"The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb". To understand a broader perspective of the interface of technology and law is a need of the hour.

The TNDALU provides remarkable opportunity to study Cyber Law in convergence with IPR in a collaborative Environment. This discipline is established to provide a continuing legal education in the growing field of Cyber Law. The Objective of this course further stretch out to enrich the students as tech legal experts to serve in Forensics department, Cyber Labs and Technical Expertise in various crime branches.

Human beings are now cyber beings, choosing to spend a considerable amount of time in cyber world. As cyber world expands cybercrimes grows with it. Anonymity awarded by the cyber space makes the matters more complex which can't be handled by conventional laws. The course is designed to enrich the new generation of legal fraternity to grow as cyber law professionals. This Department in LLM will enlighten the students to find career prospects in this arena in convergence with other laws as the choice-based credit system in the Institution will provide them an access with other departments such as IPR, Business Law, Criminal Law and Administration and Human Rights.

The Department of LLM Cyber Space - Law and Justice is formed with a special focus on creating a tech savvy legal fraternity with specialized knowledge and competence in the field of Cyber Laws. The Programme offers 6 Core Papers, 3 Discipline Specific Elective Papers, 2 Generic Elective Papers which synchronizes Technology, Law and Administration. This two-year (four semesters) course will equip them as expertise in this new field of law.

The Elective Papers are constructed with the aim of exploring the global prospects of cyber space. The syllabus of this course is formulated through meticulous research which prepares the students to fetch career opportunities worldwide in an international sphere. The generic electives will create an overall perspective of cyberspace and provides a comprehensive approach towards emerging challenges in Cyber Security and related laws which augments the students as able researchers.

The LLM Programme is offered to create Techno legal Education and Awareness about cyberspace aspects in the society. The University aims at creating equity in education by providing opportunity to all sects including students from rural background for whom Higher Education is unreachable is one of the visions of TNDALU.

THE TAMIL NADU DR. AMBEDKAR LAW UNIVERSITY

BRANCH - X

DEPARTMENT OF CYBER SPACE -LAW & JUSTICE

LL.M SYLLABUS

HARD CORE COURSES – 06

1. Cyber Laws and Regulations in India.
2. Intellectual Property Rights and Cyberspace.
3. Techno Legal aspects of Cyberspace.
4. Global Scenario of Cyberlaws.
5. Cyber Crime in India.
6. Computer Forensics.

DISCIPLINE ELECTIVE COURSES – 03

1. Digital Evidence.
2. Transnational Cyber Crimes.
3. Cyberspace and Telecommunications: Legal and Security Issues.

ELECTIVE COURSES - 02

1. E-Commerce and Consumer Protection.
2. International Cyber Security and Governance

SUBJECTS IN SEMESTERS

First Semester	• Legal Education and Research Methodology. **(Common Course-I)** • Judicial Process. **(Common Course-II)** • Cyber Laws and Regulations in India. **(Hard Core Course-I)** • Intellectual Property Rights and Cyberspace. **(Hard Core Course-II)** • E-Commerce and Consumer Protection. **(Elective Course-I)**
Second Semester	• Constitutional Law: The New Challenges (**Common Course-III)** • Law and Social Transformation in India **(Common Course-IV)** • Techno Legal aspects of Cyberspace. **(Hard Core Course-III)** • Digital Evidence. **(Discipline Elective Course-I)** • Applied Research Methodology.
Third Semester	• Global scenario of Cyber laws. **(Hard Core Course-IV)** • Cyber Crime in India. **(Hard Core Course-V)** • Transnational Cyber Crimes. **(Discipline Elective Course-II)** • International Cyber Security and Governance. **(Elective Course-II)**
Fourth Semester	• Computer Forensics. **(Hard Core Course-VI)** • Cyber Space and Telecommunication: Legal and Security Issues. **(Discipline Elective Course-III)** • Skill Enhancement Course (SEC) • Dissertation

COURSE – I

CYBER LAWS AND REGULATIONS IN INDIA

(Hard Core Course - I)

OBJECTIVE OF THE COURSE:

The main objective of this course is to make students familiar with the developments that are being taking place in cyber sphere with the help of Computer and Information Technology. The students will acquire knowledge in the Fundamentals of Cyber Law . The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000.

LEARNING OBJECTIVES

- *To understand the origin and development of cyber space and cyber laws*
- *To understand the various rules and procedures for the applicability of the cyber laws with reference Indian laws*
- *To understand the contemporary issues and challenges in cyber laws*

COURSE OUTLINE

MODULE I - FUNDAMENTALS OF CYBER SPACE AND CYBER LAW

a) Computers and its impact in society - Computer and web technology

b) History of Internet - Cyber Security Definition - Meaning, definition, Genesis of cyber law - Growth and development of cyber law in India - Significance and objectives of cyber law

c) The difference between Real Space and Cyber Space - Conceptual and theoretical perspective of Cyber Law - Cyber sovereignty - Various components of cyber law - Data and privacy - Cybercrimes - Intellectual property - Electronic and digital signatures

d) Categories of cybercrimes - Cybercrimes against Individual - Cybercrimes against Property - Cybercrimes against Government

MODULE II - LEGISLATIONS RELATING TO CYBER LAWS IN INDIA

a) Information Technology Act, 2000 - Aim, objects and Overview of the Act - Jurisdiction - Electronic Governance

b) Electronic Evidence - Digital Signature and Electronic signature - Subscribers, Certifying Authorities, Internet Service providers - Penalties, Compensation and Adjudication - The Cyber Appellate Tribunal - Offences

c) The national cyber Security Policy, 2013 - Prevention of Money Laundering Act,2002

d) The Indian Evidence Act, 1872 - The Banker's Book Evidence Act, 1891- Indian Penal Code 1860 - Reserve Bank of India Act, 1934

MODULE III – E-COMMERCE

a) Meaning and definition of E-Commerce - Evolution of E-Commerce - Types of E-Commerce

- UNCITRAL Model on E-Commerce and its implementation

b) Legal aspects of E-Commerce relating to -Digital Signatures - Technical and Legal issues of E-Commerce

c) Trends and Prospects of E-Commerce - E-taxation -E-banking, Payment mechanism in cyberspace - Online publishing - Online payment - E- Contracts

d) Legal aspects relating to Payment mechanism in cyberspace

MODULE IV – CONSUMER PROTECTION IN CYBER SPACE

a) E-Consumers, E-Consumers support and services

b) Caveat Emptor: Consumers Beware - Private policy - Terms of service

c) Legal remedies - Consumer Protection Act, 2019 - The Specific Relief Act, 1963 - The sale of Goods Act, 1930

MODULE V– LEGAL FRAMEWORK OF PROTECTING PRIVACY IN CYBER SPACE

a) Concept of Privacy, Principles of Privacy Law, Threats to Privacy in New Technological Regime, Digital and Internet Privacy Challenges - Constitutional perspective of Right to Privacy - Tortious Liability for Protection of Privacy

b) Regulatory perspective of Privacy under - Information Technology Act, 2000

c) Right to Information Act, 2005 - Easements Act, 1882 - Indian Penal Code, 1860 - Indecent Representation of Women (Prohibition) Act, 1987

d) Intellectual Property Rights - Specific Relief Act, 1983

MODULE VI – ONLINE CONTRACTS

a) Formation and validity of Online Contracts - Types of Online Contracts

b) Evidentiary value of Online Contracts
c) Legal issues in Online Contracts
d) Discharge and Remedies of Online Contracts - Advantages of Online Contracts over conventional contracts

MODULE VII – DISPUTE RSOLUTION IN CYBER SPACE - ODR

a) Alternate Dispute Resolution (ADR) And Online Dispute Resolution (ODR) - Kinds of ODR

- Functioning of ODR System - Disputes Handled through ODR Environment

b) Mode of Communication in ODR
c) Generation of Confidence in ODR
d) The impact of ODR in cyberspace - Legal Aspects on ODR

MODULE VIII – CONTEMPORARY ISSUES IN CYBER SPACE AND CHALLENGES IN CYBER LAW

a) Cloud Computing - Block Chain Technology
b) Challenges in mobile laws
c) Legal problems relating to social media
d) Spam laws

BIBLIOGRAPHY

RECOMMENDED READING:

BOOKS

1. N.S Nappinai – Technology Laws, 1st Ed LexisNexis (2017)
2. Apar Gupta, Commentary on Information Technology Act (2016).
3. Justice Yatindra Singh, Cyber Laws, Universal Law Publishing, UP, 2016.
4. Farouq Ahmed, Cyber Law in India, Allahabad Law Agency, 2015
5. Karnika Seth, Computers, Internet and New Technology Laws-A Comprehensive Reference Work With Special Focus On Developments In India, LexisNexis, Nagpur, 2016.
6. Kamath Nandan: Law relating to Computer, Internet and E-Commerce, Universal Law Publishing, UP, 2007.

JOURNALS / ARTICLES

1. Nishith Desai, E-commerce in India – Legal, tax and regulatory analysis available at http://www.nishithdesai.com/fileadmin/user_upload/pdfs/Research%20Papers/ECommerce_in_India.pdf
2. Hemali Shah and Aashish Srivastavat ―Signature Provisions in the Amended Indian Information Technology Act 2000: Legislative Chaosl, 43 Comm. L. World Rev. 208 2014 available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2748441
3. Christopher Reed, ―Legally binding electronic documents: Digital Signatures and Authentication 35(1) International Lawyer 89-106 available at http://www.jstor.org/stable/40707597
4. Darrel C. Menthe, Jurisdiction in Cyberspace: A Theory of International Spaces, 4 Mich. Telecomm. & Tech. L. Rev. 69 (1998). Available at: http://repository.law.umich.edu/mttlr/vol4/iss1/3
5. Cyber Laws of India‖, www.iibf.org.in/documents/Cyber-Laws-chapter-in-Legal-AspectsBook.pdf (Book on IT security of IIBF published by Taxmann Publishers)
6. Amlan Mohanty, New Crimes under the Information Technology Amendment Act, 7 Ind. J. L. & Tech. 103 (2011) available at Westlaw India.
7. Rachna Choudhary, Remedies For Breach of E-Contracts, Journal on Contemporary Issues of Law Volume 3 Issue 9. Available at https://jcil.lsyndicate.com/wp-content/uploads/2017/10/Rachna- Choudhary.pdf

FURTHER READING:

BOOKS

1. Harish Chander, Cyber Law and IT Protection, PHI Learning Private Limited, Delhi (2015)
2. V. D. Dudeja, Information Technology and Cyber Law , Common wealth Publisher (2017)
3. Anirudh Rastogi, Cyber Law: Law of Information Technology and Internet, Lexis Nexis, (2014).
4. Mark A Lemley, Peter S. Menell, Robert P Merges, and Pamela Samuelson, Software and Internet Law, Aspen Publishers, New York, (2006).
5. Cohen, Lore, Okediji, and O'Rourke, Copyright in a Global Information Economy. Aspean Publisher, New York, (2010)

6. Abhivardhan, Artificial Intelligence Ethics and International Law: An Introduction, BPB Publisher, Delhi (2019)
7. Don Tapscott and Alex Tapscott, Block Chain Revolution, Penguin Random House, UK (2018).
8. Information Technology Law and Practice- Cyber Laws and Laws Relating to E-Commerce Paperback – 1 Nov 2016 by Vakul Sharma
9. Anne S.Y. Cheung, Privacy and Legal Issues in Cloud Computing, Edward Elgar Publishing, (2016).
10. Satish Chandra: Cyber Law in India, ABS Edition 1, 2017
12. Lawrence Lessig, Code and Other Laws of Cyberspace 1999, Code version 2.0, Basic Books Publication (2006).
13. Law Relating to COMPUTERS, Internet and E-Commerce - A Guide to CYBER LAWS & the IT

Act, with Rules, Regulations, Notifications & Case Law By NandanKamath (Ed.), Foreword by N.R.Madhava Menon.

14. Cyber Law- Indian And International Perspectives On Key Topics Including Data Security, E- Commerce, Cloud Computing And Cyber Crimes Hardcover – 2012 by AparnaViswanathan
15. Scott Charney & Kent Alexander, Computer Crime, 45 Emory L. J. 931, (1996).

JOURNALS / ARTICLES

1. Teoh, Chooi & Mahmood, Ahmad Kamil. (2017). National cyber security strategies for digital economy. Journal of Theoretical and Applied Information Technology. Available at https://www.researchgate.net/publication/322150967_National_cyber_security_strategies_for_digit al_economy
2. Ethan Katsh (2007). Online Dispute Resolution: Some Implications for the Emergence of Law in Cyberspace. Available at https://www.tandfonline.com/doi/abs/10.1080/13600860701492096
3. David G.Gordon (2016), Legal Aspects of Cloud Computing. Available at https://www.researchgate.net/publication/316350308_Legal_Aspects_of_Cloud_Computing

CASES FOR GUIDANCE

1. Google India Pvt Ltd. Vs.Vishaka Industries and Anr. AIR 2020 SC 350
2. Sharat Babu Digumarti v. Govt. of NCT of Delhi AIR 2017 SC 150
3. W.B. State Election Commission v. Communist Party of India (Marxist), 2018 SCC On Line SC 1137AIR2018 SC 3964
4. Sonu alias Amar v. State of Haryana: (2017) 8 SCC 570
5. Ramesh Rajagopal vs. Devi Polymers Private Limited AIR 2016SC 1920
6. B.N. Firos vs. State of Kerala and Ors. 2018(9)SCC 220
7. Union of India (UOI) and Ors. vs. G.S. Chatha Rice Mills and Ors. MANU/SC/0714/2020
8. The State of Uttar Pradesh vs. Aman Mittal and Ors. 2019(19)SCC740
9. The Bank NSP Case: State by Cyber Crime Police vs. Abubakar Siddique
10. Bazee.com case: Avnish Bajaj vs. State (N.C.T.) Of Delhi 3 Comp LJ 364 Del, 116 (2005) DLT 427, 2005 (79) DRJ 576
11. Parliament Attack Case: State vs. Mohammad Afjal Delhi 1, 107 (2003) DLT 385, 2003 (71) DRJ 178, 2003 (3) JCC 1669
12. Andhra Pradesh Tax Case: Andhra Pradesh State Road vs. The Income-Tax Officer 1964 AIR SCR (7) 17.
13. State of Tamil Nadu v. Suhas Katt
14. Shreya Singhal v. U.O.I AIR 2015 SC 1523
15. Ranjit D. Udeshi v. state of Maharashtra AIR 1965 SC 881
16. Yahoo Inc v. Akash Arora & Anr, 78 (1999) DLT 285
17. Casio India Co. Ltd., v. Ashita Tele systems Pvt Ltd, 106 (2003) DLT 554

LEARNING OUTCOME

After completion of the course students will be able to

- *Understand and explain the rudiments of cyber space*
- *Learn the scope and function of legal and technological regulations of the internet.*
- *Understand with the Social and Legal issues emerging from Cyberspace.*
- *Explore the legal and policy developments in India to regulate Cyberspace.*
- *Develop the understanding of relationship between commerce and Cyberspace*
- *Give learners in depth knowledge legal frame work of cyber laws in India*

COURSE – II

INTELLECTUAL PROPERTY RIGHTS AND CYBER SPACE

(Hard Core Course - II)

OBJECTIVES OF THE COURSE:

Intellectual Property, which is the creation of human mind, plays a prime role in the virtual world. The growing demand of electronic commerce urges the peoples to visit a large number of websites and to explore the ways for digitalizing the works embodying intellectual property. Musical works, pictures, movies, multimedia works and audio-visual works, pictures, software, designs are various products and services based on Intellectual Property which can easily be accessed through the Internet. Though the advent of information technology provides enormous opportunity to entrepreneurs and creators to make profit in a new and rapidly growing medium, the international character of e-Commerce raises various IPR issues relating to domain names, cybersquatting, protection of copyrights and related rights, linking, framing, music and audio-visual works, patents and patentable subject matter, online service providers' liability etc. This course will focus on these new issues and challenges in cyberspace.

With this objective the course is designed to

- *Analyze the expansion of the scope of Intellectual property due to the technological progress of recent years.*
- *Understand the legal issues involved in the protection of Intellectual property in the virtual world under various legislations.*
- *Study the difficulty to resolve disputes of copyright and trademarks in cyberspace since the inadequacy of Intellectual property statutes to cover the new aspects of Information technology.*
- *Discuss the challenges and issues pertaining to Cloud computing, Artificial Intelligence, Block Chain Technology, Big Data Analytics- Data Protection.*

COURSE OUTLINE

Module I Introduction to Intellectual Property Rights:

a. Intellectual Property - Meaning, Nature, and Concept-Theories of IPR- theoretical justification for Protection of Intellectual Property.
b. Origin and Development of Intellectual Property Rights-types of intellectual property-Copyright, Patents, Trademark, Designs etc.,

c. Internationalization of IP Protection-Paris Convention, Berne Convention, TRIPS Agreement

–basic principles and minimum standards- flexibilities under TRIPS

d. Principles of Reciprocity and Priority- Concept of Minimum Standards- Concept of National Treatment-Concept of Most Favoured Nation (MFN), Doctrine of Exhaustion with respect to Intellectual Property Rights

Module II: Copyright Issues in Cyberspace

a. Origin of Copyright protection for computer software-originality, doctrine of merger, doctrine of sweat of the brow, idea expression dichotomy
b. Scope of copyright protection of computer programme-protection for literal element and non- literal element of programme code-protection for functional elements and protocols-protection for program outputs-user interfaces.
c. Exclusive rights in computer programme- fair use-reverse engineering-software interoperability-Google v Oracle- Copyright Misuse

Module III: Copyright Infringement in Cyberspace

a. Direct and secondary Liability-volition as an element of direct liability-contributory and vicarious liability for copyright Infringement
b. Liability of online service providers-safe harbors- Viacom International, Inc. v. YouTube, Inc.
c. Liability of device manufacturers- doctrine of staple article of commerce- inducement theory

Module IV: Technological Protections for Copyrighted Works

a. Early History of Technological Protection Measures- The Audio Home Recording Act-WIPO Internet Directives-WCT & WPPT- Obligation concerning technological measures
b. The Digital Millennium Copyright Act- EU Copyright Directive – Indian Copyright (Amendment) Act 2012-DRM
c. Second generation of DMCA disputes

Module V: Patent Protection of Computer Programme

a. Development of patent protection of computer programme in US- algorithm as patentable subject matter-patentability of computer related inventions-computer programme as a 'means to an end' for patent protection
b. Business method patent- State Street Bank, Bilski v kappos, Alice Corp Private Ltd v CLS bank
c. TRIPS Agreement-Patent Protection for Computer programme in India –guidelines for computer related inventions.
d. Design patents on Software

Module VI: Trademark issues in Cyberspace

a. Domain name and cybersquatting-trade mark infringement and dilution-Anti-cybersquatting Consumer Protection Act-ICANN –Uniform Dispute Resolution Policy
b. Domain Name as speech
c. Other uses of trademarks-metatagging-pop up advertisements-key word advertising-gripe sites

Module VII: Software Licensing

a. Contract formation-shrinkwrap licenses-click wrap licenses, browse wrap licenses and electronic commerce
b. The contract –intellectual property boundary –IP preemption- Anti trust
c. Open source licensing

Module VIII: New issues and Challenges in Cyberspace

a. Artificial Intelligence Big Data Analytics- Concept of Artificial Intelligence-Intellectual Property challenges relating to the recognition of AI creations- Ownership concerns.
b. Block chain and Management of Intellectual Property Rights-Concept of Block chain-Block chain technology for the management and strengthening of IP regime- Licensing and Smart contracts
c. Database Protection- EU Database Directive-Right to privacy

BIBLIOGRAPHY

RECOMMENDED READING:

BOOKS

1. Nandan Kamath, Law relating to Computers Internet & and E-commerce, Universal Law Publishing Co Pvt Ltd. (2009)
2. Rodney D Ryder, Intellectual Property and the Internet, Lexis Nexis Butterworths, New Delhi.
3. David Bainbridge, Information Technology and Intellectual Property Law, Bloomsbury Professional, 7th Edition, (2019).
4. Vakul Sharma, Information Technology Law and Practice, Universal Law Publishing Co Pvt Ltd
5. David Lindsy, International Domain Name Law ICANN at the UDRP, (2007) Hart Publishing, Oxford and Portland, Oregon.
6. Samuelson and others, Software and Internet Law, Aspen Publishers, U.S.

FURTHER READING:

1. Jeanne C. Fromer and Christopher Jon Sprigman, Copyright Law Cases and Materials (2021).
2. Pamela Samuelson et.al. "A Manifesto Concerning the Legal Protection of Computer Programs, Columbia Law Review (1991).
3. Cohen, Loren, Okediji, & O'Rourke, Copyright in a Global Information Economy, Aspen Publishers, Third Edition (2010)
4. Chris Reed, Internet Law, Text and Material, Universal Law Publishing Co. Pvt. Ltd. (2005)
5. Pamela Samuelson, "Privacy as Intellectual Property", Stanford Law Review
6. Raymond S R Ku & Jacqueline D Lipto, Cyberspace Law- Cases and Materials, Aspen Publishers, Second Edition (2006)
7. P. Bernt Hugen Holtz, Copyright and Electronic Commerce, Kluwer Law International, London
8. Mark J. Davidson, Legal Protection of Databases, Cambridge University Press, London
9. Robert P. Morges, Peter S. Menell, Mark A. Lemley, Intellectual Property in the New Technological Age, Aspen Publishers, New York

10. Dr. Irini A. Stamatoudi & Paul L.C. Torremans, Copyright in the New Digital Environment: The Need to Redesign Copyright, Sweet & Maxwell, London

JOURNALS / ARTICLES

1. Stacey L. Dogan & Mark A. Lemley, Trademarks and Consumer Search Costs on the Internet, 41 Hous. L. Rev. 777 (2004).
2. Mark A. Lemley and R Anthony Reese, Reducing Digital Copyright Infringement without Restricting Innovation, 56 Stan. L. Rev. 1345 (2004).
3. Pamela Samuelson, intellectual Property and The Digital Economy: Why the AntiCircumvention Regulations Need to be Revised, 14 Berkely Tech. L. J. 519 (1999).
4. Julie Cohen, Reverse Engineering and the Rise of Electronic Vigilantism: Intellectual Property Implications of "Lock-Out" Technologies 68 S. Cal. L. Rev 1091 (1995)
5. Rochelle Cooper Dreyfuss, Are Business Method Patent Bad for Business? 16 Santa Clara Computer & High Tech. L.J. 263 (2000)
6. Mark A. Lemley, Intellectual Property and Shrinkwrap Licenses, 68 S. Cal L. Rev. 1239 (1995)
7. Jinku Huang, Is the ACPA a Safe Haven for Trade Mark Infringers? Rethinking the Unilateral Application of the Lanham Act, J. Marshall, J. Comp. & Info. L. 655 (2004)
8. Jessica Litman, Sharing and Steeling, 26 Hastings Comm. & Entertainment L. (2004)
9. Neil W. Netanel, Impose a Non Commercial Use Levy to allow Free Peer-to-Peer File Sharing 17 Harv. J. L. & Tech. l. (2003)
10. Pamela Samuelson, Did MGM Really Win the Grokster Case? 48 Communications ACM 19 (2005)

CASES FOR GUIDANCE

1. Diamond v Diehr 1981
2. Bilski v Kappos (2010)
3. Alice Corp Private Ltd v CLS bank (2014)
4. Computer Associates international inc., v. altai 982 F.2d 693 (3rd Cir 1992)
5. Sega EnterPrises Ltd v. Accolade Inc., (1992)
6. A & M Records v Napster Inc., 239 F. 3d 1004 (9th Cir. 2001)
7. Metro-Goldwyn-Mayer Studios Inc v. Grokster, Ltd 125 S. Ct. 2754 (2005)
8. Yahoo Inc v. Akash Arora & Anr, 78 (1999) DLT 285
9. Panavision International L. P. v. Toeppen 141 F.3d 1316 (9th Cir 1998)

10. Brookfield Communications inc v. West Coast Entertainment Corporation 174 F.3d 1036 (9th Cir 1999)
11. Tata Sons V Greenpeace International (2011)178 DLT 705
12. Perfect 10, Inc. v. Amazon.com, Inc. 508 F.3d 1146 (9th Cir. 2007
13. Perfect 10, Inc. v. Visa International Service, Association 494 F.3d 788 (9th Cir. 2007)
14. Viacom International, Inc. v. YouTube, Inc. 676 F.3d 19 (2d Cir. 2012)
15. Stephanie Lenz v. Universal Music Corp. 815 F.3d 1145 (9th Cir. 2016)
16. Sony Corporation of America v. Universal City Studios, Inc. 464 U.S. 417 (1984)
17. A&M Records, Inc. v. Napster, Inc. 239 F.3d 1004 (9th Cir. 2001)
18. Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd. 545 U.S. 913 (2005)
19. Chamberlain Group, Inc. v. Skylink Technologies, Inc. 381 F.3d 1178 (Fed. Cir. 2004)
20. Google LLC v. Oracle America, Inc. 141 S. Ct. 1183 (2021

LEARNING OUTCOME

After the completion of the course, students will be able to-

- *Understand the significance of protecting the different aspects of information generally recognized as Intellectual Property in Computers.*
- *Critically analyze the complicated issues in enforcing Intellectual Property Rights in Cyberspace.*
- *Analyse the challenges posed by the new technologies and examine the role of Intellectual Property protection in the digital environment.*
- *Explore the legal framework in individual states with respect to the articulation of cyber jurisdiction in its personal laws.*
- *Appreciate the relevance of new technologies in the management of Intellectual Property Rights.*

COURSE – III

TECHNO LEGAL ASPECTS OF CYBER SPACE

(Hard Core Course - III)

OBJECTIVES OF THE COURSE:

Technology interacts with social, economic and legal frameworks to set the basic affordances and constraints of human activity over time. The most significant present transformation revolves about computers and the emergence of the networked information economy. These new technological and economic conditions are creating new forms of production and new forms of social behavior that are fundamentally altering the way we know the world, how we learn about how the world. It is important that we know this transformation and understands it in political as well as economic terms. Exploring The Law and Technology Relationship is a significant aspect to learn in this era.

With this objective the course is designed to

- *Understand the rise of technology and advancements in this century*
- *Produce a clarity in the application of technological aspects in Judiciary*
- *Focus on the convergence of law and technology, its impact over upcoming generation*
- *Develop a sense of responsibility in tech legal world as a citizen*
- *Create a Prospective career in E - Law and its tributaries*

COURSE OUTLINE

Module I: Cyber Space - Nature and Framework

a. Cyber Space - Evolution of Cyber Jurisprudence
b. Distinction between Conventional Crime and Cyber Crime

Module II: Cyber Crimes - Detailed Outline

a. Computer Source Code - Cyber Pornography - Cyber Security - Cyber Terrorism
b. Data Privacy & confidentiality - Digital Signature
c. Intermediaries - Malware - Other Computer related offences - Unauthorized Access - Violation of privacy - IP Theft
d. Impersonation - Cyber corporate frauds - Internet frauds and financial crimes - Cyber-Smearing - Interception of communication and theft of commercial data.

Module III: Law and Technology - The Blended Mechanism

a. Frontiers in Artificial Intelligence - Fundamental Rights in cyberspace - Consumer Rights in the Online Environment
b. Resolving Legal Complexity - Alternate Dispute Resolution - Online Dispute Resolution
c. Legal and Ethical Aspects of Artificial Intelligence

Module IV: Judicial Framework

a. Alternate Dispute Resolution - Online Dispute Resolution
b. Development of E - Courts - Access to E - Courts - Procedural Impediments
c. Awareness and Educational Programme on Tech - Legal Mechanism -Pandemic and Issues of Cyber Space

Module V: Convergence of Technical and Legal Aspects of Cyber Space

a. Growth of Education in Cyber Space - Menace of Digital Piracy - Copyright in Cyber Space

- Measures to Combat

b. Role of Technology in Economy - E – Contracts - Digital and E – Commerce Markets
c. Cyber Warfare - Technical Protection and Stealing of Information - Information Warfare

Module VI: Role of Technology in Investigative Framework

a. Cyber Forensics - The Use of Facial Recognition Technology for Policing
b. Interpol and Cyber Space - Jurisdictional Issues in Cross - Border Cyber Issues

Module VII: International Approach towards Tech - Legal Prospects

a. UN's Initiative - E - Treaties - Budapest Convention
b. Impact of Technology in Right to Privacy - Imparting Human rights through Technological aspects

BIBLIOGRAPHY

RECOMMENDED READING:

BOOKS

1. Stephen Mason and Andrew Sheldon, Proof: "The investigation, collection and examination of digital evidence, in Electronic Evidence", LexisNexis, 2013.

2. Vivek Dubey, "Admissibility of electronic evidence: an Indian perspective" , 2017
3. SHACKELFORD, S.J., 'The Law of Cyber Peace', Chicago Journal of International Law, 2017
4. GOLDSMITH, J., 'Cybersecurity Treaties: A Skeptical View', A Future Challenges Essay, 2011
5. SANDER, B., 'Cyber Insecurity and the Politics of International Law', 2017

FURTHER READING:

1. SCHMITT, M. (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge University Press, 2017).
2. SINGER, P.W., & FRIEDMAN, A, "Cybersecurity and Cyberwar" (Oxford University Press, 2014
3. TSAGOURIAS, N., 'The legal status of cyberspace', in TSAGOURIAS, N., & BUCHAN,

R. (eds.), Research Handbook on International Law and Cyberspace, 2015

4. VISHIK ET AL., C., 'Key Concepts in Cyber Security: Towards a Common Policy and Technology Context for Cyber Security Norms', 2016
5. FINNEMORE, M. & HOLLIS, D.B., 'Constructing Norms for Global Cybersecurity', 110 American Journal of International Law (2016)

LEARNING OUTCOMES

After completion of the course students will be able to

- *Understand the impact of technology on legal sphere*
- *Explore the new career prospects in technological phase of legal and para legal arena.*
- *Have clarity over the interface of technology with new dimensions of law and administrative procedures*
- *Focus on the E - Litigation in various countries and its impact over new developments*
- *Analyse the impact of technical intrusion in law and social justice.*

COURSE – IV

GLOBAL SCENARIO OF CYBER LAWS

(Hard Core Course - IV)

OBJECTIVES OF THE COURSE:

Cyber space is the intangible dimension that is difficult to govern and regulate using conventional legislation and Cyber Law is the need of the hour in this digital age. This course explains the growth of cyber law and the growing challenges ahead in the digital society.

With this objective the course is designed to

- *Understand the role of Cyber legislation in current scenario.*
- *Analyze the global structure of cyber law and its implications through international conventions and guidelines*
- *Study the changing dimensions of cyber law along with the parallel growth of technologies.*
- *Discuss the dispute settlement approaches in international sphere.*

COURSE OUTLINE

Module I: Global Digital Sovereignty

a. Information Warfare - Cyber Warfare - Cyber Terrorism - Cyber Operations and Jus ad Bellum - The "Interstate" Dimension of Cyber Operations - Cyber Operations as "Armed Attacks" - Article 51 of UN Charter
b. Cyber Attacks as "Force" under Article 2(4) of UN Charter - Worldwide Cyber Attack Cases - Experian Breach case - Cognizant Technology Solutions Corp case - Australian Broadcaster - Channel Nine case
c. Cyber Attack on World Health Organization (WHO) - 25,000 email addresses and passwords stolen - its impact - Zoom App - Zoom bombing case
d. Cyber Attacks targeting Education Sector - University of the Highlands and Islands - California University case

Module II: International Scenario of Cyber Legislation

a. International law on Cyberspace - Existing Challenges on International Law and Governance on Cyberspace - Jurisdictional Challenges

b. International legal framework for combating cybercrime - Budapest convention on cybercrime - The OECD Global Forum on Digital Security - North Atlantic Treaty Organisation NATO on Cyber Attacks carried by countries against NATO members - NATO & EU on Cyber defence
c. Asia Pacific Economic Cooperation (APEC) - The Global Cyber-Security Agenda of the International Telecommunication Union - Shanghai Cooperation Organization - Cyber Sovereignty of China and Soviet countries
d. Cyber Operations and UN Security Council Enforcement - maintenance of international peace and security - ICJ on Cyber Operations and the Law of Neutrality

Module III: International Legal Frameworks for Combating Cyber Crime

a. Virtual Global Task Force - Society for the Policing of Cyberspace - Protecting Children in Cyber Space
b. The UNODC perspective - UNODC Global Programme on Cybercrime - UNODC Cybercrime Repository
c. Convention on Cybercrime - Budapest Convention - Council of Europe Convention on Cybercrime: benchmark of international standards

Module IV: Online Dispute Resolution in Cyber Crimes (ODR)

a. History of Online Dispute Resolution - Online Negotiation - Online Mediation - Online Arbitration - ODR vs Litigation
b. Cybersecurity in Online Dispute Resolution - Advantages of Cyber-Mediation - Cost Savings and Convenience - Avoidance of Complex Jurisdiction Issues
c. Disadvantages of Cyber-Mediation - Limited Range of Disputes - Potentially Inaccessible -

Limited Access - Concern over Confidentiality - The eBay ODR Experiment Case

d. Traditional Mediation vs Cyber-Mediation Using Software and a Neutral Third-Party Facilitator - Future of ODR

Module V: Cyber Crimes and International Economy

a. Ransomware - Attacks on Cryptocurrency Exchanges - Bitcoin - United States v. Ross William Ulbricht
b. Cyber Attacks and its impact on Economy to an organization - Insider Attacks - Social Sites - Cybercrime-as-a-Service (CaaS) - loss of IP and business - confidential information - Net extortion

c. IP Theft - Cyber Espionage and International Economy - Cyber Insurance

Module VI: Social Impact on Global Cyber Crimes

a. Cyber Crime & Society - Cyber pornography impacts on younger adults - Cyber-bullying and Phycological impact
b. Cyber Violence against Women - Crime against Privacy - Cyber Victimization
c. Cyber Crimes on social media - Its Impact

Module VII: Cyber Diplomacy and Defensive Mechanism

a. Cyber Diplomacy - Cyber Ethics - EU's approach to Cyber diplomacy and Cyber defence
b. Uniform implementation of basic security measures - Investment in defensive technologies
c. ITU, ICANN, and Internet Governance Forum - governing fundamental norms, principles, and operationalities of cyberspace - Increased cooperation among international law enforcement agencies - Harmonization of legislation and guidelines

Module VIII: International Human Rights on Cyber Space

a. Online speech and Freedom of Expression - UN Human Rights Council
b. Right to Privacy - Article 17 of the International Covenant on Civil and Political Rights (ICCPR) - Riley v. California - warrant for searching cell phones
c. Cyber Racism - Freedom from discrimination - Art 2 of UDHR - Art. 26 of ICCPR - Gender- based interpersonal cybercrime - UN Office of the High Commissioner for Human Rights

BIBLIOGRAPHY

RECOMMENDED READING:

BOOKS

1. Prof. Dr. Marco Gercke, “Understanding cybercrime: Phenomena, challenges and legal response”, 2012
2. Barney, Prometheus Wired: The Hope for Democracy in the Age of Network Technology, 2001
3. Nils Melzer “ Cyberwarfare and International Law”, 2011

4. Esther van den Heuvel , “ONLINE DISPUTE RESOLUTION AS A SOLUTION TO CROSS-BORDER E-DISPUTES AN INTRODUCTION TO ODR”
5. E. Katsh, J. Rifkin and A. Gaitenby, E-Commerce, E-Disputes and E-Dispute Resolution: In the Shadow of “eBay Law”, 2000

FURTHER READING:

1. WIPO Reading Material on Intellectual Property, WIPO, Geneva
2. Mukul Vermai, “Are Laws Pertaining to Cyber Crimes in India Sufficient in the Current Scenario”, International Journal of Law Management & Humanities, 2021
3. Ajayi, “Challenges to enforcement of cyber-crimes laws and policy”, E. F. G. School of Law, Kenyatta University, Nairobi, Kenya, 2016
4. The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006
5. Hetram yadav and Shashant Gour, “Cyber Attacks: An impact on Economy to an organization”, 2014
6. Mueller, M., “Will the Internet fragment? Sovereignty, globalization and cyberspace.”, Cambridge, UK: Polity Press, 2017

LEARNING OUTCOME

After completion of the course students will be able to –

- *Understand the different dimensions of cyber issues and legislations.*
- *Know the role of International Organizations and Conventions in combating cybercrimes.*
- *Examine various doctrines and precedents in resolving the emerging disputes.*
- *Understand the global framework of cyber law and its implications across the nations.*
- *Explore futuristic issues and the need for robust law mechanism to meet the changes.*

COURSE – V

CYBER CRIME IN INDIA

(HARD CORE COURSE - V)

OBJECTIVES OF THE COURSE:

Cybercrimes is recognised to be as one of the most important subject or part of Cyber law as we are visualising and realising many computer crimes in India and globally. The purpose of cybercrime related legislations is mainly to protect the internet users from the hands of cyber criminals who could potentially spoil the fruits of cyber space technology. It is generally allied with the analysis of computer forensics and digital evidence in criminal proceedings. Evidence composed from cyber forensic analysis is typically subjected to similar procedures and performs as supplementary digital evidence. With these developments it is pertinent to study and also update the dynamic changes in cybercrimes happening in India.

With this objective the course is designed to

- *Equip the students with understanding of criminal activities in cyberspace*
- *To encounter students with the regulatory regime cybercrimes;*
- *Increase knowledge on investigation of cyber offenses and online frauds and combating procedures.*
- *Develop Proficiency in various techniques to mitigate the complexities associated with cyber threats.*
- *Understand the impact of cybercrimes in our society*
- *Explore professional career prospects in the field of cyber crimes*
- *Recognize the need for amendments, polices to combat and prevent cyber crimes*

COURSE OUTLINE

Module I: Meaning and Nature of Cyber Crimes

a. Evolution of Cyber Crimes - Meaning of Cyber Crimes - types of Computer Crimes
b. Cyber Criminology and victimology - Theories in cyberspace and cybercrimes
c. Cybercrimes and Traditional Crimes

Module II: Cybercrime's offences

a. Online based Cyber Crimes - Phishing and its Variants - Web Spoofing and E-mail Spoofing

b. Cyber Stalking - Web defacement - Financial Crimes - ATM and Card Crimes - Spamming - Commercial espionage - Commercial Extortion online - Money Laundering - Software and Hardware Piracy
c. Cyber Terrorism - Online Sale of Drugs - Online Sale of Arms - Crime-as-a-Service (C-aa-S) - Ransomware - Criminal misuse of Data - Cyber-attack on Core Banking System - Dark Net Crime
d. Obscenity in electronic form& child pornography in cyberspace

Module III: Jurisdiction and Legislative Issues in Cyber crimes

a. Section 75 of Information Technology Act ,2000 - Section 178 & 179 of Code of Criminal Procedure, 1973
b. Section 65B (4) of Indian Evidence Act 1872 - Convergence of I.T. Act & Indian Penal Code
c. Contradiction in applicability of other legislations and I.T.Act for Cybercrimes - Adjudication of Offences (Cybercrimes) under I.T. Act, 2000 - Adjudication - E Courts (Electronic courts) - Online Dispute Resolution (ODR)
d. Cross Border Investigations - Cyber Conflict Investigations

Module IV: Implementation and enforcement issues in cyberspace

a. Territorial issues - Doctrine of Extraterritoriality - Technological Constraints in Policing and Investigations
b. Digital Evidence and Cybercrimes - Growth of Cyber Forensics
c. Legal Issues and Court Room Skills - Constraints in Search and Forensics

Module V: Latest Trends in Cybercrimes Jurisprudence

a. Women - Children - Vulnerable targets – Recent legal developments
b. Techno legal perspectives of cybercrimes - Need for Risk Assessment and Vulnerability test
c. Need for Cybercrime possibility awareness in technologies - IP and Cybercrimes
d. Cyber Forensics - Tools and Targets

Module VI: ISP liability and Cyber crime

a. Primary and Secondary Liability - Theories related to liability in Cyber Crime

b. Principle of due diligence - Techno Legal Constraints in the applicability of Safe Harbour
c. Notice & Take-down principle - ISP liability-global model - ISP liability-perspective of I.T. Act, 2000

BIBLIOGRAPHY

RECOMMENDED READING:

BOOKS

1. NandanKamath, Law Relating to Computers, Internet and E-commerce, Universal Publication ,4th edition 2009.
2. Rodney Ryder, Cyber Laws, Wadhawa Publication (2008)
3. UNICITRAL MODEL LAW (1996).
4. Vakul Sharma, Information Technology Law and Practice, Universal Law Publicaiton, 3rdedition (2012)
5. Russel g. Smith, Peter Grabosky&GregorUrbas: Cyber criminals on Trial, Cambridge University Press, 2011
6. Nina Godebole, SumitBelapure, Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, 2011
7. Bill Nelson, Amelia Phillips, Frank Enfinger, and Christopher Steuart, Guide to Computer Forensics and Investigation, 2nd Edition

FURTHER READING:

1. Andrew Murray, Information Technology Law: Law & Society, Oxford University Press, 2010
2. PavanDuggal, Mobile Law, Universal Law Publishing Co. 2011
3. Michal D. Scott, Scott on Information Technology Law, 3rd ed., (Volume I & II), Wolters&KluwerPublications
4. Russel g. Smith, Peter Grabosky&GregorUrbas: Cyber criminals on Trial, CambridgeUniversity Press, 2011
5. Diane Ronald & Elizabeth MacDonald: Information Technology Law, Cavendish Publishing Limited, 1997

JOURNALS / ARTICLES

1. Ashok Wadje, Obscenity in Electronic Form: Exploration of Regulations, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2196473
2. Cyber Crime and Cyber Law in India: An Analysis by PrabhashDalei and TannyaBrahme. Available at: http://psrcentre.org/images/extraimages/IJHAS024054.pdf
3. Cyber Laws by Karnika Seth, Annual Survey of Indian law, Indian Law Institute Publication,2011
4. Joel P. Trachtman, Cyberspace, Modernism, Jurisdiction and Sovereignty. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=91668
5. IT Act 2000 vs 2008- Implementation, Challenges, and the Role of Adjudicating Officers by Karnika Seth. Available at: http://www.karnikaseth.com/publications
6. Information Technology (Amendment) Act, 2008: A new vision through a new change, by VikasAsawat. Available at: http://ssrn.com/abstract=1680152
7. Evolving strategies for the enforcement cyber laws by Adv. Karnika Seth, High Level ConsultationMeeting for formulation of a National Policy and Action plan for Enforcement of Cyberlaw , New Delhi on 31, Jan 2010 Available at: http://www.karnikaseth.com/publications
8. Vijay Kumar Singh, Role played by Police Authorities in prosecution of offences under theInformation Technology Act-A need for reform, Indian Bar Review, Vol. XXXI (1 & 2) 2004
9. Cyber Laws by Karnika Seth, Annual Survey of Indian law, Indian Law Institute Publication,2011
10. Cyber Laws, by Yatinder Singh J., Journal of Indian Law Institute, Vol. 44 2002.

LEARNING OUTCOME

After completion of the course students will be able to

- *Develop strategy, policy, advocacy in cybercrimes related technology and regulations.*
- *Develop and grow as cybercrime experts in corporations, law firms, and companies*
- *Expertise as forensically sound in legal matters in various courts.*
- *Analyse and Apply knowledge of electronic data during investigation and examination in legal matters.*

COURSE – VI

COMPUTER FORENSICS

(Hard Core Course - VI)

OBJECTIVES OF THE COURSE:

Cyber forensics, also known as computer forensics, which is a subdivision of digital forensic science, relating to evidence detection in computers and digital storage media. The purpose of cyber forensics is the forensically-sound investigation of digital media with the intent to: identify, preserve, recover, analyze, present facts, and opinions; concerning the digital information. Even though it is generally allied with the analysis of cyber-based crimes, computer forensics may also be used in civil proceedings. Evidence composed from cyber forensic analysis is typically subjected to similar procedures and performs as supplementary digital evidence. With these advancements, it was desired that cyber forensics be to protect users and remain citizen-centric.

With this objective the course is designed to

- *Expertise with the knowledge on investigation of cyber offenses and online frauds and combating procedures.*
- *Proficiency in various techniques to mitigate the complexities associated with cyber threats.*
- *Understand the impact of cyber forensics in societal development.*
- *Explore professional career prospects in the field of cyber forensics*
- *Recognize the new policy regulations in the nation which focuses on cyber forensics and its development*

COURSE OUTLINE

Module I: Artificial Intelligence and Law

a. Evolution of Cyber Forensics - Introduction to Cyber Forensics - Overview of types of Computer Forensics
b. Network Forensics - Mobile Forensics, and E-mail Forensics - Cloud Forensics - Database Forensics - Services offered by Digital Forensics - Role of First Responder
c. Identity Management Security Systems - Identity Theft - Biometric Security Systems

Module II: Cyber Forensics and Computer Crimes

a. Online based Cyber Crimes - Phishing and its Variants - Web Spoofing and E-mail Spoofing
b. Cyber Stalking - Web defacement - Financial Crimes - ATM and Card Crimes - Spamming - Commercial espionage - Commercial Extortion online - Money Laundering - Software and Hardware Piracy
c. Cyber Terrorism - Online Sale of Drugs - Online Sale of Arms - Crime-as-a-Service (C-aa-S)

- Ransomware - Criminal misuse of Data - Cyber-attack on Core Banking System - Dark Net Crime

Module III: Cyber Forensics - Evidentiary Aspects from Techno - Legal Perspective

a. Extraction of Evidence - Examination - Organisation of Evidence - Admissibility of Forensic Evidence In Digital Format In A Legal Court In India - In Shafi Mohammad v. The State of Himachal Pradesh - Twentieth century Film Fox Corporation v. NRI Film Production Association (Pvt) Ltd.
b. Cyber Forensics Investigation - Managing the Digital Crime Scene - Data Recovery - Role of the Computer Forensics Analyst in Court
c. Forensics in social media - Search and Seizure - Evidence in the form of e-mails, internet history, documents or other files related to crimes such as murder, kidnapping, fraud and drug trafficking
d. Role of Cyber Forensics in Intellectual Property Theft - Industrial Espionage - Internet Fraud - Electronic Forgery - Impediments in Cyber Forensic Investigation in India

Module IV: Jurisdiction on Cyber Forensics Arena

a. Section 75 of Information technology Act ,2000 - Section 178 & 179 of Code of Criminal Procedure, 1973 - Section 65B (4) of Indian Evidence Act 1872
b. SIL Import V. Exim Aides Silk Importers - Asahi metal industry co. v. Supreme court - Complexity in deciding the territorial jurisdiction of cyberspace as the user can access website at any place in the world
c. Adjudication - E Courts (Electronic courts) - Online Dispute Resolution (ODR)

Module V: Role of Cyber Security in India

a. Sec 66 - Information Technology (Amendment) Act, 2008 - NASSCOM - Data Security Council of India (DSCI))

b. Cyber Security Task Force - National E-Governance Plan (NeGP)
c. Role of CBI - Cyber Crimes Research and Development Unit (CCRDU) - Cyber Crime Investigation Cell (CCIC) - Cyber Forensics Laboratory - Network Monitoring Centre.
d. Need for uniformity in Cyber Security Control and Enforcement Practices - Dilipkumar Tulsidas v. Union of India

Module VI: International Approach towards Cyber Forensics

a. Role of Federal Bureau of Investigation (FBI), CIA, NSA, and GCHQ - Regional Computer Forensic Laboratory
b. Position in UK - The five-year National Cyber Security Strategy - Centre for the Protection of National Infrastructure (CPNI) - National Cyber Security Centre -
c. The International Society of Forensic Computer Examiners (ISFCE) - Cyberspace Regulations and Role of UN
d. Council of Europe's Convention on Cybercrime - Budapest Convention.

Module VII: Impact of Cyber Forensics in Society and Individual

a. Ethics of Cyber Forensics in India - Impact of Cybercrimes - To the Individual - Corporate and Companies - Government and the Nation
b. Right to Privacy in Cyber Forensics and Cyber Security - Data Theft - Constitutional Mandate - Aadhar Card Case - Justice K.S. Puttaswamy v Union of India

Module VIII: Growing Challenges and Future Paradigm in Cyber Forensics

a. Insufficient Cyber Forensic Laboratories - Lack of Cyber Crime Police Stations (CCPS) – Cyber Courts - Cyber Crime Investigation & Forensic Training Facilities - Centres of Excellence in Cyber Forensic in all major cities
b. Absence of universally coherent accepted guidelines in digital forensics
c. Legal and Judicial Reforms - Proposal of National Litigation Policy of India (NLPI)

BIBLIOGRAPHY

RECOMMENDED READING:

BOOKS

1. Albert J. Marcella, “Computer Forensics : A Field Manual for Cancelling, Examining, and Preserving Evidence of Computer Crimes”

2. V.R. Dinkar, Scientific Expert Evidence,-determining the probative value and admissibility in the courtroom, Eastern Law House, 2013
3. S.K. Verma& Raman Mittal eds. 2004, Dimensions of Cyber Space, Indian Law Institute Legal
4. Andrew Murray, Information Technology Law: Law & Society, Oxford University Press, 2010
5. Russel g. Smith, Peter Grabosky&GregorUrbas: Cyber criminals on Trial, Cambridge University Press, 2011
6. Nina Godebole, SumitBelapure, Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, 2011
7. Bill Nelson, Amelia Phillips, Frank Enfinger, and Christopher Steuart, Guide to Computer Forensics and Investigation, 2nd Edition

FURTHER READING:

1. Maras, M. (2015). Computer forensics: Cybercriminals, laws, and evidence. (2nd ed). Burlington, MA: Jones & Bartlett Learning.
2. Bill Nelson, Amelia Phillips and Christopher Steuart; "Guide to Computer Forensics and Investigations", 2010
3. John R. Vacca, "Computer Forensics - Computer Crime Scene Investigation, Second Edition"
4. Debra Littlejohn Shinder, "Scene of the Cybercrime" Computer Forensics Handbook, 2002
5. Broadhurst, R. G, "Developments in the global law enforcement of cyber-crime. Policing: an International Journal of Police Strategies and Management", 2006, 29(3), 408-433
6. Dr. Anjani Singh Tomar, "Cyber Forensics in Combating Cyber Crimes", 2014
7. Shrivastava, Gulshan & Sharma, Kavita & Khari, Manju & Zohora, Syeda, "Role of Cyber Security and Cyber Forensics in India", 2018

JOURNALS / ARTICLES

1. Kirankumar Akate Patil, Shrinivas Vyawahare, Kiran Shejul, Madhuri Girase, " Hurdles in Cyber Forensic Investigation in India", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, PP 18-21

2. Dubey V. Admissibility of electronic evidence: an Indian perspective. Forensic Res Criminol Int J. 2017;4(2):58-63
3. Dr. Sudhir Kumar Sharma, "Cyber Security: A Legal Perspective", International Journal of Computer and Internet Security. ISSN 0974-2247 Volume 9, Number 1 (2017), pp. 1-11 © International Research Publication House
4. Nilima Prakash, Dr. Roshni Duhan, "COMPUTER FORENSIC INVESTIGATION PROCESS AND JUDICIAL RESPONSE TO THE DIGITAL EVIDENCE IN INDIA IN LIGHT OF RULE OF BEST EVIDENCE", International Journal in Management and Social Science Volume 08 Issue 05, May 2020 ISSN: 2321-1784

LEARNING OUTCOME

After completion of the course students will be able to

- *Play roles in strategy, policy, advocacy, and legal advisory and litigation roles for businesses, individuals, and organisations that depend upon technology.*
- *Develop and grow as digital forensic experts in corporations, law firms, insurance agencies, and law enforcement organisations.*
- *Expertise as forensically sound in legal matters across the nation.*
- *Analyse and Apply knowledge of electronic data during investigation and examination in legal matters.*
- *Explore and research the new advancements of Cyber Forensic Policies and career prospects across the world*

COURSE – VII

DIGITAL EVIDENCE

(DISCIPLINE ELECTIVE COURSE - I)

OBJECTIVES OF THE COURSE:

Digital evidence as a form of physical evidence creates several challenges for forensic examiners. It's a different form of evidence that can be difficult to handle. On the other hand, fortunately digital evidence has several features that mitigate the problem technically and legally.

With this objective the course is designed to

- *Identify and correctly define the instances for the application of computer forensics - digital evidence*
- *To understand the laws and ethics by which digital evidence is governed in our country and worldwide.*
- *Consider the role of the regulating bodies in identification and application of digital evidence*
- *Understand and evaluate how these cyber forensics impacts the financial and other legislation*

COURSE OUTLINE

Module I: Digital Evidence - Nature and Source

a. Sources - Standards for Collecting and Handling Digital Evidence
b. Presentation - Admissibility of Digital Evidence in Court
c. Integrity, Discovery, and Disclosure of Digital Evidence
d. Constitutional Validity - The Nature and Challenges of Digital Evidence

Module II: Digital Evidence - Indian Perspective

a. Law relating to Digital Evidence in India - Electronic Evidence and the Indian Evidence Act 1872 - Amendments in Evidence Act - Sec 2A - Sec 2(3) - Changes in the Banker's Book Evidence Act, 1891
b. Sec 172 - 175 - Sec 463 - Sec 465 - Changes in Indian Penal Code, 1860 - 45 A - Information Technology Act, 2000 - Section 79A of the IT(Amendment) Act, 2008

c. Recent rulings of Indian courts on Digital Evidence - State of Punjab v. Amritsar Beverages Ltd - Evidence recorded on to CD In the case of Jagjit Singh v. State of Haryana (2006) - Parliament Attack Case
d. Admissibility of intercepted telephone calls - The case of State (NCT of Delhi) v. Navjot Sandhu, (2005) - whether a hard disk of a computer can be considered as documentary Evidence - Dharambir Vs. CBI - Call Records: In Rakesh Kumar and Ors. Vs. State
e. Examination of a witness by Video Conference - The State of Maharashtra v. Dr. Praful B Desai, 2003

Module III: Electronic Evidence and the Indian Supreme Court

a. Som Prakash vs. State of Delhi - Admissibility of Electronic Evidence - State vs. Mohd. Afzal And Ors
b. Anvar vs. Basheer - Section 65B of the Evidence Act - special provision governs digital evidence - 'lex specialis derogat legi generali'
c. Ratan Tata v. Union of India - CD containing intercepted telephone calls was introduced in the Supreme Court without following the procedure laid down under section 65B of the Evidence Act

Module IV: Digital Evidence and Cloud Forensics - Comparative Study

a. Digital Forensic Investigation - Digital Evidence in the Cloud - The Emergence of Cloud Storage - Existing Legal Frameworks for Capturing Digital Evidence in the Cloud - Legal Challenges for Cloud Forensics
b. The USA Legal Framework - Microsoft Ireland case.
c. European Legal Framework - The Group of Eight (G8) - Principles on Transborder Access to Stored Computer Data - Principles on Accessing Data Stored in a Foreign State
d. Law Enforcement Authorities - Co-operation with service providers

Module V: IT ACT 2000 & ADMINISTRATIVE IMPLICATIONS

a. Digital Signature Certificates - Securing Electronic records - Duties of Subscribers - Role of Certifying Authorities - Regulators under the Act
b. The Cyber Regulations Appellate Tribunal - Internet Service Providers and their Liability - Powers of Police under the Act - Impact of the Act on other Laws
c. E -Taxation issues - E - Contract issues and Digital Evidence

d. Financial Amendments and Digital Evidence - Income-tax Act, 1961 - Finance Act, 2001 - Finance Act, 2002 Finance Act, 2009 - Reserve Bank of India Act, 1934

Module VI: Digital Evidence Legislation on Major Countries - The Comparison

a. United States: Uniform Electronic Transactions Act, 1999 - United Kingdom: Electronic Communications Act 2000 - UK Electronic Signatures Regulation 2002
b. Canada - Personal Information Protection and Electronic Documents Act, (PIPEDA), 2004
c. Australia - Electronic Transactions Act 1999 - European Union: European Directive 199/93/EC on Digital Signature laws
d. South Africa - Electronic Communications Act, 2005

Module VII: Digital Evidence - International Scenario

a. Article 1 - Section 3.1.1 of the Budapest Convention on Cybercrime
b. Power of Disposal - United Nations Commission on International Trade Law (UNCITRAL) model Law on Digital Evidence
c. Legal Standard of Admissibility of Evidence - In Purview of International Criminal Court (ICC) - Rule 69(4) of the ICC Rules of Procedure and Evidence - Probative Value & Evidentiary Weight of Evidence - The Bemba Case
d. Evidentiary Considerations of Digital Evidence - Prosecutor v. Bagosora

Module VIII: Digital Evidence - The Challenges Ahead

a. Old procedural guarantees vs. new digital evidence processes
b. Unaddressed threats to fairness and the presumption of innocence - Inappropriate use of poorly tested technology undermines the right to a fair trial
c. Difficulties in Search and seizure of Physical Evidence vs. Digital Evidence
d. The sanctity and relevance of Digital Evidence - The Retrieval Mechanism: Physical vs. Logical - Reliability Crisis in Digital Forensics

BIBLIOGRAPHY

RECOMMENDED READING:

BOOKS

1. Tejas D. Karia, “Admissibility of Digital Evidence”, 2007

2. Stephen Mason and Andrew Sheldon, Proof: “The investigation, collection and examination of digital evidence, in Electronic Evidence”, LexisNexis, 2013.
3. Christos Karagiannis and Kostas Vergidis, “Digital Evidence and Cloud Forensics: Contemporary Legal Challenges and the Power of Disposal”, 2021
4. Vivek Dubey, “Admissibility of electronic evidence: an Indian perspective” , 2017
5. Radina Stoykovaa, “Digital evidence: Unaddressed threats to fairness and the presumption of innocence”, 2021

FURTHER READING:

1. J. Hofman, “Electronic Evidence in Criminal Cases”, 2006
2. Paul, George L. “CANVASSING THE EMERGING LAW OF DIGITAL INFORMATION: STEPHEN MASON'S”, ELECTRONIC EVIDENCE”, 2017
3. E. Casey, “Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet”, 2011
4. An Overview of the Use of Digital Evidence in International Criminal Courts’ (Salzburg Workshop on Cyber Investigations), 2013
5. G. Kessler, “Judges Awareness, Understanding, and Application of Digital Evidence”, 2011

LEARNING OUTCOME

After completion of the course students will be able to

- *Understand the Nature of Electronic Information and the devices and software used to create, store, retrieve and present it.*
- *Understand and discuss the legislation governing Digital Evidence and its impact in the society*
- *Critically interpret the shortcomings of the legislation and the need for new changes*
- *Increase the proficiency in analysing digital evidence admissibility issues and the cases concerned*
- *Gain clarity of how evidentiary issues are affected when material is in an electronic form and current updated changes across the globe.*

COURSE – VIII

TRANSNATIONAL CYBERCRIMES

(Discipline Elective Course - II)

OBJECTIVES OF THE COURSE:

Today in the epoch of technology, all aspects of a life including professional, personal, finance & educational are gravitating towards digitalization. Because of this heavy dependency on computers and other similar computing devices and networks, we store and transmit profuse data on regular basis which creates the aspect of cyberspace which is more vulnerable to cyber-attacks. This course explains Transnational Cybercrimes and the need for Cyber Security in a robust manner.

With this objective the course is designed to

- *Identify the emerging legal issues in a digital networked environment including issues of jurisdiction and enforcement of rights and liabilities in cyberspace*
- *Consider the role of the regulating bodies in identifying and combating transnational cybercrimes.*
- *Identify and analyse recent developments in national and global law-making policies of cybercrimes*
- *Understand and evaluate how these developing concepts affect the flow of information in society and the techno legal framework for regulating the crimes.*

COURSE OUTLINE

Module I: The Transnational Nature of Cyber Crime

a. The Global Landscape of Cybersecurity - "Lex loci delicti" rule - Cybercrimes - Extraterritorial aspects
b. Cybercrime regulation challenges - State and Transnational laws versus Global laws

Module II: Transnational Cyber Crimes - Jurisdictional Framework

a. Jurisdiction - Cause of Action - Legislative Enforcement - Adjudicative Jurisdiction
b. Indian Context of Jurisdiction - International position of Jurisdiction in Cybercrimes - Internet Jurisdiction
c. Overcoming Jurisdictional Challenges - Foreign Judgments - The need for a global response to a multi-jurisdictional crime - Dispute Settlement - Victim Management

Module III: Cyber Crimes Scenario in India

a. Cyber Digital Piracy - Nation's Piracy - Funding transnational organized crime networks trade in counterfeit and pirated products
b. Sony. Sambandh.com case- 1st cybercrime conviction in India - The Bank NSP Case – Satya v. Teja Singh
c. Cyber Defamation - SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra - Google India Pvt. Ltd. vs. Visaka Industries Limited
d. Dangerous Offenders and Vulnerable Victims - Disparities in National Laws of Protection and Cooperation

Module IV: Cyber Terrorism, Hacktivism and National Security

a. The Transnational Dimension of Cyber Terrorism - Nation's security - Hacktivism - Use of Internet for Anti-Social Activities - Parliament Attack Case
b. Affecting Trust - Cyber War - Internet - Offensive Information Warfare - State-Sponsorship to Cyber Terrorism
c. Cyber Policing - Role of Interpol - Utilization of INTERPOL - Cybercrime Collaborative Platform
d. National Computer Emergency Response Teams (CERTs) - Implementation of Prevention Measures and Awareness

Module V: Cyber Theft of Intellectual Property

a. Transnational Cybercrime Groups vs Exploitation of Intellectual Property Protection Trademark Counterfeiting - Casio India Co. Ltd. v. Ashita Tele Systems Pvt. Ltd - Theft of Trade Secrets
b. Cyber Piracy - Copyright Violations - Impact on Education and Economy
c. Harmonization of Intellectual Property Laws with Organized Cyber Crime Laws - Within a Single Nation

Module VI: Financial Transnational Cybercrime and Narco -Terrorism

a. Corruption - Money Laundering - Threat to the Economy - Nation's Competitiveness - Strategic Market
b. Narco - Trafficking - Narco Terrorism - Organized Cybercrimes related to Drugs – UNODC - Challenges to Social Stability - Need for robust techno - legal system

Module VII: International Law Implications on Transnational Cybercrimes

a. United Nations Human Rights Council's resolution - "The Promotion, Protection and Enjoyment of Human Rights on the Internet." - Role of the Internet in worldwide human rights protection - Concept of Dark Net
b. United Nations Convention Against Transnational Organized Crime (TOCC) - U.N. Office on Drugs and Crime (UNODC)
c. Regulation of the Internet and Net Neutrality - National government's responsibility on allowing their citizens free access to and use of the Internet - Responsibility of State
d. United Nations Security Council - Special Notices regarding terrorism

Module VIII: Cyber Security and Futuristic Challenges

a. Cyber Crimes and Covid Pandemic - Growing Human Trafficking - Building Enforcement Capacity - combating IP theft - training and technical assistance
b. Networks and Netwars - The Future of Terror, Crime, and Militancy
c. Technology and Terrorism - The New Threat for the Millennium - The Information Revolution and National Security
d. Cybercrime Epidemic - Not an IT issue - Impact on Society - Nation's Development - Nation's Privacy and Data Protection Laws

BIBLIOGRAPHY

RECOMMENDED READING:

BOOKS

1. Kshetri, N," Cybercrime and cybersecurity in the global south", 2013
2. Maureen Walterbach, "International Illicit Convergence: The Growing Problem of Transnational Organized Crime Groups Involvement in Intellectual Property Rights Violations", Florida State University Law Review, 2007
3. Justice Yatindra Singh, Cyber law 36(universal law publications, Delhi 6th edition 1998)
4. Mathew Collins, "The law of defamation and the internet" ,2001
5. Iblina Begum and H. K. Sharma, "Piracy: A threat to Academicians and Publishers", 2019

FURTHER READING:

1. Kshetri, N., & Dholakia, N, "Professional and trade associations in a nascent and formative sector of a developing economy: a case study of the NASSCOM effect on the Indian offshoring industry. Journal of International Management", 2009
2. B.Swaathi and M.kannapan, "Cybercrime an Indian Scenario" 2010
3. Castells Manuel, "The Internet Galaxy: Reflections on the Internet, Business and Society" (Oxford University Press 2003)
4. Cybercrime, Cyberterrorism, Cyberwarfare: Averting an Electronic Waterloo, Center for Strategic and International Studies, Bristish Library
5. Michael Erbschloe, "Information Warfare: How to Survive Cyber Attacks", New York. London, 2001

LEARNING OUTCOME

After completion of the course students will be able to –

- *Identify and analyse challenges of a theoretical and practical nature regarding the legal response to transnational cybercrime.*
- *Understand and discuss the limits of the law regarding transnational cybercrime and post- conflict situations.*
- *Independently and critically interpret and apply relevant sources of cyber legislation in India*
- *Examine various doctrines and precedents in resolving the emerging disputes.*
- *Understand and reflect on social dilemmas that may arise in the field of transnational cybercrimes and deal with these in a responsible and comprehensive manner.*

COURSE – IX

CYBERSPACE AND TELECOMMUNICATION: LEGAL AND SECURITY ISSUES

(Discipline Elective - III)

OBJECTIVES OF THE COURSE:

The impact of cyberspace is found in many technologies and sectors but the most widely affected sector is telecommunication industry as the use if IT in this sector is more widely dominant. The need for studying the convergence and interrelationship between the telecom industry law and cyberspace has become pertinent to specialise and update.

With this objective the course is designed to

- *To provide an overview of legal and security aspects of Telecom Sector and Cyberspace*
- *To understand the intricacies of legislative perspectives of telecom sector regulations and Information technology law*
- *To understand the forensic and evidentiary issues in Telecom related cybercrimes.*

COURSE OUTLINE

Module I: Introduction to Cyberspace and Telecommunication

a. Growth and Development of Digital telecommunications
b. Telecommunication network and Law
c. Electromagnetic Spectrum
d. PSTN and ISDN

Module II: Legislations related to Technology Sector

a. Information Technology law and Telecom Sector - Cellular & Mobile Services, Internet Services, Communication Outsourcing - Historical Evolution of Telecommunication Law and Policy
b. Telecommunication Policy of India, Regulatory Framework for Spectrum Management - Indian Telegraph Act
c. Indian Wireless Telegraphy Act - TRAI

Module III: Telecommunication Legal and Regulatory Issues

a. Telecom Commission - Data Protection in Telecom sector
b. Content Regulation in Telecom sector - Online Media Regulations

c. Telecom Dispute Settlement and Appellate Tribunal - Licensing and Assignment
d. Competition Law in Telecommunication - Telecommunication & IP issues

Module IV: International Legal Perspectives

a. Telecom Law in different jurisdictions - International Telecommunications Law in US and UK
b. International Organizations and Telecom Regulations - World Trade Organization
c. International Dispute Resolution in online Telecom Sector - ADR and ODR

Module V: Online Telecommunications and Cybercrimes

a. Types of Telecommunications related Cybercrimes - Indian Penal Code and Telecommunication Crimes
b. IT Act and Telecommunications crimes
c. Legislative perspectives of Telecommunication Crimes
d. Judicial approach towards Telecommunication Crimes

BIBLIOGRAPHY

RECOMMENDED READING:

BOOKS

1. TDSAT. Telecom Broadcasting and Cable Laws. TDSAT, 2008.
2. Dev. or Robert K. Bell and Neil Ray, "Telecommunications Regulation Handbook. EU Electronic Communications Law". Richmond Law & Tax Ltd., UK. 2004.
3. Bomil Suh, Ingoo Han, "The Impact of Customer Trust and Perception of Security Control on the Acceptance of Electronic Commerce, International Journal of Electronic Commerce", Vol. 7, No. 3 (Spring, 2003)
4. FIDLER, D.P., 'Internet Governance and International Law: The Controversy Concerning Revision of the International Telecommunication Regulations', ASIL Insights (7 February 2013).
5. HOLLIS, D.B, "Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack?", in J.D. Ohlin et al. (eds.), Cyber War: Law and Ethics for Virtual Conflicts, 2015

FURTHER READING:

1. EICHENSEHR, K.E., 'Data Extraterritoriality', 95 Texas Law Review (2017)

2. Aleksandar Risteski, Mitko Bogdanoski, Marjan Stoilkovski and Miroslav Jovanovic, “Cyber Security Issues of Telecommunication Infrastructure”
3. Short, J., Williams, E., & Christie, B. (1976). The social psychology of telecommunication. London, England: John Wiley.
4. Rice, R.E. (1987). Computer-mediated communication and organizational innovation. Journal of Communication. 37. 65-94
5. Rice, R.E. & Love, G. (1987). Electonric emotion: Socioemotional content in a computer Mediated communication network. Communication Research. 14. 85-108.

LEARNING OUTCOME

After completion of the course students will be able to –

- *Become an expert in the areas of law related to convergence of Cyberspace and Telecom sector*
- *To become a lawyer in telecom corporates for resolving issues in online scenario*
- *To practice in courts in cases related to telecom sector in online scenario.*
- *Explore and research the new advancements of online telecom Policies and career prospects across the world*

COURSE – X

E-COMMERCE AND CONSUMER PROTECTION

(Elective Course - I)

OBJECTIVES OF THE COURSE:

With the advent of internet, we have undergone a revolutionary change in the business transactions and communications, which led to an astounding growth to the fields of e-commerce and web advertising. Apart from general e-disputes that arise by the acts or omission in the internet world, the parties to the e-contract may face different kinds of complex disputes. Consumer Protection Act identifies right to redressal as a significant consumer right based on which the three tier Redressal system has been established. This Course is designed to understand the significance and emerging need of consumer awareness in the globalised world. The course aims to give an insight into the concepts of e-commerce, its non-territorial nature towards consumer protection in the territorial based grievance redressal mechanism and explains on the existing legal and regulatory framework on consumer protection and discusses on the important challenge of determination of jurisdiction in the cyber world with various tests and principles along with International Conventions.

With this objective the course is designed to:

- *Understand the Concepts of E-Commerce and to have a comprehensive understanding of the Evolution of Consumer Protection Laws in India*
- *To give an Overview of Legal and Regulatory Framework on Consumers Protection in India To understand the working and functioning of Grievance Redressal mechanism To give an insight into the challenges faced by the e-consumers*
- *To discuss on the International and Indian legal framework on determination of jurisdiction in internet contracts.*

COURSE OUTLINE

MODULE I CONCEPTUAL FRAMEWORK

Consumer and Markets; Globalization – E-Commerce – Categories: Electronic Markets, Electronic Data Interchange, Internet Commerce – Business Models – Based on Transaction Type, Based on Party Type – B2B, B2C, C2B, C2C, E-Governance; Consumerism to E- Consumerism

MODULE II EVOLUTION OF E-COMMERCE AND CONSUMER PROTECTION LAWS IN INDIA

Internet and Advancement in Information and Technology – EDI – E-Commerce; E-Contract a medium of E-Commerce transaction – Legal Provisions related to E-Contracts: Indian Contract Act, 1872, IT Act 2000 (2008), Indian Evidence Act,1872 – Modes for entering into E-Contract; UNCITRAL Model Law 1996 – Information Technology Act, 2000 (2008): Electronic Records, Electronic Signature and Digital Signature; Overview of Legal and Regulatory Framework on Consumers Protection in India before 1986; Consumer Protection Act - Amendments; Consumer Movements in India; National Consumer Helpline; Quality and Standardization

MODULE III E-COMMERCE AND CONSUMER PROTECTION

Consumers Rights; Specific provisions relating to B2C Model of E-Commerce in Consumer Protection Act 2019 – Express Definitions relating to Electronic transactions – Product Liability – Other key changes benefitting all Consumers: Territorial Jurisdiction, E-Complaints, Central Consumer Protection Authority, Endorser Liability, Unfair Contracts, Unfair Trade Practices, Mediation in consumer disputes; Consumer Protection (E-Commerce) Rules, 2020; Legal Metrology(Packaged Commodities) (Amendment) Rules, 2017; Foreign Exchange (Non-Debt Instrument) Rules, 2019; Information Technology (Intermediaries Guidelines) Rules, 2011

MODULE IV ORGANISATIONAL SET UP UNDER CONSUMER PROTECTION ACT

Advisory Bodies: Consumer Protection Councils at the Central, State and District Levels; Adjudicatory Bodies: District Forums, State Commissions, National Commission: Their Composition, Powers and Jurisdiction (Pecuniary and Territorial); Central Consumer Protection Authority; Mediation Cell; Grievance Against Misleading Advertisements (GAMA)

MODULE V GRIEVANCE REDRESSAL MECHANISM UNDER CPA, 2019

Who can file a complaint? Grounds of Filing a Complaint; Limitation Period; Procedures for filing and hearing of a complaint; Disposal of cases; Relief / Remedy; Temporary Injunction; Enforcement of Order; Appeal, frivolous and vexatious complaints; Offences and penalties.

MODULE VI CONTEMPORARY ISSUES OF E-CONSUMERS

E-Payment Mechanism: Threats and Protection; Legal Remedies for Breach of Contract including E-Contract; Identity Theft; Fraudulent websites; Phishing Websites

MODULE VII JURISDICTIONAL FRAMEWORK OF CONSUMER PROTECTION - INDIAN AND INTERNATIONAL PERSPECTIVE

Concept of Jurisdiction; The Principles of Conflict of Law; Jurisdictional Concept in Electronic Commerce: General Jurisdiction and Specific Personal Jurisdiction – Minimum Contacts Doctrine – Jurisdictional Concept of Active and Passive Websites – Zippo Sliding Scale Approach – Effects Doctrine; Jurisdiction Concept Under Civil Procedure Code 1908 and Indian Contract Act 1872 and Jurisdictional Issues Under IT Act 2000: Place of Formation of the Contract – Choice of Forum – Choice of Law;

International Conventions Relating to Jurisdictional Issues in Cyberspace: Brussels Regulation 2002 – Convention on the Law Applicable to Contractual Obligations – Rome Convention 1980 – Hague Convention – Hague Convention on Choice of Court Agreement – 2019 Convention on the Recognition and Enforcement of Foreign Judgments in Civil or Commercial Matters

BIBLIOGRAPHY

RECOMMENDED READING:

BOOKS

1. Karnika Seth, "Computers Internet and New Technology Laws" (LexisNexis Butterworths Wadhwa, Nagpur 1st edn., 2012).
2. Chris Reed, "Internet Law Text and Materials" (Universal Law Publishing Co, 2nd edn., 2004). Dr. V.K.Agarwal, "Consumer Protection" (Bharat, 6th Edition, 2008)
3. Majumdar.P.K. & Kataria.R.P. "Law of Consumer Protection in India" (Orient Publishing Company, New Delhi, 9th edn., 2020).

JOURNALS / ARTICLES

1. Kulesza, Joanna, "Internet Governance and the Jurisdiction of States: Justification of the Need for an International Regulation of Cyberspace" III GigaNet Symposium Working Paper, (December 2, 2008) available at SSRN: http://papers.ssrn.com/sol3/papers.cfm?abstract_id= 1445452

2. Gaurang Kanth and Divjot Singh Bhatia “India: The Consumer Protection Act, 2019: An Overview” Mondaq, (Jan. 14, 2020) available at : https://www.mondaq.com/india/dodd-frank-consumer-protection-act/876600/the-consumer-protection- act-2019-an-overview
3. Dr. V.K. Agarwal, “Determination of complex issues under Consumer Protection Act: a question of jurisdiction” 3 Comp LJ 9 (2004).

FURTHER READING:

BOOKS

1. Khanna, Sri Ram, Savita Hanspal, Sheetal Kapoor, and H.K. Awasthi, “Consumer Affairs” (Universities Press, 2007)
2. Choudhary and Ram Naresh Prasad, “Consumer Protection Law Provisions and Procedure”(Deep and Deep Publications Pvt Ltd, 2005)
3. G. Ganesan and M. Sumathy, “Globalization and Consumerism: Issues and Challenges” (Regal Publications, 2012)
4. Suresh Misra and Sapna Chadah, “Consumer Protection in India: Issues and Concerns”(IIPA, New Delhi, 2012)
5. Pavan Duggal, “Cyber Law-The Indian Perspective” (Saakshar Law Publication, New Delhi, 2nd edn. 2004).
6. V.D. Dueja, “Crimes in Cyber Space: Scams and Frauds” (Commonwealth, 1st edn., 2003).

JOURNALS / ARTICLES

1. Misra Suresh, “Is the Indian Consumer Protected? One India One People (Aug 2017) Raman Mittal, Sonkar Sumit and Parineet Kaur, “Regulating Unfair Trade Practices: An Analysis of the Past and Present Indian Legislative Models” Journal of Consumer Policy (2016)
2. S.Chakravarthy, “MRTP Act metamorphoses into Competition Act” CUTS Institute for Regulation and Competition position paper (2014) available at www.cuts-international.org/doc01.doc
3. Kapoor Sheetal “Banking and the Consumer” Akademos ISSN 2231-0584 (2013)
4. K.N. Bhatt, Misra Suresh and Chadah Sapna “Consumer, Consumerism and Consumer Protection” Abhijeet Publications (2010)

5. Kapoor Sheetal, “Advertising - An Essential Part of Consumer’s Life - Its Legal and Ethical Aspects” Consumer Protection and Trade Practices Journal, October 2010
6. D.P.S.Verma, “Regulating Misleading Advertisements, Legal Provisions and Institutional Framework” Vikalpa. Vol. 26. No. 2. pp. 51-57, 2002

CASES FOR GUIDANCE

1. Abdul Manas.N.A v. Homeshop and The Professional Couriers CC No.11/4, Consumer Disputes Redressal Forum, Kasaragod.
2. Akarsh (In person) v. eBay India Pvt. Ltd., CC No. 410-2012, Disputes Redressal Forum Mysore
3. Asa Ram v. Bakshi (1920) ILR 1 Lah 203, 531 B31.
4. Banyan Tree Holding Pvt. Limited v. A. Murali Krishna Reddy 2010 (42) PTC 361 (Del)
5. Blackburn v. Walker Oriental Rug Galleries, E.D. Penn. 7 April 1998
6. Burger King Corp v. Rudzewicz 371 US 362 (1985, 372)
7. Calder v. Jones 365 US 783 (1983)
8. CompuServe Inc. v. Patterson 89 F. 3d 1257 (6th Cir. 1998)
9. Delhi State & District Consumer Courts Practitioner's Welfare Association (Regd.) v. Hon'ble Lt. Governor Govt. Of NCT Delhi and Ors., W.P. (C) 9458/2015, (Delhi High Court) (India)
10. Hakam Singh v Gammon (India) Limited, (1971) 1 SCC 286, AIR 1971 SC 740
11. International Shoe Co. v. Washington 326 U.S.310, 316(1945)
12. Jaideep Kaur v. Yatra Online Pvt. Ltd., and Another 388 CC No.174 of 2011, District Consumer Disputes Redressal Forum, Ludhiana
13. Lucknow Development Authority v. M.K. Gupta (1994) 1 SCC 243 (India)
14. M/s Afcons Infra Ltd. v. M/s Cherian Varkey Construction Company Ltd. and Others Civil Appeal No.6000 of 2010
15. Minnesota v. Granite Gate Resorts568 N.W.2d 715 (Minn. Ct.App.1997)
16. National Insurance Co. Ltd. v. Hindustan Safety Glass Works Ltd., (2017) 5 SCC 776 (India)
17. Nissan Motor Company Ltd. v. Nissan Computer Corporation 89 F Supp 2d 1153 (CD Cal 2000)
18. People v. World Interactive Gambling 1999 NY Misc Lexis 325 (Supp. Ct. N.Y.Co., 23th July 1999)

19. Perkins v. Benguet Consolidated Mining Company 332 US 337 (1952) 337
20. Rajinder Singh Chawla v. Makemytrip.com SCDRC Chandigarh, First Appeal 355/2013
21. Renaissance Hotel Holding Inc. v. Vihaya Sai and other 2010 (8) RCR Civil 1289
22. Sameer Karania v. Indiaplaza.com CC No.708/2012, I Additional District Consumer Disputes Redressal Forum Seshadripuram Bangalore
23. Siriram City Union Finance Corporation Limited v. Rama Mishra, (2002) 9 SCC 613; AIR 2002 SC 2402
24. Sonic Surgical v. National Insurance Company Ltd., (2009) CPJ 40(SC)
25. Sukhpreet Kaur v. Makemytrip.com CC No.396/2013, District Consumer Disputes Redressal Forum-I, U.T. Chandigarh
26. Zippo Manufacturing Co. v. Zippo.com Inc. 952 F Supp 1119 (DCWD Pa 1997

LEARNING OUTCOME

After completion of the course students will be able to –

- *A general outline on the conceptual framework of e-commerce and consumer protection*
- *Learn the existing legal and regulatory frameworks protecting consumers including e-consumers Understand the concept of approaching to a consumer dispute*
- *Learn the key principles and myriad tests to determine jurisdiction in e-consumer disputes along with the legal framework on determination of jurisdiction in internet contracts in India and in the International scenario which includes international conventions relating to jurisdictional issues in cyberspace.*

COURSE – XI

INTERNATIONAL CYBER SECURITY AND GOVERNANCE

(Elective Course - II)

OBJECTIVES OF THE COURSE:

Cybercrime is a borderless crime where the repercussions and consequences are endless. There has been an emergence in cyber-crime since the exponential rise in the Internet in 1998. The United Nations and countries together should have a prominent role in establishing international laws to govern and mitigate the effects of these cybercrimes that plague a multitude of nation States.

With this objective the course is designed to

- *To understand better the challenges of developing a unified system of global cyber governance, a comparative analysis of national cybersecurity strategy*
- *Clarity over Cyber Forensic Ethics, Security and its Impact over the Countries and Economy*
- *Consider the role of the regulating bodies and policy frameworks in combating the digital crime*
- *Examine the statistical rise of cyber crime and compare with the mitigating measures taken by the nations*
- *Know and analyse its effects on societal order and human rights of each individual*

COURSE OUTLINE

Module I: Cyber Security - The Growing Concern

a. Cybercrime, a borderless crime - Cyber Warfare - Cyber Terrorism - Cyber Espionage
b. The Untold Story of NotPetya - the Most Devastating Cyberattack in History

Module II: Major Cyber Attacks Across the Globe

a. The DigiNotar case - The Netherland Incident - Cyber-Attack on Deutsche Telekom – North Korean Case - United States of America Vs Pak Jin Hyok - CyberEspionage – Threat to Global Corporations - Case of Vietnam
b. Global Cyber War - Market for Cyber Weapons - Cyber Economics
c. Iran’s War Against US - Attack on EU, US and Asian Countries by Chinese Hackers
d. Digital Geneva Convention

Module III: Cyber Security Regulation of Developed and Developing Nations

a. Japan - Cyber Hygiene - Cyber Clean Day - Japan and US Cyber Dialogue on the Internet Economy - Japan - EU Internet Security Forum
b. National Security of UK - Critical National Infrastructure Protection (CNIP) - National Security Advice Centre (NSAC) and the National Infrastructure Security Coordination Centre (NISCC) - The United Kingdom National Risk Register
c. The Canadian Centre for Cyber Security - Canadian Shield - Chinese Hackers - FBI and the U.S. Cybersecurity and Infrastructure Security Agency (CISA) - Statement exposing a spearfishing campaign by Chinese state-sponsored hackers between 2011 and 2013 - Maritime Military Secrets - Maritime Cyber Risk
d. Indian Cyber Legislation - Policy Governance - Issue of Pegasus - Recent Threats and Amendments

Module IV: Cyber Security and Third World Nations

a. Cyber dependency - Security Policies in E-Commerce for Developing Countries
b. Increasing Cyber Victimization in Africa - Severe Scarcity of Cybersecurity Manpower
c. E - African Union Commission (AUC) and the cybersecurity
d. Global Cyber-Threats from Third World Countries

Module V: Cyber Insecurity and Geo Politics

a. Cyber Security in the Context of Economic, Humanitarian and National Security - 2017 WannaCry ransomware Case
b. Role of Organisations - The Global Commission - Regulation of ICT
c. The Paris Call for Trust and Security in Cyberspace - Major Powers and Multi Stake Holder Approach

Module VI: UN's Cyber Security Governance

a. The Role of Security Council in Cyber Security Governance - a part of the United Nations with the primary responsibility of maintaining international peace and security - Art.41, 22 of ICJ
b. World Wide Web of Terror - Cyber Jihadist - Maintenance of International Peace and Security in Cyber Context - Role of The UN Group of Governmental Experts (UNGGE)
c. UN General Assembly, Resolution 73/266 - Advancing Responsible State Behaviour in Cyberspace in the Context of International Security

Module VII: Human Rights Approach towards Cyber Security Governance

a. The Concept of Network Equality - Right to Liberty and Security on the Internet – Right to Fair Trial
b. Article 17 and 19 (2) of the International Covenant on Civil and Political Rights, 1966 - Privacy and Freedom of Expression - Article 12 of the Universal Declaration of Human Rights, 1948
c. Role of UN Human Rights Council - In conceptualising and Developing Accountability Mechanisms

Module VIII: The Challenges Ahead

a. Lack of Definitional Clarity of Cyber Space
b. Challenges in fighting Global Insurgency - Threat to Economic Health
c. Cyber Crime and Poverty - Need for a Unified Framework on Global Governance
d. 'Ensuring Digital Peace' - Urgent Need - Concept of 'Inclusiveness' - Importance of Shared Database and Harmonization of Cyber Security Legislation and Policies

BIBLIOGRAPHY

RECOMMENDED READING:

BOOKS

1. Lotrionte, Catherine. Symposium: International Law and the Internet: Adapting Legal Frameworks in Response to Online Warfare and Revolutions Fueled by Social Media: State Sovereignty and Self-Defense in Cyberspace; A Normative Framework for Balancing Legal Rights, 26 Emory Int'l. Rev. 825
2. Clarke, Richard A. and Robert Knake. Cyber War: The Next Threat to National Security and What To Do About It. Ecco, April 2010.
3. M. Reilly, 'When nations go to cyberwar', New Scientist, 23 February 2008. 7
4. I. Thomson, 'Nato builds cyber-security bunker', Information World Review, 15 May 2008
5. Paul Cornish, "EU and NATO: Co-operation or Competition?", Chatham House Report, October 2006
6. Nir Kshetri (2019) Cybercrime and Cybersecurity in Africa, Journal of Global Information Technology Management, 22:2, 77-81

7. Martha Finnemore and Duncan B. Hollis, "Constructing Norms for Global Cybersecurity," American Journal of International Law 110, no. 3, 2016

FURTHER READING:

1. Sasha Romanosky, "Examining the costs and causes of cyber incidents", Journal of Cybersecurity, Volume 2, Issue 2, December 2016, Pages 121–135
2. Warren SD", Brandeis LD; "The right to privacy", Harvard L Rev 1890;4:193–220.
3. Introna LD, "Privacy and the computer: why we need privacy in the information society. Metaphilosophy", 1997;28:259–75.
4. Hughes E, "A Cypherpunk's Manifesto. The Electronic Privacy Papers. New York, NY, USA: John Wiley & Sons, Inc, 1997, 285–87.
5. 'Cyberjamming', Wall Street Journal Europe, 29 April 2008.
6. Daniel Ochieng Otieno, "Cyber security challenges: The Case of Developing Countries", 2020
7. Kshetri, N, "Cybercrime and cybersecurity in the global South", Basingstoke, U.K, 2013.
8. Jonathan Beer, "'WannaCry' Ransomware Attack Losses Could Reach $4 Billion," CBS News, May 16, 2017
9. Amnesty International, (2020b) 'India: Human Rights Defenders Targeted by a Coordinated Spyware Operation'

LEARNING OUTCOME

After completion of the course students will be able to -

- *Understand the theoretical cybercrime framework and policy mechanisms.*
- *Develop Proficiency in Global Cyber security Infrastructure*
- *Interpret the findings and recommendations arising out universal cybercrime incidents and its impact*
- *Elucidate the nature and framework of International Organisations and their role in Cyber Security Governance*
- *Attain Clarity and know the growing menace and challenges ahead in combating global cybercrimes.*