Cyberlaw Univ

CYBERLAW UNIV

COURSES CATALOGUE

www.cyberlawuniversity.com

CONTENT

CONTENT

CONTENT

CONTENT

CONTENT

CONTENT

ABOUT CYBERLAW UNIV

Cyberlaw Univ is an online University that is specifically dedicated to the study of Cyberlaw and related legal issues. Cyberlaw Univ aims to provide various courses and diplomas that would make the participants more aware about the various legal issues pertaining to cyberspace, Internet and the World Wide Web.

OUR BELIEF: Cyberlaw Univ believes that Cyberlaw indeed provides the foundation on which the current and future online transactions and the surrounding ecosystem is based. Having strong foundations is critical for having a tall building. For the Digital online society, Cyberlaw shall continue to be the foundation fulcrum on which the edifices of future growth, progress and technological advancement would be made. Cyberlaw Univ is committed to bring the constantly evolving trends pertaining to legal issues impacting computers, computer systems, computer networks, communication devices as also data and information in the electronic form, to the participants of its various courses. In having a sound cyber legal regime, lies the success for a modern nation and its online economy. Cyberlaw Univ is committed to the principles of transparency and further growth of enabling structures, frameworks and principles of Cyberlaw. In the times to come, Cyberlaw Univ hopes to lead by thought leadership, academic initiatives aimed at cyber legal studies.

ABOUT HONORARY CHANCELLOR, CYBERLAW UNIV

Dr. Pavan Duggal, is the Founder & Chairman of International Commission on Cyber Security Law. He is also the President of Cyberlaws.Net and has been working in the pioneering area of Cyber Law, Cyber Security Law & Mobile Law. While a practicing Advocate, Supreme Court of India, Dr. Pavan Duggal has made an immense impact with an international reputation as an Expert and Authority on Cyber Law, Cyber Security Law and E-commerce law.

Dr. Duggal has been acknowledged as one of the top 4 Cyber Lawyers around the world.

WDD [World Domain Day] recognizes him as one of the top 10 Cyber Lawyers around the world.

Pavan is also heading the Artificial Intelligence Law Hub and Blockchain Law Epicentre.

His empanelment as a consultant to UNCTAD and UNESCAP on Cyber Law and Cyber Crime respectively, membership of the AFACT Legal Working Group of the UN / CEFAT, consulting as an expert with the Council Of Europe on Cyber Crime, inclusion in the Board of Experts of European Commission's Dr. E-commerce and his work as an expert authority on a Cyber Law primer for E-ASEAN Task Force and as a reviewer for Asian Development Bank speaks volumes of his worldwide acceptance as an authority. Pavan is the President of Cyberlaw Asia, Asia's pioneering organization committed to the passing of dynamic cyber laws in the Asian continent. Dr Duggal is also a member of the WIPO Arbitration and Mediation Center Panel of Neutrals.

Dr. Pavan Duggal, in association with International Telecommunications Union, conducted two Training cum Sensitization Programmes for the elected Judges and Officers of the International Court of Justice (ICJ) at The Hague, Netherlands on 23rd May, 2019.As an internationally renowned Cyber law and Cyber security subject expert, at the world stage during the High-Level Policy Statement delivered by him at the World Summit on Information Society (WSIS) organized by the International Telecommunications Union (ITU), UNESCO, UNCTAD & UNDP in Geneva, Switzerland from 25th May – 29th May, 2015. Pavan Duggal has recommended the need for coming up with an International Convention on Cyberlaw & Cyber Security. As a thought leader, Dr. Duggal has suggested that India requires a new legislation that is wholly dedicated to cyber security.

Pavan, as an international expert and authority, conducts 37 different online courses at Cyberlaw Univ, which have been subscribed by more than 26,000 students from 172 countries, speaking 52 national langauges with excellent ratings.

Pavan is a member of the Board of Globethics.net, global network of persons and institutions interested in various fields of applied ethics.

Dr. Duggal has been the Member of the Public Interest Registry's.Org Advisory Council. He is a member of ICT policy and governance working group of the UNICT taskforce. He is the legal and policy Consultant to Internet Mark 2 Project, which is examining the next level of internet. He has been invited to be an Associated Fellow of the Centre for Asia Pacific Technology Law and Policy (CAPTEL) at Singapore. He is a Member of Panel of Arbitrators of the Regional Centre for Arbitration, Kuala Lumpur and Asian Domain Names Dispute Resolution Centre at Hong Kong. He is a Panel Member Of Permanent Monitoring Panel For Information Security-World Federation Of Scientists.

ABOUT VICE CHANCELLOR, CYBERLAW UNIV

Mrs. Kusum Duggal is the Vice Chancellor of Cyberlaw Univ, an internationally known Online University which is specifically dedicated to the study of Cyberlaw and related legal issues.

Mrs. Duggal is currently working hard to establish the University with a wider perspective. The honour of establishing University has been entrusted to her because of her passion to work endlessly and take the University to greater heights. She has compelling leadership qualities and has the knack of taking faculty alongwith her to put in their best. She has indeed an aura about herself that she touches hearts and inspires minds.

A distinguished academician and administrator, Mrs. Duggal started her career as a teacher in Delhi Public School of DPS Society, one of the prestigious societies in India in 1960. She has had a successful tenure of nearly five decades and since then, she has been regularly contributing to the evolving standards of excellence in education. Her strong willpower, calibre, conviction, dedication and leadership qualities contributed in modernizing the revitalizing the school education system to the extent that she was selected to represent India in the United States under the Government of India Exchange Programme for Teachers in 1976.

She also made her remarkable contribution in her visit to the United States of America and not only strengthened Indo-US relations on education but further introduced new strategies and methodologies of education and teaching during her stint at the United States of America.

Mrs. Duggal has always endeavoured to bring new educational approaches and methodologies to uplift the cause of school education and capacity building. She is of the view that in the present scenario, there is a need for the teachers to be regularly updated and trained and motivated. Mrs. Duggal believes that in today's world, education has to be an ongoing phenomenon. She is a strong believer of the thought process that the existing traditional education is good and will continue. However, with the changing wings of today's time and with transient new developments taking place, it is absolutely imperative for any person to keep on updating his knowledge and skills set up by constant education and professional developments. She has been contributing to the cause of uplifting the school education in India. Her thrust has been into generating responsible, confident and self-reliant students for a better world.

Mrs. Kusum Duggal is convent educated. She did her graduation from University of Delhi and Bachelors of Education (B.Ed) from Punjabi University topping in her college and was awarded "All Round Best Student Award" by the gracious hands of the then Governor of Punjab. She further completed her Masters in History from Punjab University. She did Diploma in "Skills for Effective Teaching" and also "Administration and Supervision of Schools" from Maryland University, USA.

She served Delhi Public Schools Society in various capacities. She was the President of the Thrift & Credit Society which gave loans to the various staff members. She was member of the Delhi Public School Managing Committee for a number of years. She was Incharge of the Activities in managing various functions viz. International Dance Extravaganza with all the Embassy students participating. She served as a Principal in five schools. She was the Founder Principal of various schools – Delhi Public School, Ranipur and Delhi Public School, Navi Mumbai and Indraprastha International School, Dwarka, Delhi. She has also been the Principal of MDH International School, Janak Puri, Delhi. She retired as the Director of JM International School, Dwarka, Delhi.

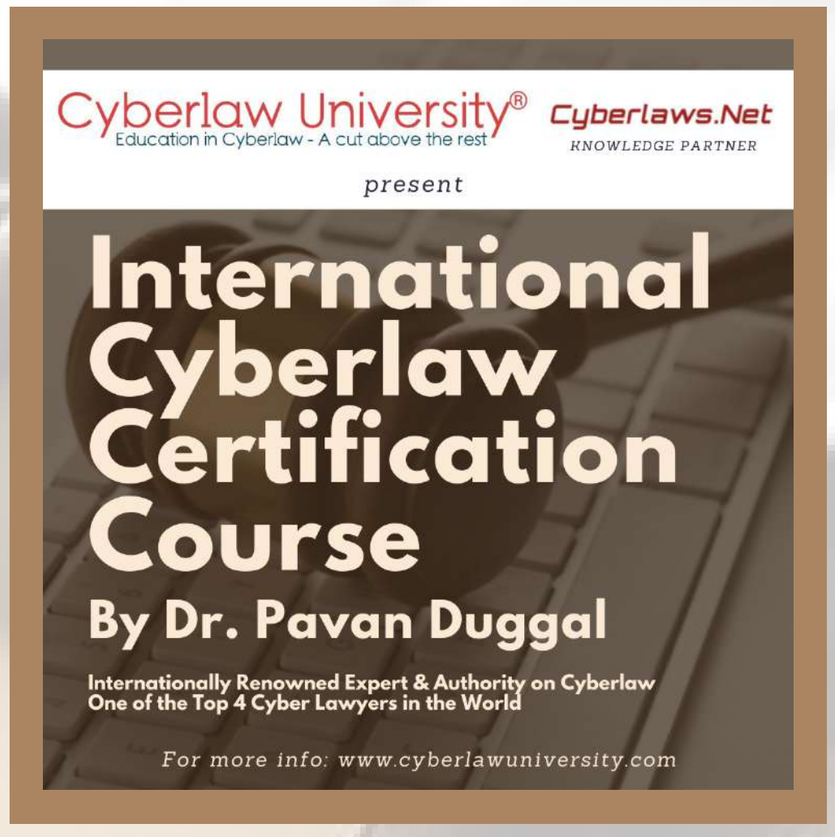
Cyberlaw Univ

INTERNATIONAL COURSES

WWW.CYBERLAWUNIVERSITY.COM

INTERNATIONAL CYBERLAW CERTIFICATION COURSE

ABOUT THE COURSE



A truly international course which opens the doors to varied developments happening on the Cyberlaw horizon. This course will sensitize you about the emerging cyber legal issues, topics and aspects at global level and how they are sought to be regulated and addressed by stakeholders in the international arena.

The International Certificate Course on Cyberlaw pushes you to discover more about cyber legal aspects, challenges and perspectives. A truly enrichen course which encourages you to dive deep into the emerging Cyberlaw trends by providing the enabling access to gateway of Cyberlaw jurisprudence.

The course which could open up new doors of Cyberlaw jurisprudence for you in the coming times.

A course which takes you to the broad ambit of current day issues engaging the attention of Cyberlaw experts and stakeholders at the international plane.

COURSE CURRICULUM

WEEK 1:- CYBERLAW- CONCEPT, ORIGINS AND TRADITIONAL GROWTH

a) Cyberlaw
b) Early Developments In Cyberlaw Jurisprudence
c) Role OfUNCITRAL Model Laws On Electronic Commerce And Electronic Signatures
d) Initial Focus On Granting Legality To Electronic Format And Electronic Commerce
e) Enabling Legal Frameworks
f) Electronic Contracts
g) Electronic Signatures
h) Different National Cyber Laws
i) Key Thrust Areas Of Cyberlaw

WEEK 2:- CYBERLAW- NATIONAL APPROACHES

a) UNCITRAL Model Laws on Electronic Commerce and Electronic Signatures
b) UNCTAD Cyberlaw Tracker
c) Cyberlaws.Net Cyberlaw Repository
d) Differing variations in national approaches
e) Broad Principles in Cyberlaw
f) National interest and cyber legal framework
g) Exchange of information and cooperation on Cybercrimes and Cyber Security
h) Bilateral cooperation mechanisms
i) Data localization and its regulation

COURSE CURRICULUM

WEEK 3:- CYBER SOVEREIGNTY & CYBERLAW

a) Sovereignty & Cyberspace
b) Definition of Cyber Sovereignty
c) Completing Theories on Cyber Sovereignty
d) Challenges of Cyber Sovereignty
e) Cyber Sovereignty & Cyber Security
f) Chinese and Russian Experience In Cyber Sovereignty
g) Vietnam Approach on Cyber Sovereignty

WEEK 4:- FAKE NEWS AND CYBERLAW

a) Fake News – Concept & Definition
b) Fake News & Cyberlaw
c) Fake News, Cybercrimes & Cyber Security
d) Challenges thrown up by Fake News Globally
e) Fake News & Privacy
f) Fake News, Attribution & Internet Jurisdiction
g) Lack of International Law on Fake News
h) National Approaches to Regulate Fake News
i) Reliance on National Penal Laws to Regulate Fake News
j) Specific Cyber Legal Issues posed by Fake News During COVID-19 Times Infodemic

WEEK 5:- FREE SPEECH, PRIVACY AND CYBERLAW

a) Free Speech and Expression in Cyberspace & Cyberlaw

i) Freedoms in Cyber space & issues
ii) Position pertaining to freedom of speech and expression jurisprudence across the world
iii) Significance of freedom of speech and expression on the Internet
iv) Salient elements to constitute freedom of speech and expression on the Internet

b) Privacy Issues, Access Rights & Cyberlaw

i) Right to privacy
ii) Existing right to privacy in the actual world
iii) Kind of privacy issues existing in the digital ecosystem and on the Internet
iv) Relationship between privacy and access rights

WEEK 6:- BLOCKCHAIN, CRYPTO ASSETS AND CYBERLAW

a) Blockchain and Salient Features
b) Blockchain, its regulation & Cyberlaw
c) National laws on regulating Blockchains, Bitcoins, crypto-assets and crypto-currencies
d) Belarus crypto-currencies law
e) 3 Blockchain laws of Malta
f) Blockchain law in Estonia & Switzerland
g) Bitcoins and its legalities
h) Indian ban on bitcoins and Supreme Court Judgment in IAMAI v/s RBI
i) New emerging trends on Blockchain regulation

COURSE CURRICULUM

WEEK 7:- CYBER LAW AND CYBERCRIME REGULATION - SALIENT ELEMENTS AND ISSUES

a) Regulation of Cybercrimes under Cyberlaw frameworks
b) Cybercrimes and their regulation globally
c) Kinds of cybercrimes targeting persons, property and nations and emerging cybercrimes and examples
d) Legalities concerning Ransomware as a cybercrime
e) Challenges with respect to detection, investigation and prosecution of Cybercrimes
f) Electronic evidence, collection, preservation, production and proof
g) Differing national strategies on electronic evidence laws
h) Poor Cybercrime convictions rate across the world & related reasons

WEEK 8:- CYBERLAW – KEY THRUST AREAS

a) Freedom and Rights in Cyberspace & Cyberlaw – Issues & Challenges
b) Internet jurisdiction
c) Electronic governance and related issues in cyberspace
d) Intermediary liability
e) Cloud Computing & Cyberlaw
f) Child Protection & Cyberlaw
g) Regulation of social media

WEEK 9:- INTERCEPTION, ENCYRPTION, DARKNET AND CYBERLAW

a) Interception, monitoring, decryption & blocking
b) Encryption
c) Darknet & Current Legal Issues
d) Legal Challenges posed by Darknet
e) Regulation of Cybercrime on Darknet
f) Important latest cases

WEEK 10:- BIG DATA, DATA PROTECTION, INTELLECTUAL PROPERTY RIGHTS AND CYBERLAW

a) Big Data & Cyberlaw – Issues & Challenges
b) Data Protection & Cyberlaw – Issues & Challenges
c) Intellectual Property Rights & Cyberlaw – Issues & Challenges

COURSE CURRICULUM

WEEK 11:- INTERNET OF THINGS AND CYBERLAW

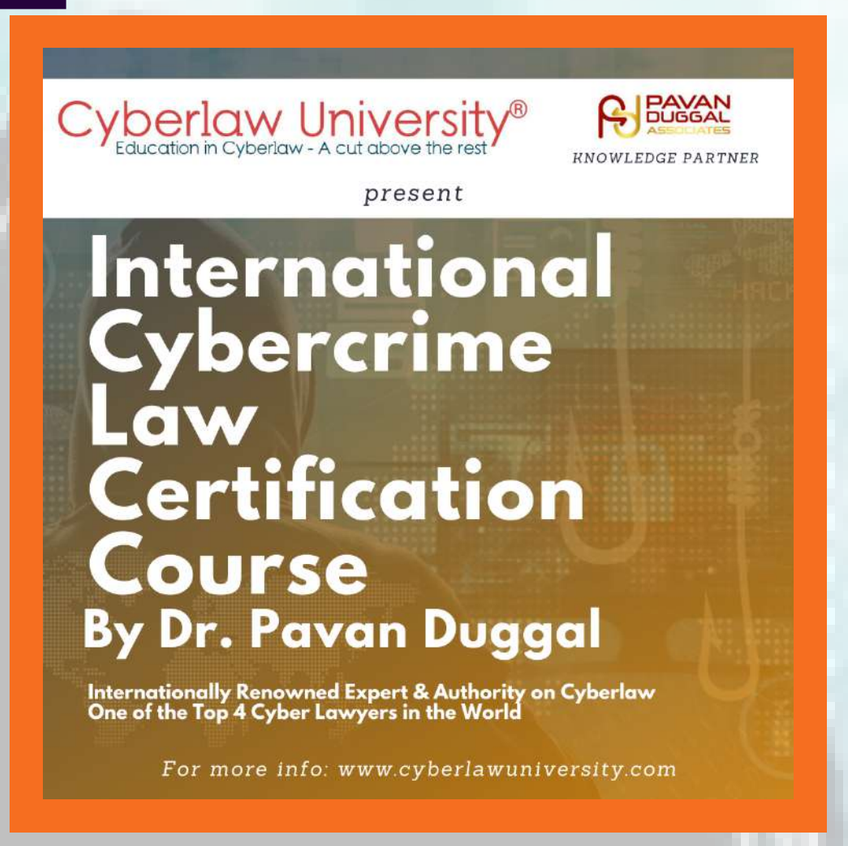
a) Internet of Things & Salient features
b) Internet of Things regulation through Cyberlaw frameworks
c) New dedicated laws on regulating Internet of Things
d) California Internet of Things law
e) UK Internet of Things guidelines
f) Challenges in regulating Internet of Things
g) Internet of Things and Cyber Security
h) Internet jurisdiction and Internet of Things
i) Internet of Things & Data Protection
j) Internet of Things & Privacy, both personal privacy and data privacy

WEEK 12:- ARTIFICIAL INTELLIGENCE, COVID-19 TIMES DEVELOPMENTS AND EMERGING CYBERLAW TRENDS

a) Artificial Intelligence – Introduction & Concept
b) Cyberlaw and Artificial Intelligence
c) Cyberlaw developments in COVID-19 times
d) COVID-19 and its impact on Future Developments in Cyberlaw
e) Cyberlaw Rules, Regulations passed in COVID-19 times
f) New Cyber World Order Post COVID-19
g) Cyber Security- a subject of growing concern in Cyberlaw

INTERNATIONAL CYBERCRIME CERTIFICATION COURSE

ABOUT THE COURSE



The International Certificate Course on Cybercrime Law aims to sensitize you about all major developments concerning the field of cybercrime and its evolution. This three-months Course will sensitize you to various emerging trends, issues and perspectives and aspects concerning cybercrime and legalities which are increasingly engaging the attention of all stakeholders at the global level.

With cybercrime being an international phenomenon having international ramifications, it is imperative to understand the holistic international perspectives pertaining to criminal activities in cyberspace and connected legal, policy and regulator issues. This course will sensitize you of what new manifestations and avatars of cybercrime as a paradigm is beginning to shape and why there is an urgent necessity at the international level to address the complicated legal, policy and regulatory nuances pertaining to cybercrime and its emerging avatars.

All in all, the International Certificate Course on Cybercrime Law will enable you to have substantial clarity of how cybercrime has evolved and how cybercriminals are increasingly adopting new and innovative approaches to target stakeholders in the digital and mobile ecosystem for their criminal and illegal designs.Hope you enjoy doing this course and get to learn more about the international ramifications of cybercrime and connected legal aspects.

COURSE CURRICULUM

WEEK 1:- CYBERCRIME – INTRODUCTION

a) Advent of ubiquitous internet
b) Cybercrime – Definition, Concept & Salient Features
c) Cybercrime – Statistics and Figures
d) Emerging Trends in Cybercrime
e) Prevention of Cybercrime

WEEK 2:- KINDS AND CATEGORIES OF CYBERCRIME

a) Kinds And Categories Of Cybercrime
b) Three Kinds Of Cybercrime - Cybercrime Against Person, Cybercrime Against Property And Cybercrime Against Nations
c) Other Kinds Of Cybercrime

WEEK 3:- INTER-PERSONAL CYBERCRIME

a) Cybercrime Against Confidentiality, Integrity And Availability Of Computers, Computer Systems, Computer Networks And Electronic Data
b) Computer related Cybercrimes
c) Offences against confidentiality, integrity and availability of computer data and systems
d) Lithuanian Plastic Surgeon Hacking case
e) Distributed Denial of Service Attacks and Malware
f) Computer Related Frauds or Forgery and Phishing
g) Spare Phishing and Whailing
h) Computer Related Identity Theft Offences
i) Computer related Copyright Offences and Computer related acts causing personal harm

COURSE CURRICULUM

WEEK 4:- CONTENT & HARM RELATED CYBERCRIME

a) Content Related Cybercrime
b) Content related offences and child sexual abuse material
c) Social Media Cybercrime
d) Newly Emerging Cybercrime
e) Cyber Bullying
f) Cyber Stalking
g) Cyber Harassment

WEEK 5:- ONLINE CHILD SEXUAL ABUSE & CYBER ORGANISED CRIME

a) Online Child Sexual Abuse And Exploitation
b) Online child grooming and live streaming of child sexual abuse
c) Gender based cybercrimes
d) Cyber organized crimes
e) Dark market and cyber organized crimes
f) Cyber organized crime prevention
g) Inter-Personal Cybercrime – Concept And Salient Features

WEEK 6:- SOCIAL MEDIA, OVER THE TOP (OTTS) APPLICATIONS AND CYBERCRIMES

a) Advent And Importance Of Social Media
b) Social Media Cybercrime – Kinds And Categories
c) Social Media Growth – Facts And Figures
d) Social Media & Over The Top Applications (OTT) Cybercrime
e) Challenges And Issues Raised By Social Media Cybercrime And OTT Cybercrime

WEEK 7:- CYBERCRIME REGULATION THROUGH NATIONAL LAWS

a) Absence Of Global Law On Cybercrime
b) Different Dedicated NationalLaws On Cybercrime
c) Invoking National Penal Laws For Regulating Cybercrimes
d) Experience Of National Cybercrime Laws On Regulating Cybercrimes
e) Practical Challenges Faced In Cybercrime Regulation Through National Laws

WEEK 8:- CYBERCRIME DETECTION, INVESTIGATION AND PROSECUTION – ISSUES AND CHALLENGES

a) Reporting Of Cybercrime
b) Investigation Of Cybercrime
c) Challenges In Cybercrime Investigation – Obstacles In Prosecution Of Cybercrime
d) Role Of Knowledge Management In Cybercrime Investigation

COURSE CURRICULUM

WEEK 9:- CONTENT & HARM RELATED CYBERCRICYBER FORENSICS AND LEGAL ISSUES

a) Electronic / Digital Evidence – Concept And Growing Increased
b) Cyber Forensics & Significance
c) Digital Forensics Process Elements
d) Cyber Forensic & Connected Legal Issues
e) Important Legal Frameworks / Laws Impacting Cyber Forensics & Connected Legal Issues
f) Cyber Forensics – Process Elements

WEEK 10:- CYBERCRIME AND CYBER SECURITY – ISSUES, CHALLENGES AND ASPECTS

a) Cyber Security – Concept And Salient Features
b) Relationship Between Cyber Security And Cybercrime
c) Cybercrime And Cyber Security – Facts And Figures
d) Jurisdiction And Attribution Challenges Facing Cybercrime And Cyber Security
e) Cyber Security Strategies – Salient Features
f) National Cyber Security Strategies And Impact On Cybercrime
g) International Cooperation On Cyber Security Matters

WEEK 11:- CYBERCRIME, DATA PROTECTION, PRIVACY, INTELLECTUAL PROPERTY RIGHTS & INTERNATIONAL COOPERATION

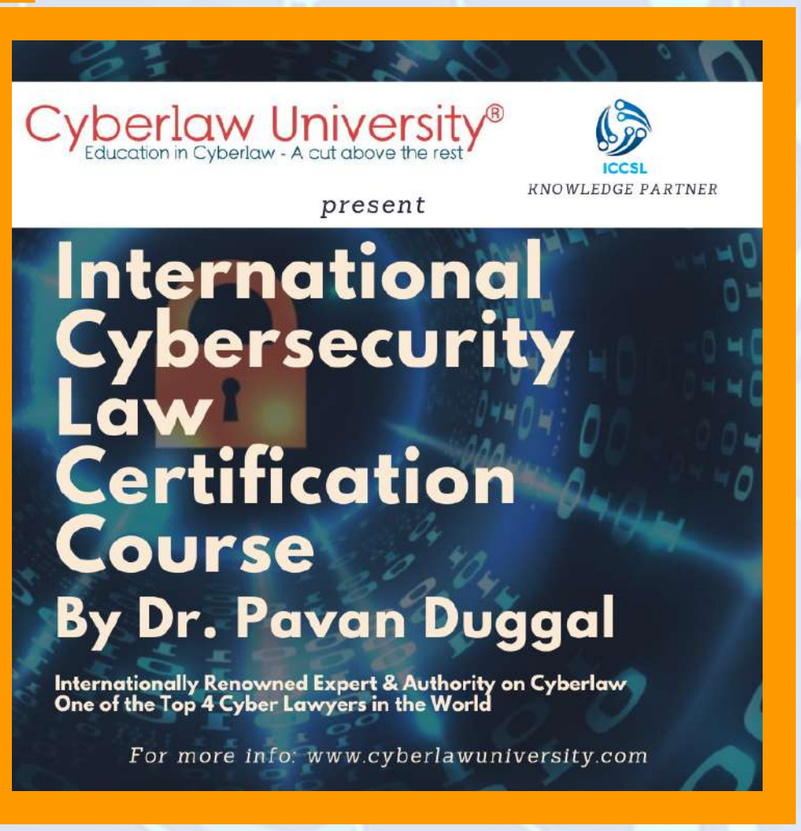
a) Cybercrime – Global Paradigm
b) Cybercrime, Sovereignty And Jurisdiction
c) Extra-Territorial Jurisdiction, Extra-Territorial Evidence And Related Challenges
d) National Capacity Building On Cybercrime
e) Data Protection – Introduction, Concept And Salient Features
f) Privacy – Introduction, Concept And Salient Features
g) Respecting intellectual property rights in E-Data

WEEK 12:- CYBERCRIME - INTERNATIONAL COOPERATION, EMERGING TRENDS IN COVID-19 AGE & FUTURE AHEAD

a) International Cooperation Against Cybercrime - Formal Mechanism
b) International Cooperation Against Cybercrime - Informal Mechanism
c) Advent Of Covid-19 And Impact On Cybercrime
d) Facts And Figures With Respect To Covid-19 Cybercrime
e) New Predominant Cybercrime In Covid-19 Age
f) Phishing, Identity Theft And Fraud In Covid-19 Era
g) Emerging Trends On Cybercrime
h) Need for new global approaches on cybercrime
i) Projected Facts And Figures
j) Regulating Cybercrime - A Global Response Needed

INTERNATIONAL CYBERSECURITY LAW CERTIFICATION COURSE

ABOUT THE COURSE



The International Certificate Course on Cyber Security Law is your gateway to world's new emerging trends and perspectives pertaining to legalities of cyber security at the international level. Cyber security is central to our lives and hence present legal, policy and regulatory challenges of cyber security becomes crucial interest of today's times.

To address these specific legalities pertaining to cyber security, a new sub-discipline of legal study being Cyber Security Law has evolved under the broad umbrella of Cyberlaw. Cyber Security Law as legal jurisprudence is developing at a very rapid pace, with different countries contributing to this evolving jurisprudence.

In this International Certificate Course on Cyber Security Law, you will got opportunity to discover the emerging thrust areas in Cyber Security Law jurisprudence. The international approaches being taken for regulating cyber security, distinctive national approaches and perspectives for cyber security and also massive impact of continuing cyber security breaches on Critical Information Infrastructure, cyber sovereignty, emerging technologies like Artificial Intelligence, Internet of Things and Blockchain and also emerging trends of Cyber Security Law.

COURSE CURRICULUM

WEEK 1:- CYBER SECURITY AND CYBER SECURITY LAW

a) Introduction
b) Cyber Security – Concept, Origin and Growing Importance
c) Various Elements of Cybersecurity
d) Increasing Cyber Security Breaches and their impact – Historical Evolution And Current Position
e) Relation between Cybersecurity and Cybercrime
f) Cyber Security Law – Concept, Origin And Development
g) Areas of Cybersecurity Law Jurisprudence
h) Relationship between Cyberlaw and Cybersecurity Law

WEEK 2:- ABSENCE OF GLOBAL LEGAL REGIME ON CYBER SECURITY

a) Absence of a Global Law on Cyber Security
b) Budapest Convention and its impact on Cyber Security
c) National Cyber Security Laws And Their Role in Cyber Security Regulation
d) Cybersecurity Laws Worldwide

WEEK 3:- AMERICAN LAWS ON CYBER SECURITY

a) American Position on Cyber Security Law
b) New York's "Stop Hacks and Improve Electronic Data Security Act" (SHIELD ACT) and its Impact
c) The NYDFS Cybersecurity Regulation (23 NYCRR 500) - Pathbreaking and Impactful
d) California Internet of Things Cyber Security Law - Dawn of a New Era
e) US Computer Fraud and Abuse Act - Salient Features & Significance
f) Ohio Cyber Security Safe Harbor Legislation- Salient Aspects & Importance
g) South Carolina Insurance Cyber Security Law – Essential Elements & Impact

COURSE CURRICULUM

WEEK 4:- EUROPEAN AND ASIA PACIFIC LAWS ON CYBER SECURITY

a) The European Union's Cybersecurity Act –Salient Features and Importance
b) New European Cyber Security Framework -Scope & Impact
c) Russia RU Net law- A Different Beginning
d) China’s Cyber Security Law and New Cyber Security Rules of China in 2020
e) Vietnam Cyber Security Law And Its Significance
f) Australian Anti-Encryption Law- A new approach to Regulating Encryption

WEEK 5:- NATIONAL CYBER SECURITY POLICIES, STRATEGIES AND BREACH NOTIFICATION LAWS

a) National cyber security policies and their impact
b) National cyber security strategies and their growing significance
c) Implementation of national cyber security laws, policies and strategies and Practical Challenges
d) Breach notification laws in different countries and their impact on cyber security regulation
e) Rights, duties and responsibilities of cyber security ecosystem stakeholders

WEEK 6:- CYBER ATTACKS AND CYBER SOVEREIGNTY

a) Cyber Attacks- Definition, Salient Features and Historical Evolution
b) Impact of Cyber Attacks
c) Cyber legal approaches to deal with cyber-attacks
d) Lack of international law / legal frameworks to deal with cyber-attacks
e) Attribution and Jurisdiction issues in cyber-attacks
f) Existing Mutual Legal Assistance Treaty (MLAT) and their efficacy in cyber-attacks sharing information
g) Lack of international norms of behaviour in cyberspace with respect to cyber-attacks
h) Tallinn Manual 1.0 and Tallinn Manual 2.0 and their impact on pushing jurisprudence on cyber attacks
i) Cyber-attacks and Sovereignty
j) Cyber Sovereignty - Concept, Features and Evolution
k) Legal and Policy issues and challenges concerning Cyber Sovereignty

WEEK 7:- CYBER RESILIENCE

a) Cyber Resilience – Definition and Historical Evolution
b) Salient Features of Cyber Resilience
c) Increasing Cyber Security Breaches and growing importance of Cyber Resilience
d) Legal, Policy and Regulatory Issues Concerning Cyber Resilience
e) Cyber Security & Cyber Resilience
f) Cyberlaw, Cybercrimes & Cyber Resilience
g) Cyberlaw & Cyber Resilience
h) Data Protection, Intermediaries and Cyber Resilience
i) Global Cyber Resilience Framework
j) Cyber Resilience & Cyber Insurance
k) Cyber Hygiene, Cyber Insurance and Cyber Resilience

COURSE CURRICULUM

WEEK 8:- ARTIFICIAL INTELLIGENCE AND CYBER SECURITY ISSUES

a) Artificial Intelligence- Concept and Growing Importance
b) Potential Misuse Of Artificial Intelligence - Need For Protecting And Preserving Cybersecurity Of AI Systems
c) Artificial Intelligence and Cybersecurity
d) Attribution Challenges In AI Ecosystem
e) Duty To Incorporate Cybersecurity As An Integral Component Of Artificial Intelligence Architecture
f) Duty Of Cybersecurity Due Diligence For AI Developers
g) Applicability Of Existing Cyber Security Laws To Artificial Intelligence
h) Darknet, Cyber Security And AI
i) Intermediary Liability In The Context Of AI
j) Norms Concerning Cybersecurity In The Context Of AI

WEEK 9:- CRITICAL INFORMATION INFRASTRUCTURE AND CYBER SECURITY ISSUES

a) Concept and Growing Importance of Critical Information Infrastructure
b) Increasing Cyber Security Breaches on Critical Information Infrastructure
c) Protection of Critical Information Infrastructure under national cyber law frameworks
d) Legal, policy & regulatory issues with respect to protecting Critical Information Infrastructure in COVID-19
e) US national emergency regarding cyber-attacks on Electric Grids
f) Chinese cyber security regulations and their impact on protecting Critical Information Infrastructure
g) Emerging international best practices for protecting Critical Information Infrastructure

WEEK 10:- CYBER SECURITY DURING COVID-19 TIMES

a) Advent of COVID-19 and its impact on Cyber Security
b) Increased Phishing Instances
c) Important Cyber Security Breaches and their Characteristics
d) Bruno University Hospital Case
e) Cyber Attacks on US Health Department
f) Phishing targeting Hospitals
g) COVID-19 legislations and rules and impact on cyber security

WEEK 11:- INTERNET OF THINGS AND CYBER SECURITY

a) Internet of Things- Definition and Salient Features
b) Internet of Things & Cyber Security Breaches
c) Lack of unanimity on cyber security standards for IoT
d) California Law on IoT and reasonable security features
e) United Kingdom approach on Cyber Security and IoT
f) Jurisdiction & Internet of Things
g) Liability of service providers in Internet of Things
h) Surveillance & Monitoring of Internet of Things and Cyber Security

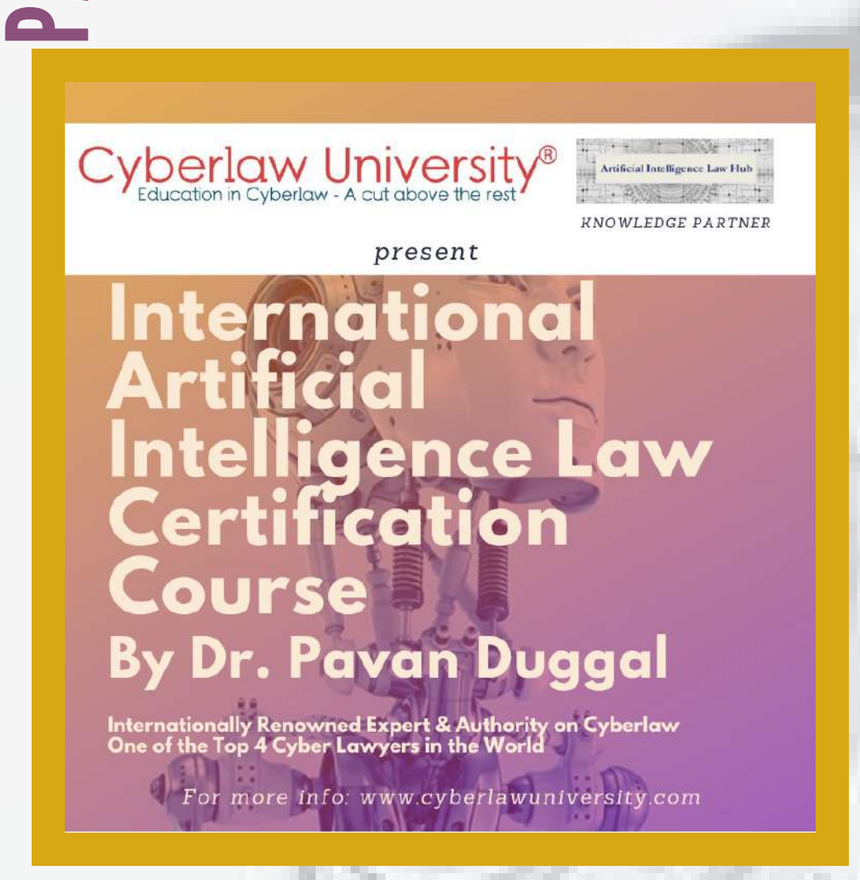
COURSE CURRICULUM

WEEK 12:- EMERGING TRENDS AND ISSUES ON CYBER SECURITY AND CYBER SECURITY LAW

a) Growing Cyber Security Incidents during COVID-19 Times
b) Cyber Security and Work From Home
c) Corporate Liability for Cybersecurity Breaches
d) Cyber Security & Video Conferencing and Connected Challenges
e) Video Conferencing and Cyber Security–Legal, Policy and Regulatory Issues
f) Advent of the New Cyber World Order and its impact on Cyber Security;
g) Need for building and strengthening Cyber Security capacity amongst countries through technical assistance and training, policy roundtables, crisis management exercises, and the exchange of best practices related to information and communication technologies
h) Building Cyber Security Capacity – The Organization of American States (OAS) Model
i) Emerging Trends in Cyber Security Law

INTERNATIONAL ARTIFICIAL INTELLIGENCE LAW CERTIFICATION COURSE

ABOUT THE COURSE



The International Certificate Course on Artificial Intelligence Law aims to sensitize about emerging developments, issues, aspects and trends pertaining to regulation of Artificial Intelligence through Artificial Intelligence Law at the global level. Massive advances taking place in Artificial Intelligence in last many years have propelled the need for stakeholders to address the legal, policy and regulatory issues emanating from Artificial Intelligence. Artificial Intelligence Law is evolving to address legalities concerning Artificial Intelligence and various challenges thrown up by Artificial Intelligence.

In this course, you will get to have landscape overview of the emerging approaches at the international level for regulating different aspects of Artificial Intelligence and how these approaches are increasingly contributing to further evolving of Artificial Intelligence Law.

In this 12 weeks course, the International Certificate Course on Artificial Intelligence Law will aim to equip you with the latest trends, perspectives and issues that are emerging in different areas on the intersection of Artificial Intelligence with various sectors of human activities. This course will further sensitize you as to how Artificial Intelligence Law is evolving and becoming important legal discipline not only today but also in the coming times.

COURSE CURRICULUM

WEEK 1:- AI LAW– INTRODUCTION, CONCEPT & GROWTH

a) Artificial Intelligence – Introduction & Concept
b) What is Artificial Intelligence?
c) AI Definition by John McCarthy
d) Other Definitions of Artificial Intelligence Salient features of Artificial Intelligence
e) Importance of Artificial Intelligence
f) Statistics about Artificial Intelligence
g) Advantages and Benefits of Artificial Intelligence
h) Need for Artificial Intelligence law

WEEK 2:- AI AS A LEGAL ENTITY

a) Legal definition of Artificial Intelligence in Nevada
b) Treating of AI as a legal entity 05:12
c) AI as a legal entity
d) Essentials of legal person
e) Artificial Intelligence and human intelligence
f) Artificial Intelligence as an agent
g) Treating Artificial Intelligence as a company
h) Salient features of a company under law
i) Company's legal features and their applicability to AI

WEEK 3:- AI CONTRACTS AND LEGALITIES

a) AI contracts and inspiration from Smart Blockchain contracts
b) Artificial Intelligence and Smart Contracts
c) Blockchain Contracts, their Legalities Legal Challenges with respect to Blockchain Contracts

COURSE CURRICULUM

WEEK 4:- AI - SOME LEGAL PRINCIPLES AND CHALLENGES

a) Respect for rule of law and fundamental rights
b) Rule of law principles endorsed by OECD, Japanese Society For AI and Google
c) Practical value of AI legal frameworks respecting rule of law
d) Principles for non-discrimination / non-bias
e) Microsoft TAY Case and Discrimination
f) International stakeholders supporting AI non-discrimination
g) Principles for Fairness for AI
h) International players backing fairness by AI
i) Principles of security for AI and international support

WEEK 5:- ARTIFICIAL INTELLIGENCE LAW AND ETHICS

a) AI & Ethics
b) Legal Profession – AI & Ethics
c) Morality & AI
d) Morality Questions in AI
e) Ethical principles and Artificial Intelligence

WEEK 6:- AI CRIMES AND THEIR REGULATION

a) AI and Cybercrimes
b) Categories Of Artificial Intelligence Cybercrimes
c) Attribution Of AI Cybercrimes
d) Electronic Evidence
e) Misuse Of AI
f) Existing Cybercrime Legislations Which Could Be Made Applicable To AI
g) Shutting Down AI Systems For Cybercrimes

WEEK 7:- AI, CYBER SECURITY BREACHES AND REGULATION

a) Cybersecurity & AI
b) Positive Uses Of Artificial Intelligence For The Purposes Of Protecting Cyber Security
c) Potential Misuse Of Artificial Intelligence - Need For Protecting And Preserving Cybersecurity Of AI Systems
d) Increasing Cybersecurity Breaches In The Context Of AI
e) Cybersecurity Breaches In AI Ecosystem & Their Attribution
f) Duty To Incorporate Cybersecurity As An Integral Component Of Artificial Intelligence Architecture
g) Duty Of Care And Due Diligence For AI Developers
h) Norms Concerning Cybersecurity In The Context Of AI
i) Applicability Of Existing Cyber Security Laws And Other Bills To Artificial Intelligence
j) Lack Of International Cyber Legal Frameworks To Deal With Artificial Intelligence And Cyber Security
k) Cyber Legal Approaches To Deal With AI & Cyber Security
l) Darknet, Cyber Security And AI

COURSE CURRICULUM

WEEK 8:- AI AND LEGAL LIABILITY

a) Legal Rights, Duties And Liabilities Of AI
b) Artificial Intelligence and legal liability – various questions
c) Legal liability for company owning or licensing Artificial Intelligence
d) Liability under law of torts and Artificial Intelligence
e) Enforcement of legal liability of Artificial Intelligence
f) Intermediary Liability In The Context Of AI
g) Self RegulationBy AI Developers

WEEK 9:- AI AND DISPENSATION OF JUSTICE, DATA PROTECTION AND LEGALITIES

a) Dispensation Of Justice Through AI Courts E.G. China, Estonia
b) Questions Regarding Justice Dispensation
c) Data protection in AI
d) Applicability of existing data protection laws in AI

WEEK 10:- AI & INTELLECTUAL PROPERTY RIGHTS

a) Artificial Intelligence and intellectual property rights
b) Can Artificial Intelligence be an inventor of an invention
c) AI & Patents- Important Questions
d) AI & Copyright- Important Questions
e) AI & Designs- Important Questions

WEEK 11:- AI, PRIVACY AND HUMAN RIGHTS

a) Privacy & AI
b) Privacy Norm & Their Incorporation in AI
c) Privacy Violation by AI
d) Applicability of Existing Privacy Law & AI
e) Roles & Responsibilities of AI users
f) Need to balance existing privacy legislations with AI
g) AI And Human Rights

WEEK 12:- NEWLY EMERGING AI LAW, TRENDS AND FUTURE AHEAD

a) Illinois AI Video Conferencing Act
b) Impact of AI
c) International overview & relation of AI in India
d) Some Questions on AI Regulations in India
e) Need for broad legal AI framework
f) Road ahead for AI laws

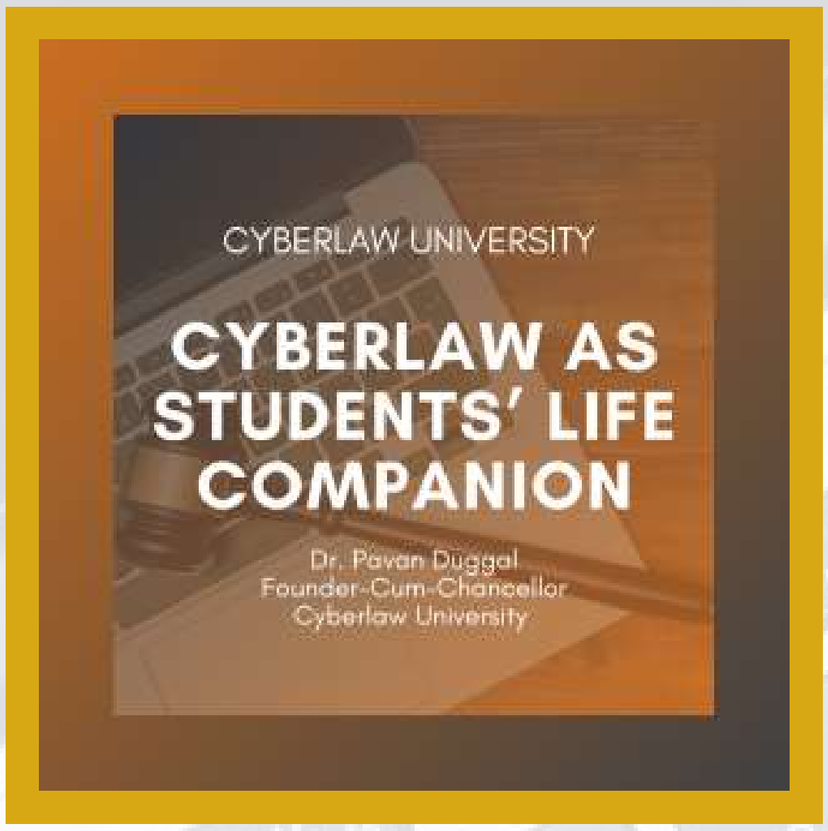
Cyberlaw Univ

SPECIAL COURSES

WWW.CYBERLAWUNIVERSITY.COM

CYBERLAW AS STUDENTS' LIFE COMPANION

ABOUT THE COURSE



Today students constitute a significant portion of the digital population. Students are the building blocks of the future. In addition, every person is a student in his entire life.

Given the advent of Covid-19 and given the increasing reliance on cyberspace, there is no denying the fact that Cyberlaw plays an extremely important role in the life of students today, whether it is a student in any educational institution, university or institute of higher learning or even a student in the paradigm of life.

This course encourages students to expand the horizon of their knowledge and learn more as to how the cyber legal principles deal with ramifications of activities in cyberspace.

This course promises to become a game changer in terms of enabling students in enhancing the horizons of their vision and digital knowledge, so as to be more prepared to face distinct challenges of cyberspace.

After doing this course, students will be far better prepared to deal with the challenges concerning their day-to-day digital lives and connected activities.
This course will enable the students to think about the legal ramifications of their digital activities and encourages them to be more careful and duly diligent, while doing various activities in the online medium.

COURSE CURRICULUM

PART 1:- COMING OF COVID-19 AND IMPACT ON INCREASING USE OF CYBERSPACE

a) Coronavirus – Advent and Constant Growth
b) Cybersecurity in Coronavirus Age
c) Coronavirus Mobile App
d) Coronavirus & Cybercrime
e) Phishing in Coronavirus Age
f) Tips to avoid becoming Coronavirus Phishing Victim
g) Coronavirus
h) Increasing Cybersecurity Breaches in Coronavirus Age
i) Coronavirus as Infodemic

PART 2:- WHY CYBERSPACE IS IMPORTANT?

a) Norms of Behaviour in Cyberspace
b) Cyberspace Statistics

PART 3:- WHAT IS CYBERLAW AND WHY IS IT IMPORTANT?

a) Definition of Cyberlaw
b) Ambit of Cyberlaw
c) Applications of Cyberlaw
d) Cyberlaw constantly evolving

COURSE CURRICULUM

PART 4:- ANONYMITY IN CYBERSPACE AND IMPACT ON BEHAVIOR

a) Anonymity on the Internet and Legal Vacuum
b) Electronic incriminating evidence and anonymity

PART 5:- SOCIAL MEDIA – THE NEW PHENOMENON

a) Misuse of Social Media
b) Professionals on social media and legal ramifications
c) Ramifications of Your Acts On Social Media
d) Cyber Hate on Social Media
e) New Kinds of Cybercrime on Social Media Emerging
f) Need for Reporting Cybercrime on Social Media
g) E-Evidence in Social Media Cybercrime
h) Social Media Providers
i) MLATs
j) Precaution to Prevent Being Victim of Social Media Cybercrime

PART 6:- CYBERSPACE AND RIGHT TO BE FORGOTTEN

a) Do you have a Right To Be Forgotten?

PART 7:- ROLE OF INTERMEDIARIES AND SERVICE PROVIDERS

a) Role of intermediaries in online defamation
b) Roles of data intermediaries in cyberlaw
c) Regulating data intermediaries and service providers

PART 8:- REMOVAL OF CONTENT FROM INTERNET- CHALLENGES AND CURRENT POSITION

a) Can You Get Your Personal Data Removed From The Web?

PART 9:- FAKE NEWS AND IMPACT ON PERSONAL REPUTATION

a) Fake News Challenges

PART 10:- CYBERCRIMES TARGETING USERS

a) Regulating Cybercrime through Cyberlaw
b) Budapest Convention on Cybercrime
c) Cybercrime Statistics
d) Increasing Cybercrime Challenges
e) Internet jurisdiction in cybercrime matters under international laws
f) Cybercrime as an essential issue
g) Cybercrime categories covered under cyberlaw

COURSE CURRICULUM

h) Cybercrime and AI
i) Applicability of existing cybercrime legislations to AI
j) Attribution of AI cybercrime
k) Shutting down AI systems for cybercrimes

PART 11:- PHISHING

a) Phishing
b) Increased Phishing
c) Phishing Targeting Hospitals

PART 12:- IDENTITY THEFT

a) Understanding Cyber Bullying And Identity Theft
b) How to deal with Cyber Bullying And Identity Theft?
c) Identity Theft
d) Legal Regulation of Identity Theft

PART 13:- GROWING CYBER SECURITY BREACHES

a) Cyber Security Breaches & Legalities
b) Cyber Security Breaches

PART 14:- REVENGE PORN AND CONNECTED CHALLENGES

a) Revenge Porn
b) Case Regarding Revenge Porn
c) Legal Responses to Revenge Porn
d) How to meet with Revenge Porn Challenges?
e) Revenge Porn And Cyber Legal Nuances

PART 15:- CYBER BULLYING AND STUDENTS TODAY

a) Cyber Bullying
b) Kinds of Cyber Bullying
c) Cyber Bullying by Social Exclusion and spreading rumors
d) Legal Regulations of Cyber Bullying
e) Cyber bullying and identity theft legalities
f) Cyber Bullying
g) Laws on Cyber Bullying
h) Understanding Cyber Bullying And Identity Theft

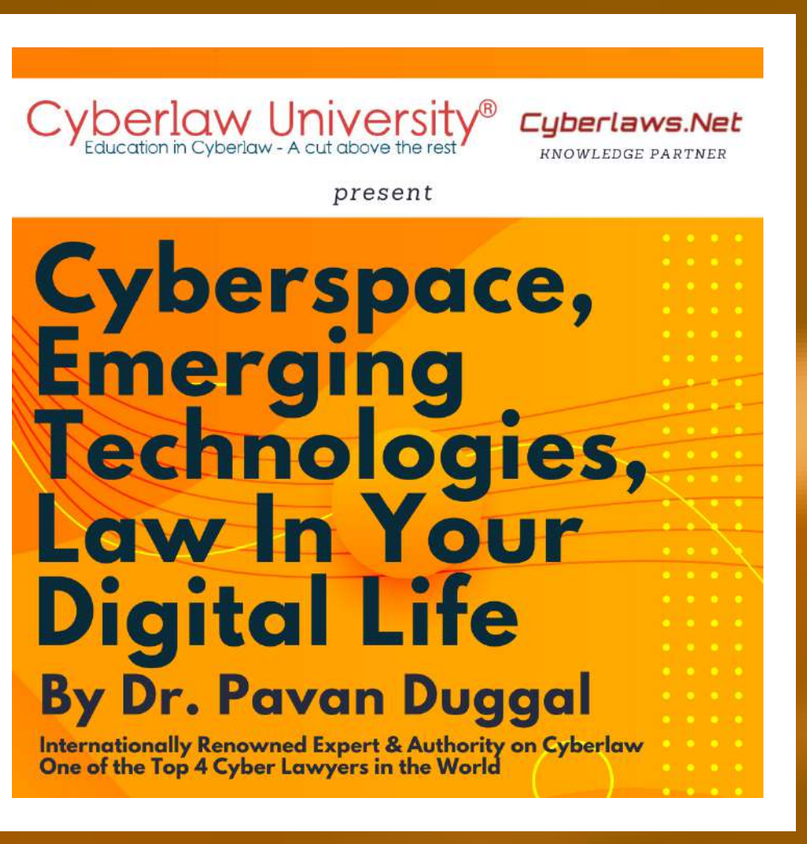
PART 16:- NEW CYBER WORLD ORDER AND PREPARATION BY STUDENTS

a) Some Broad Trends – New Cyber World Order

PART 17:- CONCLUSION

a) Conclusion

COURSE ON CYBERSPACE, EMERGING TECHNOLOGIES, LAW IN YOUR DIGITAL LIFE



ABOUT THE COURSE

With our life being intrinsically connected with cyberspace and with emerging technologies playing an important role in daily life, we need to know the legal nuances and ramifications of cyberspace and emerging technologies in our daily life.
These ramifications are important for every stakeholder as every act of them in cyberspace and/or use of emerging technologies would have legal ramifications.

Ignorance of law is no excuse in the eyes of law. Hence getting to know about the legal consequences of various acts in cyberspace and those using emerging technologies is an absolute must as we lead in our daily lives.

This course is aimed at empowering you as digital users by elaborating various legalities concerning the use of cyberspace and emerging technologies. Doing this course will further help you to navigate through technology based legal challenges in our daily life in a more proficient and pragmatic way.

Doing this course will also assist in being better prepared to aim with digital legal challenges in cyberspace and emerging technologies.

COURSE CURRICULUM

WEEK 1:- CYBERSPACE INTERNET AND DIGITAL LIFE

a) Sovereignty & Cyberspace
b) Lack of international norms of behaviour in cyberspace with respect to cyber-attacks
c) Advent of Covid-19 and its massive impact on Cyberspace
d) New Developments impacting cyberspace in Covid-19 Times
e) Coronavirus laws and impact on cyberspace issues
f) New emerging world order in cyberspace and legalities

WEEK 2:- CYBERLAW NATIONAL APPROACHES

a) Sovereignty & Cyberspace
b) Lack of international norms of behaviour in cyberspace with respect to cyber-attacks
c) Advent of Covid-19 and its massive impact on Cyberspace
d) New Developments impacting cyberspace in Covid-19 Times
e) Coronavirus laws and impact on cyberspace issues
f) New emerging world order in cyberspace and legalities
a) UNCITRAL Model Laws on Electronic Commerce and Electronic Signatures
b) UNCTAD Cyberlaw Tracker
c) Cyberlaws.Net Cyberlaw Repository
d) Differing variations in national approaches
e) Broad Principles in Cyberlaw
f) National interest and cyber legal framework
g) Exchange of information and cooperation on Cybercrimes and Cyber Security
h) Bilateral cooperation mechanisms
i) Data localization and its regulation

COURSE CURRICULUM

WEEK 3:- FREE SPEECH PRIVACY AND CYBERLAW

A) Free Speech and Expression in Cyberspace & Cyberlaw
- Freedoms in Cyber space & issues
- Position pertaining to freedom of speech and expression jurisprudence across the world
- Significance of freedom of speech and expression on the Internet
- Salient elements to constitute freedom of speech and expression on the Internet

B) Privacy Issues, Access Rights & Cyberlaw
- Right to privacy
- Existing right to privacy in the actual world
- Kind of privacy issues existing in the digital ecosystem and on the Internet
- Relationship between privacy and access rights

WEEK 4:- CYBERLAW IN INDIA

a) Cyberlaw – Definition & Concept
b) Cyberlaw – Evolving Legal Discipline
c) Concept, Definition And Features Of Cyberlaw
d) Salient Features Of Cyberlaw
e) Lack Of International Cyberlaw
f) Indian Information Technology Act, 2000
g) Coverage, Ambit And Applicability Of The Indian Information Technology Act, 2000
h) Indian Cyberlaw, IT Act, 2000 – Brief History Of Passing Of The IT Act, 2000
i) Indian Cyberlaw Circumscribed By Objectives In Preamble Of Promoting Electronic Format

WEEK 5:- CYBERLAW KEY THRUST AREAS

a) Freedom and Rights in Cyberspace & Cyberlaw – Issues & Challenges
b) Internet jurisdiction
c) Electronic governance and related issues in cyberspace
d) Intermediary liability
e) Cloud Computing & Cyberlaw
f) Child Protection & Cyberlaw
g) Regulation of social media

WEEK 6:- CYBERCRIME AN INTRODUCTION

a) Advent of ubiquitous internet
b) Cybercrime – Definition, Concept & Salient Features
c) Cybercrime – Statistics and Figures
d) Emerging Trends in Cybercrime
e) Prevention of Cybercrime

COURSE CURRICULUM

WEEK 8:- INTERPERSONAL CYBERCRIME

a) Inter-Personal Cybercrime
b) Inter-Personal Cybercrime – Concept And Salient Features
c) Various Kinds of Inter-Personal Cybercrime
d) Cybercrime Against Confidentiality, Integrity And Availability Of Computers, Computer Systems, Computer Networks And Electronic Data
e) Computer related Cybercrimes
f) Offences against confidentiality, integrity and availability of computer data and systems
g) Lithuanian Plastic Surgeon Hacking case
h) Distributed Denial of Service Attacks and Malware
i) Computer Related Frauds or Forgery and Phishing
j) Spare Phishing and Whailing
k) Computer Related Identity Theft Offences
l) Computer related Copyright Offences and Computer related acts causing personal harm

WEEK 9:- OTT CYBERCRIME

a) Advent And Importance Of Social Media
b) Social Media Cybercrime – Kinds And Categories
c) Social Media Growth – Facts And Figures
d) Social Media & Over The Top Applications (OTT) Cybercrime
e) Challenges And Issues Raised By Social Media Cybercrime And OTT Cybercrime

WEEK 10:- CONTENT & HARM RELATED CYBERCRIME

a) Content Related Cybercrime
b) Content related offences and child sexual abuse material
c) Social Media Cybercrime
d) Newly Emerging Cybercrime
e) Cyber Bullying
f) Cyber Stalking
g) Cyber Harassment
h) Cyber Forensics & Significance
i) Digital Forensics Process Elements
j) Cyber Forensic & Connected Legal Issues
k) Important Legal Frameworks / Laws Impacting Cyber Forensics & Connected Legal Issues
l) Cyber Forensics – Process Elements

WEEK 11:- CYBER SECURITY AND CYBER SECURITY LAW

a) Cyber Security – Concept, Origin and Growing Importance
b) Various Elements of Cybersecurity
c) Increasing Cyber Security Breaches and their impact – Historical Evolution And Current Position
d) Relation between Cybersecurity and Cybercrime
e) Cyber Security Law – Concept, Origin And Development
f) Areas of Cybersecurity Law Jurisprudence
g) Relationship between Cyberlaw and Cybersecurity Law

COURSE CURRICULUM

WEEK 12:- ABSENCE OF GLOBAL CYBER LEGAL REGIME ON CYBER SECURITY

a) Absence of a Global Law on Cyber Security
b) Budapest Convention and its impact on Cyber Security
c) National Cyber Security Laws And Their Role in Cyber Security Regulation
d) Cybersecurity Laws Worldwide

WEEK 13:- CYBER ATTACKS ON CYBER SOVEREIGNTY

a) Cyber Attacks- Definition, Salient Features and Historical Evolution
b) Impact of Cyber Attacks
c) Cyber legal approaches to deal with cyber-attacks
d) Lack of international law / legal frameworks to deal with cyber-attacks
e) Attribution and Jurisdiction issues in cyber-attacks
f) Existing Mutual Legal Assistance Treaty (MLAT) and their efficacy in cyber-attacks sharing information
g) Lack of international norms of behaviour in cyberspace with respect to cyber-attacks
h) Tallinn Manual 1.0 and Tallinn Manual 2.0 and their impact on pushing jurisprudence on cyber attacks
i) Cyber-attacks and Sovereignty
j) Cyber Sovereignty - Concept, Features and Evolution
k) Legal and Policy issues and challenges concerning Cyber Sovereignty
l) Sovereignty & Cyberspace
m) Definition of Cyber Sovereignty
n) Completing Theories on Cyber Sovereignty
o) Challenges of Cyber Sovereignty
p) Cyber Sovereignty & Cyber Security
q) Chinese and Russian Experience In Cyber Sovereignty
r) Vietnam Approach on Cyber Sovereignty

WEEK 14:- EMERGING TREND AND ISSUES ON CYBER SECURITY & CYBER SECURITY LAW

a) Increasing Cyber Security Breaches Globally And In India – Figures
b) Increasing Cyber Attacks On Indian Networks
c) Need For Amending Indian Cyberlaw
d) Indian Cyberlaw Needs To Constantly Evolve
e) Cyber security coverage in Indian Cyberlaw
f) Cyber security provisions under the Indian Information Technology Act, 2000
g) International developments on cyber security law and lack of dedicated Indian law on cyber security
h) Cyber security compliances by intermediary
i) Reasonable security practices and procedures
j) Cyber security reporting requirements in India
k) Protection of India’s Critical Information Infrastructure

COURSE CURRICULUM

WEEK 15:- AI & AI LAW

a) Artificial Intelligence – Introduction & Concept
b) What is Artificial Intelligence?
c) AI Definition by John McCarthy
d) Other Definitions of Artificial Intelligence Salient features of Artificial Intelligence
e) Importance of Artificial Intelligence
f) Statistics about Artificial Intelligence
g) Advantages and Benefits of Artificial Intelligence
h) Need for Artificial Intelligence law

WEEK 16:- AI – SOME LEGAL PRINCIPLES AND CHALLENGES

a) Respect for rule of law and fundamental rights
b) Rule of law principles endorsed by OECD, Japanese Society For AI and Google
c) Practical value of AI legal frameworks respecting rule of law
d) Principles for non-discrimination / non-bias
e) Microsoft TAY Case and Discrimination
f) International stakeholders supporting AI non-discrimination
g) Principles for Fairness for AI
h) International players backing fairness by AI
i) Principles of security for AI and international support

WEEK 17:- AI & LEGAL LIABILITY

a) Legal Rights, Duties And Liabilities Of AI
b) Artificial Intelligence and legal liability – various questions
c) Legal liability for company owning or licensing Artificial Intelligence
d) Liability under law of torts and Artificial Intelligence
e) Enforcement of legal liability of Artificial Intelligence
f) Intermediary Liability In The Context Of AI
g) Self Regulation By AI Developers

WEEK 18:- NEWLY EMERGING AI LAWS TRENDS AND CHALLENGES

a) Illinois AI Video Conferencing Act
b) Impact of AI
c) International overview & relation of AI in India
d) Some Questions on AI Regulations in India
e) Need for broad legal AI framework
f) Road ahead for AI laws

COURSE CURRICULUM

WEEK 19:- IOT & LAW

a) Positives and Negatives of Internet of Things
b) IoT & Statistics
c) Statistics & Barcelona case study
d) How IoT impacts your privacy?
e) Breach of medical IoT devices?
f) Internet of Things and Privacy
g) Questions regarding Internet of Things and Privacy
h) Privacy challenges on Internet of Things
i) Difficulties in privacy protection
j) California IOT law – Introduction
k) Manufacturers' obligations
l) Reasonable security features – elements
m) Clarifications regarding interpretation of California IOT law
n) IoT and Cybersecurity - An Introduction
o) Distinction between computers and communication devices on IoT evaporating
p) Duty to protect Cybersecurity in IoT devices Cybersecurity law & IoT
q) United Kingdom report on consumers IoT products and associated services
r) Common principles of UK proposed code of practice of security
s) Other common principles contd.
t) Defining IoT user rights on Cybersecurity
u) Jurisdiction & Attribution in IoT
v) Increasing frequency and cost of IoT cybersecurity breaches
w) Interception, Surveillance and Monitoring incIoT
x) Data protection &IoT
y) Traceability and unlawful profiling on IoT
z) Monitoring of data transmission on IoT

WEEK 20:- BLOCKCHAIN & LAW

a) Understanding Blockchain
b) Characteristics of Blockchain Ledgers
c) Blockchain - Statistics
d) Additional Blockchain Figures
e) Government, Blockchain Pilot Programme
f) Is Blockchain Legal?
g) Blockchain and cybersecurity
h) Challenges of cybersecurity for blockchain
i) Additional cybersecurity risks to blockchain
j) Existing Cyberlaws and Blockchain
k) Malta's Blockchain laws
l) Malta's innovative technology
m) Malta's Financial Assets Act
n) Belarus law on crypto-currency
o) Belarus legal recognition of smart contract
p) Need for new Legal framework on Blockchain
q) Legality of Blockchain, Ledger and Entry
r) Nevada Law defining blockchain

COURSE CURRICULUM

s) Blockchain Legislation in United States
t) Delaware Law on Blockchain
u) Blockchain and Privacy
v) Liability of Blockchain Service Providers
w) Banking - Blockchain and Privacy
x) Smart Contracts - An Introduction
y) Smart Contract, Blockchain and Legalities
z) Trustless trust in blockchain contracts
aa) Legality of blockchain contracts
bb) Consent and frustration of blockchain contract
cc) Projected statistics about blockchain
dd) Future projections about blockchain
ee) Trends emerging in blockchain cases around the world

WEEK 21:- DARKNET & LAW

a) Concept of Darknet
b) Definition and Features of Darknet
c) Facts About Darknet
d) Due Care and Caution on Darknet
e) Positive use of Darknet
f) No International Law on Darknet
g) Regulating Cybercrimes on Darknet
h) Categories of Darknet Crimes
i) Governmental Approaches to Darknet
j) Silk Road & Operation Onymous
k) Cryptocurrencies on Darknet
l) Legality of Darknet Transactions
m) Legality of Darknet Contract
n) Annonimity on Darknet
o) Privacy on Darknet
p) Data Protection on the Darknet
q) E-Evidence Issues on Darknet
r) Darknet Jurisdiction
s) Darknet Encryption
t) Legal Liability of Darknet Service Provider
u) Cyber Terror on Darknet
v) Cybersecurity Breaches on Darknet
w) Statistics

WEEK 22:- CYBER RESILIENCE

a) Cyber Resilience – Definition and Historical Evolution
b) Salient Features of Cyber Resilience
c) Increasing Cyber Security Breaches and growing importance of Cyber Resilience
d) Legal, Policy and Regulatory Issues Concerning Cyber Resilience
e) Cyber Security & Cyber Resilience
f) Cyberlaw, Cybercrimes & Cyber Resilience

COURSE CURRICULUM

g) Cyberlaw & Cyber Resilience
h) Data Protection, Intermediaries and Cyber Resilience
i) Global Cyber Resilience Framework
j) Cyber Resilience & Cyber Insurance
k) Cyber Hygiene, Cyber Insurance and Cyber Resilience

WEEK 23:- CYBERLAW IN INDIA – CIVIL AND CRIMINAL LIABILITIES

a) Civil and criminal liability for cyber acts by Professionals
b) Corporate Liability for Cybersecurity Breaches
c) Liability of service providers in Internet of Things
d) Artificial Intelligence and legal liability – various questions
e) Legal liability for company owning or licensing Artificial Intelligence
f) Liability under law of torts and Artificial Intelligence
g) Tortious Liability For Computer Related Acts – Section 43 IT Act

WEEK 24:- FAKE NEWS & LEGALITIES

a) Fake News – Concept & Definition
b) Fake News Challenges
c) Fake News & Cyberlaw
d) Fake News, Cybercrimes & Cyber Security
e) Challenges thrown up by Fake News Globally
f) Fake News & Privacy
g) Fake News, Attribution & Internet Jurisdiction
h) Lack of International Law on Fake News
i) National Approaches to Regulate Fake News
j) Reliance on National Penal Laws to Regulate Fake News
k) Coronavirus & Fake News
l) Covid19 as a Fake News Infodemic
m) Legal issues concerning Fake News
n) Legal Challenge concerning Fake News
o) Legal Responses to tackle with Fake News
p) Specific Cyber Legal Issues posed by Fake News During COVID-19 Times Infodemic
q) Kenya Arrest Over Coronavirus Fake News

WEEK 25:- WORK FROM HOME AND CYBER LEGAL ISSUES

a) Coronavirus - Advent and Constant Growth
b) Coronavirus & Economic Impact
c) Work from Home and It's Relevance
d) Cybersecurity in Coronavirus Age
e) Cybersecurity at Work from Home Premises
f) Cybersecurity at Work from Home Premises
g) Cybersecurity Challenges and Legal Liability for Companies
h) Corporate Liability for Cybersecurity Breaches
i) Need for Strong Telecommuting or Work from Home Policy

COURSE CURRICULUM

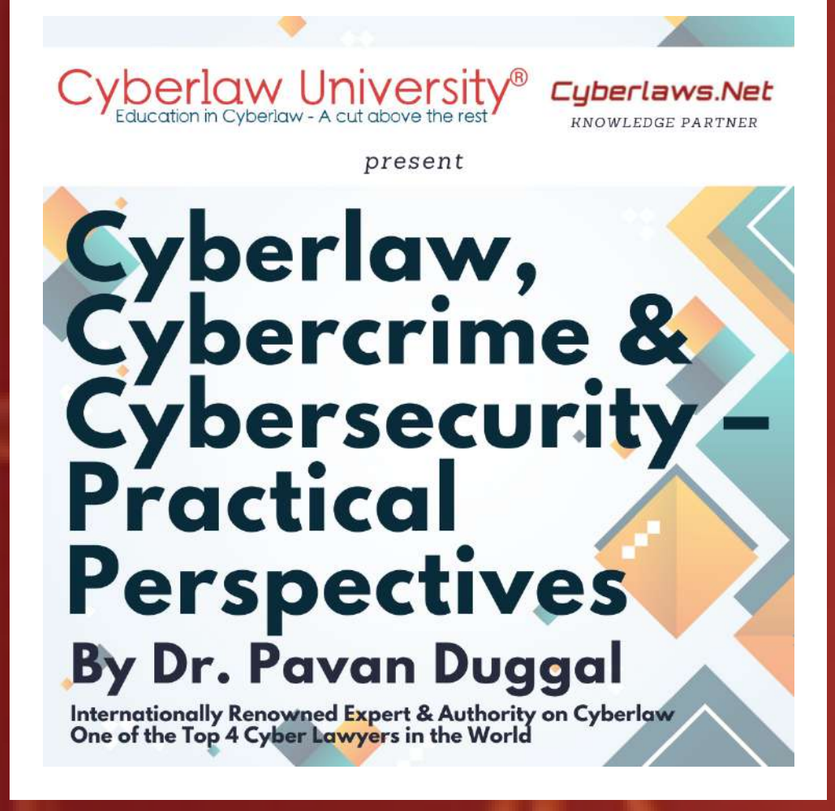
j) Important Elements of Work from Home Policy
k) Spelling Up of Employee Expectations
l) Precautions By WFH (Work from Home) Employee
m) Corporate Responsibility for Health & Safety
n) Liability for Employee at WFH Premises
o) Salient Principles from Code of Practice 2000
p) Working from Home & Child Rearing Interference
q) Monitoring of Devices Used in WFH
r) Duty to Record Time Keeping
s) White House Memo on Telework
t) Corporate Declaration on WFH in Exceptional Circumstances
u) Employee Benefits as per Local Laws
v) Proactive Duties of WFH Employee
w) Coronavirus & Cybercrime
x) Phishing in Coronavirus Age
y) Tips to avoid becoming Coronavirus Phishing Victim
z) Coronavirus & Fake News
aa) Increasing Cybersecurity Breaches in Coronavirus Age

WEEK 26:- CYBERLAW FOR DAILY LIFE & CYBERLAW IMPACT ON PROFESSIONALS

a) Defining Cyberlaw Practically
b) Why knowing Cyberlaw Is Important For Your Daily Life?
c) Due diligence By Internet Users
d) Duty of compliance with evolving cyber laws
e) Regulating data intermediaries and service providers
f) Examples Of Cyberlaw Impacting Your Daily Life
g) Cybercrime Regulation and Digital Users
h) Understanding Cyber bullying And Identity Theft
i) Legality of electronic format and electronic authentication
j) E-commerce and e-governance legally enabled
k) Need To Respect Data Confidentiality
l) Respecting intellectual property rights in electronic data
m) Different National Cybersecurity Laws
n) Increasing Cybersecurity breaches and Legal Issues
o) Your Response To A Ransomware Attack
p) Ransomware As A Cybercrime & Legal Nuances
q) Protecting professional data
r) Retention of electronic records by professionals
s) Civil and criminal liability for cyber acts by professionals
t) Ownership and handling of corporate data
u) Personal data of professionals on official devices and legalities
v) Reporting cyber frauds and cybercrimes by professionals
w) Avoiding falsification of electronic records by professionals
x) Digital future for professionals
y) New Cyber World Order

CYBERLAW, CYBERCRIME & CYBERSECURITY - PRACTICAL PERSPECTIVE

ABOUT THE COURSE



Cyberspace today has become an integral part of our daily lives. We spend a lot of time in cyberspace daily. However, cyberspace exposes us to a variety of cyber risks. Cybercrime is constantly growing in this Golden Age of Cybercrime. Increasing cyber security breaches are happening with each passing day targeting us and our data.

Similarly, different countries have come up with cyber legal frameworks for the legal activities of digital stakeholders in cyberspace. Hence, in order to navigate the cyber challenges of today, we need to work on its practical aspects.
This course aims to examine how practical perspectives on the trinity of cyber phenomena impact our daily life today being Cyberlaw, Cybercrime and Cybersecurity.

This course gives you practical nuggets of wisdom and practical tips that you need to keep in mind while you navigate cybercrime and cyber security issues and connected legalities. This course aims to empower you by knowing more about Cyberlaw, Cybercrime and Cybersecurity of their practical ramifications and impact. This course further prepares you on how to keep important cyber legal, cybercrime and cyber security ramifications in mind while doing activities in the digital ecosystem.

COURSE CURRICULUM

WEEK 1:- HOW DID CYBERLAW BEGIN?

a) Beginning of the Internet
b) Power of the Internet
c) Anonymity on the Internet and Legal Vacuum
d) Definition of Cyberlaw
e) Ambit of Cyberlaw-converted
f) Applications of Cyberlaw-converted
g) Cyberlaw constantly evolving-converted
h) Origin of Electronic Commerce and it's enabling Legal Framework
i) UNCITRAL Model Law on Electronic Commerce
j) Article 5 & 6 UNCITRAL Model Law on Electronic Commerce
k) Article 7 UNCITRAL Model Law on Electronic Commerce
l) Article 8 - Requirements for original e-records
m) Article 9 - Admissibility and evidential weight of data message
n) Article 10 - Retention of data messages
o) Formation and Validity for e-contracts
p) Attribution of data messages
q) Article 15 - Time and Place of dispatch and receipt of data messages
r) UNCITRAL role in coming up with model laws
s) UNCITRAL model laws and differences
t) Definition of e-signature
u) Electronic signature and legal requirements
v) Other issues covered by UNCITRAL Model Law on e-signature
w) UNCTAD global Cyberlaw tracker

COURSE CURRICULUM

WEEK 2:- CYBERLAW IN INDIA

a) Cyberlaw – Definition & Concept
b) Salient Features Of Cyberlaw
c) Lack Of International Cyberlaw
d) UNCITRAL Model Law On ElectronicCommerce & Electronic Signatures
e) Indian Information Technology Act, 2000
f) Coverage, Ambit And Applicability Of The Indian Information Technology Act, 2000

WEEK 3:- CYBERLAW IN INDIA

a) Cyberlaw – Evolving Legal Discipline
b) Concept, Definition And Features Of Cyberlaw
c) UNCITRAL Model Law On Electronic Commerce
d) Cyberlaw Tracker Of UNCTAD
e) Lack Of International Cyberlaw In Place
f) Different Countries Have Different Cyber Laws
g) Indian Cyberlaw, IT Act, 2000 – Brief History Of Passing Of The IT Act, 2000
h) Indian Cyberlaw Circumscribed By Objectives In Preamble Of Promoting Electronic Format

WEEK 4:- EMERGING CYBERLAW IMPACT ON PROFESSIONALS

a) Introduction
b) Legality of electronic format and electronic authentication
c) E-commerce and e-governance legally enabled
d) Retention of electronic records by professionals
e) Regulating data intermediaries and service providers
f) Civil and criminal liability for cyber acts by professionals
g) Ownership and handling of corporate data
h) Personal data of professionals on official devices and legalities
i) Electronic incriminating evidence and anonymity
j) Avoid publication of incriminating online content
k) Reporting cyber frauds and cybercrimes by professionals
l) Avoiding falsification of electronic records by professionals
m) Respecting intellectual property rights in electronic data
n) Protecting professional data
o) Duty of compliance with evolving cyber laws
p) Cyber security laws and applicability for professionals Artificial Intelligence and professionals
q) Internet of Things and professionals
r) Digital future for professionals
s) New Cyber World Order
t) Emerging Trends in Cyber Security Law Pre & During COVID-19

COURSE CURRICULUM

WEEK 5:- HOW TO RESPOND TO MAJOR CYBER LEGAL CHALLENGES

a) How to deal with Cyber Bullying And Identity Theft?
b) How to respond to Fictitious Page Of Yourself On Social Media?
c) Your Response To Defamatory Tweets
d) How to Deal With Cyber Defamation?
e) How to meet with Revenge Porn Challenges?
f) Revenge Porn And Cyber Legal Nuances
g) Understanding Legal Challenges Concerning Non Consensual Pornography
h) Can You Get Your Personal Data Removed From The Web?
i) Do you have a Right To Be Forgotten?
j) Does Sexting Pose Any Problems?
k) What are the Legal Issues Concerning Sexting?
l) Ramifications of Your Acts On Social Media
m) Do you have any Duty concerning Data held by You?
n) Legal Aspects concerning Corporate Communication Devices
o) How to deal with Misuse Of Confidential Data / Trade Secrets?
p) Should you be Complying With Cyber Legal Practices?
q) Legal ramifications of deleting Corporate Data

WEEK 6:- HOW TO DEAL WITH ONLINE FINANCIAL FRAUDS

a) Introduction
b) Instance of online financial fraud
c) Get rich quick schemes in online financial fraud
d) Online financial frauds as Cybercrime and their economic impact
e) Is online financial fraud a crime?
f) Massive increase in financial frauds and advent of Darknet
g) Identity theft
h) Mass marketing online frauds
i) Pyramid schemes of online financial fraud
j) Salient features of online financial fraud
k) Bangladesh Bank Cyber Heist Case
l) Tesco Bank Case
m) Figures about growing instances and impact of online financial fraud
n) Increasing Cybersecurity breaches & online financial frauds
o) Further figures and a grim picture
p) Online mortgage frauds
q) Credit Card & Debit Card frauds
r) Fake charities
s) Debt collection frauds
t) Misappropriation funds, employee theft and embezzlement
u) Phishing
v) Innovative approaches of online frauds
w) Theft frauds & counterfeit frauds
x) Vishing
y) Ransomware frauds
z) U.S. laws & online frauds

COURSE CURRICULUM

aa) European Union law on online financial fraud
bb) Australian law on online financial fraud
cc) Chinese law on regulating online fraud
dd) Tips to avoid becoming victims of online financial frauds
ee) Tips for corporate to avoid online financial frauds

WEEK 7:- CYBER DEFAMATION LEGALITIES

a) Actual world defamation versus online defamation
b) Challenges of online defamation
c) Freedom of speech versus defamation
d) Test of a reasonable man
e) Distinctive features of online defamation
f) Remedies for online defamation
g) Defining online defamation
h) Internet jurisdiction and online defamation
i) No international law on online defamation
j) Electronic evidence and online defamation
k) Defamation ingredients
l) Damages not effective remedy
m) Criminal online defamation
n) Role of intermediaries in online defamation
o) Principles of reforming defamation law in the internet age
p) Online personal attacks and online defamation
q) Common law presumption of reputation harm & serious harm requirements
r) Need to address new avatars and challenges of online defamation

WEEK 8:- CYBERLAW FOR YOUR DAILY LIFE

a) Defining Cyberlaw Practically
b) Why knowing Cyberlaw Is Important For Your Daily Life?
c) Due diligence By Internet Users
d) Examples Of Cyberlaw Impacting Your Daily Life
e) Corporate Communication Devices and Their Users
f) Need To Respect Data Confidentiality
g) Cybercrime Regulation and Digital Users
h) Your Response To A Ransomware Attack
i) Ransomware As A Cybercrime & Legal Nuances
j) Understanding Cyber bullying And Identity Theft
k) Increasing Cybersecurity breaches and Legal Issues
l) Different National Cybersecurity Laws
m) Artificial Intelligence And Netizens
n) Legality Of Blockchain
o) Blockchain Contracts And Legal Nuances
p) Blockchain Ledgers – How Much Legal?
q) Concept Of Smart Contracts
r) Understanding Legal Aspects of Smart Contracts & Blockchain

COURSE CURRICULUM

WEEK 9:- EMERGING TRENDS IN CYBERLAW

a) Cyberlaw Definition and Concept
b) Four Stages of Cyberlaw Evolution
c) Emerging Developments - An Introduction
d) Cyber Security Breaches & Legalities
e) Vertical Specific Cyber Security Guidelines
f) Artificial Intelligence & Legal Challenges
g) AI Liability & Legalities
h) IoT& Legal Challenges
i) IoT Statistics
j) Blockchain & Cyber Legal Challenges
k) Quantum Computing & Cyberlaw
l) Cyber Sovereignty & Legal Challenges
m) Data Localisation & Balkanisation
n) Fake News Challenges
o) Misuse of Social Media
p) Increasing Cybercrime Challenges
q) Darknet and Related Challenges
r) Big Data & Data Protection
s) Outerspace & Cybersecurity
t) Privacy Issues
u) Norms of Behavior in Cyberspace
v) Emerging Trends Only Illustrative in Nature
w) Cyberspace Statistics
x) Emerging Trends in Cyber Security Law Pre & During COVID-19

WEEK 10:- DR. PAVAN DUGGAL MANTRAS ON CYBERLAW FOR PROFESSIONALS

a) Professionals on social media and legal ramifications
b) Knowing Cyberlaw as professionals
c) Defining Cyberlaw for professionals
d) Illustrations of how Cyberlaw impacts professionals
e) Cyberlaw early developments and UN Model Laws
f) Legality of electronic format and electronic authentication
g) E-commerce and e-governance legally enabled
h) Retention of electronic records by professionals
i) Regulating cybercrime
j) Regulating data intermediaries and service providers
k) Civil and criminal liability for cyber acts by professionals
l) Professionals and corporate devices and laptops
m) Data held by professionals and connected duties
n) Ownership and handling of corporate data
o) Personal data of professionals on official devices and legalities
p) Deletion of corporate data by professionals
q) Misuse of confidential data / trade secrets
r) Electronic incriminating evidence and anonymity
s) Avoid publication of incriminating online content

COURSE CURRICULUM

t) Duty of confidentiality of data
u) Reporting cyber frauds and cybercrimes by professionals
v) Avoiding falsification of electronic records by professionals
w) Respecting intellectual property rights in electronic data
x) Protecting professional data
y) Duty of compliance with evolving cyber laws
z) Cyber security laws and applicability for professionals
aa) Artificial Intelligence and professionals
bb) Internet of Things and professionals
cc) Complying with cyber legal practices
dd) Due diligence by professionals
ee) Digital future for professionals

WEEK 11:- CYBERCRIME TODAY

a) Advent of ubiquitous internet
b) Cybercrime – Definition, Concept & Salient Features
c) Cybercrime – Statistics and Figures
d) Emerging Trends in Cybercrime
e) Prevention of Cybercrime
f) Kinds And Categories Of Cybercrime
g) Three Kinds Of Cybercrime - Cybercrime Against Person, Cybercrime Against Property And Cybercrime Against Nations
h) Other Kinds Of Cybercrime
i) Content Related Cybercrime
j) Content related offences and child sexual abuse material
k) Social Media Cybercrime
l) Newly Emerging Cybercrime

WEEK 12:- RELATIONSHIP OF CYBERCRIME & CYBERLAW

a) Cybercrime Origin
b) Kinds of Cybercrime
c) Inter-Personal Cybercrime
d) Various Kinds of Inter-Personal Cybercrime
e) Online Child Sexual Abuse
f) Cyber Legal Regional Responses to Online Child Abuse
g) International Convention Concerning the Rights of the Child
h) Online Grooming
i) Lanzarote Convention & Online Grooming
j) Child Pornography
k) Live Streaming of Child Sexual Abuse
l) Children Self Generated Sexually Explicit Content
m) Cooperation with Private Sector and Way Forward
n) European Convention on Human Rights & Cyber Harassment Laws
o) Against Cyber Stalking & Cyber Harassment
p) Misuse of Cyberlaws for Targeting Critics
q) Revenge Porn Case
r) Regarding Revenge Porn
s) Statistics
t) Other Statistics

COURSE CURRICULUM

WEEK 13:- ROLE OF CYBERCRIME IN SOCIAL MEDIA

a) Cyber Defamation
b) Legalities Regarding Cyber Defamation
c) Cyber Nuisance
d) Identity Theft
e) Legal Regulation of Identity Theft
f) Online Pornography & Child Pornography
g) Violation of Online Privacy
h) Cyber Threats
i) Cyber Extortion & Ransomware
j) Cyber Hate on Social Media
k) Cyber Terrorism & Cyber Radicalization on Social Media
l) Deep Fakes
m) New Kinds of Cybercrime on Social Media Emerging
n) Regulating Cybercrime through Cyberlaw
o) Need for Reporting Cybercrime on Social Media
p) Budapest Convention on Cybercrime
q) E-Evidence in Social Media Cybercrime
r) Social Media Providers & Their Obligations to Provide Data
s) MLATs & Social Media Cybercrime
t) Internet Jurisdiction Challenge
u) Need for Increasing Capacity Building of Law Enforcement Agencies
v) Precaution to Prevent Being Victim of Social Media Cybercrime
w) Cybercrime Statistics

WEEK 14:- CYBERCRIME IN INDIA

a) Cybercrimes
b) Massive Increase in Cybercrime and Cyber Security Breaches
c) Latest Cases on Cybercrime
d) Practical Tips to be Safe from Cybercrime and Cyber Security Breaches
e) Regulation of Cybercrimes under Cyberlaw frameworks
f) Cybercrimes and their regulation globally
g) Kinds of cybercrimes targeting persons, property and nations and emerging cybercrimes and examples

WEEK 15:- CYBERBULLYING, CYBER TROLLING, CYBER STALKING & CYBER HARASSMENT

a) Cyber Bullying
b) Kinds of Cyber Bullying
c) Cyber Bullying & Convention Over Rights of Child
d) Cyber Bullying by Social Exclusion and spreading rumors
e) Legal Regulations of Cyber Bullying
f) Laws on Cyber Bullying
g) Trolling on Social Media
h) Internet Trolling & Legal Approaches

COURSE CURRICULUM

i) Cyber Stalking
j) Legal Regulation of Cyber Stalking
k) Against Cyber Stalking & Cyber Harassment
l) Cyber Harrasment

WEEK 16:- DETECTION, INVESTIGATION & PROSECUTION OF CYBERCRIME

a) Challenges with respect to detection, investigation and prosecution of Cybercrimes
b) Electronic evidence, collection, preservation, production and proof
c) Differing national strategies on electronic evidence laws
d) Poor Cybercrime convictions rate across the world & related reasons

WEEK 17:- IMPORTANT CYBECRIME CASES & LESSONS LEARNED

a) Latest Cases on Cybercrime
b) Important Cybercrime Cases Reported In India
c) Important Cyberlaw Cases In India
d) Baazee.com case and its impact
e) Revenge Porn Case
f) Bangladesh Bank Cyber Heist Case
g) Tesco Bank Case
h) Trends emerging in blockchain cases around the world
i) Bruno University Hospital Case
j) Lithuanian Plastic Surgeon Hacking case

WEEK 18 - CYBER SEECURITY TODAY

a) Cyber Security – Concept, Origin and Growing Importance
b) Various Elements of Cybersecurity
c) Increasing Cyber Security Breaches and their impact – Historical Evolution And Current Position
d) Relation between Cybersecurity and Cybercrime
e) Cyber Security Law – Concept, Origin And Development
f) Areas of Cybersecurity Law Jurisprudence
g) Relationship between Cyberlaw and Cybersecurity Law
h) Growing Cyber Security Incidents during COVID-19 Times
i) Cyber Security and Work From Home
j) Corporate Liability for Cybersecurity Breaches
k) Cyber Security & Video Conferencing and Connected Challenges
l) Video Conferencing and Cyber Security–Legal, Policy and Regulatory Issues
m) Advent of the New Cyber World Order and its impact on Cyber Security;
n) Need for building and strengthening Cyber Security capacity amongst countries through technical assistance and training, policy roundtables, crisis management exercises, and the exchange of best practices related to information and communication technologies
o) Building Cyber Security Capacity – The Organization of American States (OAS) Model
p) Emerging Trends in Cyber Security Law

COURSE CURRICULUM

WEEK 19:- CYBERSECURITY LEGALITIES

a) Data as new oil of data economy
b) Kinds of cybersecurity breaches
c) Lack of International Law on cybersecurity
d) Budapest convention & cybersecurity
e) National Cybersecurity Policies & Strategies
f) Chinese regulatory approach on cybersecurity
g) Chinese cybersecurity law - Features
h) Cybersecurity regulation in another countries
i) Jurisdictional Challenges
j) Cyber sovereignty
k) Encryption as Challenge
l) Bilateral Cooperation on Cybersecurity
m) International Cooperation on Cybersecurity
n) Vacuum at International level on cybersecurity regulation
o) Cybersecurity in outer space
p) Artificial intelligence & cybersecurity
q) Internet of things & cybersecurity
r) Grave Figures About Cybersecurity Breaches
s) Cybersecurity Risks Ahead
t) Future Growth of Cybersecurity Law

WEEK 20:- REGULATING CYBER SECURITY

a) Increasing Cybersecurity Breaches
b) Equifax Cybersecurity Breach
c) Lack of International Law on Cybersecurity
d) Budapest Convention & Cybersecurity
e) National Cybersecurity Policies
f) The Emerging Discipline of Cybersecurity Law
g) Areas of Cybersecurity Law Jurisprudence
h) Cyberlaw & Cybersecurity Law
i) Cyber Law & Cybersecurity Law
j) Cybersecurity Law in Different Countries
k) Germany Cybersecurity Law
l) Extraterritorial Applicability of Cybersecurity Regulation
m) Attribution
n) Cyber Attribution Techniques & Challenges
o) International Cooperation on Cybersecurity
p) Bilateral Cybersecurity Cooperation Agreements
q) Features of Bilateral Cooperation Agreements
r) Artificial Intelligence & Cybersecurity
s) Internet of Things & Cybersecurity
t) Quantum Computing & Cybersecurity
u) Need For New Proactive Approaches
v) Cybersecurity Challenges Galore

COURSE CURRICULUM

WEEK 21:- LEGAL CHALLENGES OF CYBER SECURITY

a) Increasing Cybersecurity Breaches
b) Equifax Cybersecurity Breach
c) Uber Cybersecurity Breach
d) Attribution
e) Cyber Attribution Techniques & Challenges
f) Current Issues Before Cyber Attribution
g) Encryption as Challenge
h) Regulation of Encryption by Cybersecurity Law
i) Jurisdictional Challenges
j) Electronic Evidence Challenge
k) Protecting Critical Information Infrastructure
l) New Approaches for Securing Critical Information Infrastructure
m) Darknet & Cybersecurity Breaches
n) Lack of International Law on Cybersecurity
o) MLATs not Successful
p) Bilateral Cooperation on Cybersecurity
q) International Cooperation on Cybersecurity
r) Cybersecurity Law in Different Countries
s) National Cybersecurity Policies & Strategies
t) Prevailing Position of Cybersecurity Breaches
u) Grave Figures About Cybersecurity Breaches
v) Cybersecurity Risks Ahead
w) Future Growth of Cybersecurity Law
x) Cybersecurity Challenges Galore

WEEK 22:- CYBER SECURITY IN INDIA & APPROACHES SO FAR

a) Absence of a Global Law on Cyber Security
b) Budapest Convention and its impact on Cyber Security
c) National Cyber Security Laws And Their Role in Cyber Security Regulation
d) Cybersecurity Laws Worldwide
e) National cyber security policies and their impact
f) National cyber security strategies and their growing significance
g) Implementation of national cyber security laws, policies and strategies and Practical Challenges
h) Breach notification laws in different countries and their impact on cyber security regulation
i) Rights, duties and responsibilities of cyber security ecosystem stakeholders

WEEK 23:- INTERMEDIARIES & THEIR LIABILITIES

a) Intermediary – An Introduction
b) Section 79 of the Information Technology Act, 2000
c) Challenges posed by Section 79 of the Information Technology Act, 2000 from 2000 to 2008
d) Practical cases impacting intermediary
e) Baazee.com case and its impact
f) 2008 amendments to the Information Technology Act, 2000
g) Expanded concept of intermediary

COURSE CURRICULUM

h) Extensive broad ambit and definition of intermediaries
i) Amended section 79 of the Information Technology Act, 2000
j) Constitutional validity of Section 79 of the Information Technology Act, 2000
k) Need for new parameters of due diligence
l) Need for amending legal position on intermediary

WEEK 24:- DATA PROTECTION & PRIVACY IN INDIA

a) Data Protection – Introduction, Concept And Salient Features
b) Data protection and Cyberlaw
c) Data protection provisions under the Indian Cyberlaw
d) Justice B. N. Srikrishna Committee and data protection
e) Covid-19 learnings on data protection
f) Data localization – international and Indian position
g) Jurisdiction under the Indian Cyberlaw
h) Data Protection & Cyberlaw – Issues & Challenges
i) Lack Of Direct Provision On Data Protection The Indian Cyberlaw
j) Data Protection, Intermediaries and Cyber Resilience

Cyberlaw Univ

POSTGRADUATE COURSES

WWW.CYBERLAWUNIVERSITY.COM

POST GRADUATE CERTIFICATE COURSE ON CYBERLAW

ABOUT THE COURSE

This Course will give the students ability to dive deep into the some emerging and important aspects on Cyberlaw impacting India as also cyber legal nuances of emerging trends and paradigms in cyberspace. This course will enable you to get more in-depth understanding and appreciation of legal nuances pertaining to emerging cyber paradigms in India. This course will further update you with the current levels of developments on Cyberlaw in India and what all is being done at the cutting-edge levels in Indian Cyberlaw.

COURSE CURRICULUM

WEEK 1:- EVOLVING CYBERLAW GLOBALLY AND IN INDIA

a) Cyberlaw – Evolving Legal Discipline
b) Concept, Definition And Features Of Cyberlaw
c) UNCITRAL Model Law On Electronic Commerce
d) Cyberlaw Tracker Of UNCTAD
e) Lack Of International Cyberlaw In Place
f) Different Countries Have Different Cyber Laws
g) Indian Cyberlaw, IT Act, 2000 – Brief History Of Passing Of The IT Act, 2000
h) Indian Cyberlaw Circumscribed By Objectives In Preamble Of Promoting Electronic Format

WEEK 2:- INCREASING CYBERCRIME DURING COVID19 AND NEW CRIMES NOT COVERED BY INDIAN CYBERLAW

a) Social Media Misuse In India And Legal Approaches
b) Section 66A IT Act Struck Down And Its Impact On Current Social Media Misuse
c) Important Cybercrime Cases Reported In India
d) Recent trends in Cyberlaw, Cybercrime & Cyber Security
e) Important Cyberlaw Cases In India

WEEK 3:- BLOCKCHAIN, BITCOINS AND LEGALITIES- GLOBAL AND IN INDIA

a) Blockchain Laws In Different Parts Of The World
b) RBI Notification And Supreme Court Judgement
c) Bitcoins In India – Legal Position
d) Legality Of Bitcoins In India – RBICircular 2019 And Supreme Court Judgment

COURSE CURRICULUM

WEEK 4:- NEED FOR AI LEGAL REGULATION IN INDIA

a) Growth Of Artificial Intelligence Law Globally
b) Developments In India On Artificial Intelligence
c) Need For Artificial Intelligence Regulation In India
d) Development in India on Artificial Intelligence
e) Massive Growth On Artificial Intelligence Globally

WEEK 5:- ELECTRONIC COURTS AND LEGALITIES DURING COVID-19 VIDEO CONFERENCING AND LEGAL ISSUES

a) Dispensation of Justice & AI – Scope of AI
b) Position of electronic courts and virtual courts in India
c) Contribution of Covid-19 in passing use of technology for dispensation of justice
d) Videoconferencing hearings in India post Covid-19 and concerned orders passed by Indian Supreme Court and various High Courts in India
e) Development of law on videoconferencing in India prior to March 2020 – judgment of Indian Supreme Court and various High Courts in India
f) Development of legal jurisprudence on videoconferencing by courts in India post March 2020
g) Increasing electronic evidence and appreciation of electronic evidence by courts
h) Moves towards adopting technology by courts in India

WEEK 6:- CYBER SECURITY – LEGAL & POLICY LANDSCAPE IN INDIA

a) Cyber Security Regulation in India

WEEK 7:- ELECTRONIC EVIDENCE LAW- THE DEVELOPMENT OF LAW IMPACTING THE SAME

a) Arjun PanditraoKhotkar vs Kailash KushanraoGorantyal judgment
b) Crystallization Of Indian Legal Stand On Electronic Evidence
c) Supreme Court On Electronic Evidence And The Evolving Law So Far
d) Anvar PV Verus P K Basheer

WEEK 8:- CYBER SOVEREGINTY AND DATA LOCALIZATION - THE GROWTH OF LEGAL JURISPRUDENCE INTERNATIONALLY AND THE POSITION IN INDIA

a) Need For Strengthening Indian Cyber Sovereignty – Origin And Concept Of Cyber Sovereignty And The Need For Specific Provisions In Cyber Sovereignty In India
b) Data Localization Approaches In India – The Trends So Far
c) RBI Notification Dated April 2018
d) Srikrishna Report And Data Localization Requirements
e) Watered Down Data Localization In PDP Bill 2019
f) Lack Of Data Localization, Ban Of 59 Chinese Apps And Impact On India
g) Protecting Indian CII from attack

COURSE CURRICULUM

WEEK 9:- FAKE NEWS INFODEMIC AND LEGAL ISSUES

a) Covid19 as a Fake News Infodemic
b) Legal issues concerning Fake News
c) Legal Challenge concerning Fake News
d) Legal Responses to tackle with Fake News

WEEK 10:- WORK FROM HOME AND CYBER LEGAL ISSUES

a) Some Important International Best Practices concerning WFH
b) Cyberlegal issues concerning Work From Home during Covid-19
c) Advent and adoption of Work From Home during Covid-19
d) Challenges raised by Work From Home During Covid-19

WEEK 11:- A NEW WORLD ORDER EMERGING IN CYBERSPACE AND CONNECTED LEGALITES

a) New Developments impacting cyberspace in Covid-19 Times
b) Cyberlegal issues concerning internet during Covid-19
c) Coronavirus laws and impact on cyberspace issues
d) Contact Tracing apps COVID-19 and legalities
e) New emerging world order in cyberspace and legalities
f) Impact of emerging order in cyber-world and its potential impact on cyber liberties

WEEK 12:- EMERGING CYBERLAW, CYBERCRIME & CYBERSECURITY ISSUES

a) Emerging Cyberlaw, Cybercrime & Cybersecurity Issues

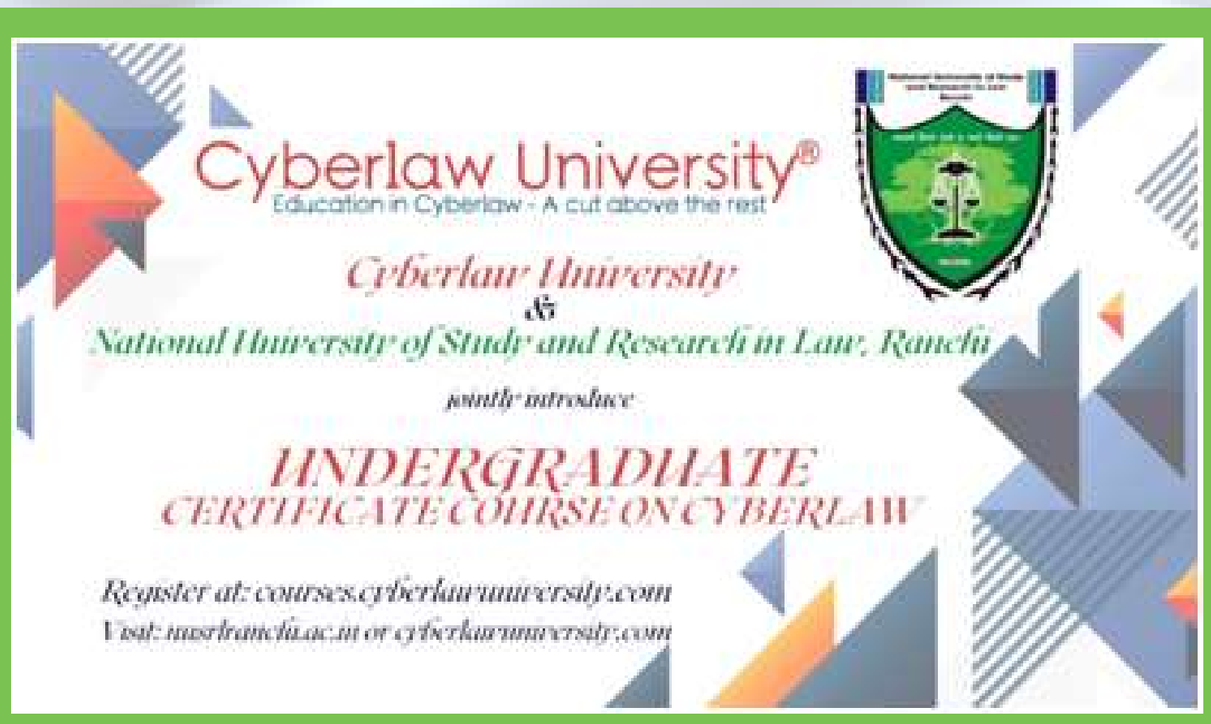
Cyberlaw Univ

UNDERGRADUATE COURSES

WWW.CYBERLAWUNIVERSITY.COM

UNDERGRADUATE CERTIFICATE COURSE ON CYBERLAW

ABOUT THE COURSE



The Undergraduate Course on Cyberlaw is a Course that aims to sensitize stakeholders about basic principles and nuances pertaining to Cyberlaw as an evolving discipline. As we have already begun starting using the digital format and as we do various activities in the online space, we have to quickly realize that our acts are governed under the Indian Cyberlaw. India has been one of the earliest nations in the world to come up with its Cyberlaw being the Indian Information Technology Act, 2000.

This Course is for all Indian students, Indian professionals and other stakeholders in the Indian digital ecosystem. This Course aims to sensitize users in India about Cyberlaw in India and how Cyberlaw impacts various activities in India. This Course further sensitize the students on how Cyberlaw is evolving in different thrust areas in India, what are the cutting-edge developments in Cyberlaw in India and how Indian stakeholders can be more prepared legally to deal with various challenges thrown up by cyberspace.

This 12 Weeks Course aims to sensitize the students about broad key tends concerning Cyberlaw in India. After doing the Course, the students will be in far more better and informed position to deal with complex legal challenges concerning their activities in cyberspace and the electronic ecosystem.

COURSE CURRICULUM

WEEK 1:- CYBERLAW IN INDIA, BEGINNINGS AND EARLY GROWTH

a) Cyberlaw – Definition & Concept
b) Salient Features Of Cyberlaw
c) Lack Of International Cyberlaw
d) UNCITRAL Model Law On Electronic Commerce & Electronic Signatures
e) Indian Information Technology Act, 2000
f) Coverage, Ambit And Applicability Of The Indian Information Technology Act, 2000

WEEK 2:- ELECTRONIC CONTRACTS, ELECTRONIC AUTHENTICATION AND ELECTRONIC GOVERNANCE LEGALITIES

a) Concept Of Electronic Contracts And Legalities -Section 6 IT Act
b) Concept Of Electronic Authentication Through Digital Signatures And Electronic Signatures
c) Retention Requirements Under The Indian Cyberlaw
d) Legality Of Electronic Format In India – Section 4 IT Act
e) Electronic Authentication In India – Section 5 IT Act
f) Digital Signature Regime In India
g) Common Myths About Retention Of Electronic Records And Legal Position
h) Duration Of Electronic Retention – Current Ambiguity In The Law And Prescription By Various Agencies
i) Misuse Of Digital Signatures – Cases
j) Controller Of Certifying Authority And Its Role In Indian Cyberlaw
k) Lack Of Direct Provision On Data Protection The Indian Cyberlaw

COURSE CURRICULUM

WEEK 3:- TORTIOUS LIABILITY FOR COMPUTER RELATED ACTS

a) Damages And Compensation For Computer Related Acts
b) Concept Of Sensitive Personal Data
c) Reasonable Security Procedures And Sensitive Personal Data
d) Unlimited Damages For Negligence In Dealing, Handling And Processing Sensitive Personal Data
e) Concept Of Personal Information And Sensitive Personal Data Under The Indian Cyberlaw
f) Reasonable Security Practices For Sensitive Personal Information
g) Unlimited Damages For Negligence In Dealing, Handling Or Processing Sensitive Personal Data Section 43A IT Act
h) Tortious Liability For Computer Related Acts – Section 43 IT Act
i) Important Cases in this regard

WEEK 4:- CYBERCRIME IN INDIA AND ITS REGULATION

a) Cybercrimes In India and Their Regulation
b) Cybercrime under the Indian Cyberlaw
c) Cybercrime under the Indian Penal Code, 1860
d) Advent of Covid-19 and its impact on Cyberlaw
e) No Dedicated law on Cybercrime regulation in India
f) Section 65 of the Information Technology Act, 2000
g) Hacking as cybercrime
h) Pornography as cybercrime and its regulation
i) Breach of Protected System
j) Penalty for misrepresentation and Cybercrime
k) Publication of Digital Signature for fraudulent purposes
l) Extra-territorial applicability of Indian Cyberlaw
m) Power of Confiscation and cybercrime
n) Power to investigate cybercrimes
o) 2008 Amendments on Bailability of Cybercrimes
p) Section 66 and 43 of the Information Technology Act, 2000
q) Section 66A of the Information Technology Act, 2000
r) Dishonestly retaining stolen computer resource or communication device
s) Identity Theft as cybercrime
t) Cheating by personation by using computer resource
u) Violation of privacy as cybercrime
v) Cyber terrorism as cybercrime
w) Publication and transmission of any records containing sexually explicit act
x) Child pornography as cybercrime Arif Azim – India’s first cybercrime conviction

COURSE CURRICULUM

WEEK 5:- INTERMEDIARY LIABILITY

a) Intermediary – An Introduction
b) Section 79 of the Information Technology Act, 2000
c) Challenges posed by Section 79 of the Information Technology Act, 2000 from 2000 to 2008
d) Practical cases impacting intermediary
e) Baazee.com case and its impact
f) 2008 amendments to the Information Technology Act, 2000
g) Expanded concept of intermediary
h) Extensive broad ambit and definition of intermediaries
i) Amended section 79 of the Information Technology Act, 2000
j) Constitutional validity of Section 79 of the Information Technology Act, 2000
k) Need for new parameters of due diligence
l) Need for amending legal position on intermediary

WEEK 6:- CYBER SECURITY RELATED REQUIREMENTS

a) Cyber security coverage in Indian Cyberlaw
b) Cyber security provisions under the Indian Information Technology Act, 2000
c) International developments on cyber security law and lack of dedicated Indian law on cyber security
d) Cyber security compliances by intermediary
e) Reasonable security practices and procedures
f) Cyber security reporting requirements in India
g) Protection of India's Critical Information Infrastructure

WEEK 7:- DATA PROTECTION, DATA LOCALIZATION & JURISDICTION

a) Data protection and Cyberlaw
b) Data protection provisions under the Indian Cyberlaw
c) Justice B. N. Srikrishna Committee and data protection
d) Covid-19 learnings on data protection
e) Data localization – international and Indian position
f) Jurisdiction under the Indian Cyberlaw

WEEK 8:- PRIVACY, DIGITAL PRIVACY AND LEGAL FRAMEWORKS IN INDIA

a) Privacy under Indian Cyberlaw
b) Justice Puttaswamy judgment and Right to Privacy in Electronic Ecosystem
c) Mobile application and digital privacy

WEEK 9:- SOCIAL MEDIA AND REGULATION IN INDIA

a) Increasing importance of social media in India
b) Regulation of misuse of social media
c) Provisions impacting social media in Indian Cyberlaw
d) Supreme Court judgment and impact on social media

COURSE CURRICULUM

WEEK 10:- AADHAAR ECOSYSTEM AND ITS REGULATION IN INDIA

a) The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016
b) Supreme Court on Aadhaar
c) Aadhaar and Other Laws (Amendment) Act, 2019

WEEK 11:- COVID19, AROGYA SETU, APPS AND OTHER CYBER LEGAL ISSUES AND CHALLENGES

a) Advent of Covid-19 and its massive impact on Cyberspace
b) ArogyaSetu App as India's COVID-19 Contact tracing app and legal issues
c) Blocking Power & App Economy in India

WEEK 12:- INADEQUACIES OF LAW AND NEED FOR MORE ENABLING AMENDMENTS & FUTURE TRENDS EMERGING IN INDIA

a) Increasing Cyber Security Breaches Globally And In India – Figures
b) Increasing Cyber Attacks On Indian Networks
c) Need For Amending Indian Cyberlaw
d) Indian Cyberlaw Needs To Constantly Evolve

CYBERLAW & CYBER SECURITY COURSE

ABOUT THE COURSE

The present one credit course on Cyberlaw and Cyber Security is being offered by National Law University, Odisha in association with Cyberlaw Univ.

This course aims to give the participants a holistic view of what is emerging globally in Cyberlaw and cyber security. In today's time, cyberspace has become an integral central lifeline of our daily lives. Hence, our reliance upon cyberspace and the internet is now a given default. More and more people are doing distinctive digital activities in the cyber ecosystem. However, every activity of every cyber actor has got a legal ramification which gets covered under the broad umbrella of Cyberlaw as a discipline.

This Course is offering practical oriented approaches and seeks to connect the evolving cyberspace jurisprudence with actual incidents and events in cyberspace. This Course is a great option for all participants who wish to update their cyber skills about Cyberlaw and cyber security. Doing the course will enable the participants to be far more better prepared to deal with emerging challenges in cyberspace in the digital ecosystem. This course should also be of great assistance in helping the participants to understand how the coming of Covid-19 has had and continues to have a remarkable and significant impact upon the evolution of jurisprudence concerning Cyberlaw and cyber security in cyberspace.

COURSE CURRICULUM

PART 1:- INTRODUCTION ON CYBERSPACE AND CYBERLAW

a) Coronavirus – Advent and Constant Growth
b) Coronavirus & Economic Impact
c) Cybersecurity in Coronavirus Age
d) Coronavirus Mobile App
e) Coronavirus & Cybercrime
f) Phishing in Coronavirus Age
g) Tips to avoid becoming Coronavirus Phishing Victim
h) Coronavirus & Fake News
i) Increasing Cybersecurity Breaches in Coronavirus Age
j) Coronavirus as Infodemic
k) Norms of Behaviour in Cyberspace
l) Cyberspace Statistics
m) Definition of Cyberlaw
n) Ambit of Cyberlaw
o) Applications of Cyberlaw
p) Cyberlaw constantly evolving
q) UNCTAD global cyberlaw tracker
r) Cyberlaw Developments South Africa
s) Introduction on cyberspace and cyberlaw

COURSE CURRICULUM

PART 2:- CYBERSPACE LEGAL CHALLENGES

a) Anonymity on the Internet and Legal Vacuum
b) Electronic incriminating evidence and anonymity
c) Internet Jurisdiction Challenge
d) Do you have a Right To Be Forgotten?
e) Can You Get Your Personal Data Removed From The Web?
f) Coronavirus & Fake News
g) Fake News Challenges
h) Privacy & AI
i) Privacy Norm & Their Incorporation in AI
j) Privacy Violation by AI
k) Applicability of Existing Privacy Law & AI
l) Need to balance existing privacy legislations with AI
m) Violation of Online Privacy
n) Privacy Issues
o) Internet of Things and Privacy
p) Blockchain and Privacy
q) Privacy on Darknet
r) Encryption as Challenge
s) Regulation of Encryption by Cybersecurity Law
t) Darknet Encryption

PART 3:- INTERMEDIARY LIABILITY AND CYBERLAW FOR CORPORATE

a) Role of intermediaries in online defamation
b) Roles of data intermediaries in cyberlaw
c) Regulating data intermediaries and service providers

PART 4:- SOCIAL MEDIA AND EMERGING CHALLENGES

a) Misuse of Social Media
b) Professionals on social media and legal ramifications
c) Ramifications of Your Acts On Social Media
d) Cyber Hate on Social Media
e) New Kinds of Cybercrime on Social Media Emerging
f) Need for Reporting Cybercrime on Social Media
g) E-Evidence in Social Media Cybercrime
h) Social Media Providers & Their Obligations to Provide Data
i) MLATs & Social Media Cybercrime
j) Precaution to Prevent Being Victim of Social Media Cybercrime
k) Internet Trolling & Legal Approaches
l) Cyber Defamation
m) Legalities Regarding Cyber Defamation
n) How to Deal With Cyber Defamation?
o) Social media and emerging challenges

COURSE CURRICULUM

PART 5:- CYBERCRIME REGULATION

a) Regulating Cybercrime through Cyberlaw
b) Budapest Convention on Cybercrime
c) Cybercrime Statistics
d) Increasing Cybercrime Challenges
e) Internet jurisdiction in cybercrime matters under international laws
f) Cybercrime as an essential issue
g) Cybercrime categories covered under cyberlaw
h) Regulating cybercrime
i) Cybercrime and AI
j) Applicability of existing cybercrime legislations to AI
k) Need for deterrence in AI cybercrime law
l) Attribution of AI cybercrime
m) Shutting down AI systems for cybercrimes
n) Phishing
o) Increased Phishing
p) Phishing Targeting Hospitals
q) Understanding Cyber Bullying And Identity Theft
r) How to deal with Cyber Bullying And Identity Theft?
s) Identity Theft
t) Legal Regulation of Identity Theft
u) Need for deterrence in AI cybercrime law
v) Massive Increase in Cybercrime
w) Cybercrime Origin
x) Kinds of Cybercrime
y) Revenge Porn
z) Case Regarding Revenge Porn
aa) Legal Responses to Revenge Porn
bb) How to meet with Revenge Porn Challenges?
cc) Revenge Porn And Cyber Legal Nuances
dd) Cyber Bullying
ee) Kinds of Cyber Bullying
ff) Cyber Bullying by Social Exclusion and spreading rumors
gg) Legal Regulations of Cyber Bullying
hh) Cyber bullying and identity theft legalities
ii) Cyber Bullying
jj) Laws on Cyber Bullying
kk) Understanding Cyber Bullying And Identity Theft
ll) Cyber Terror on Darknet
mm) Cyber Terrorism & Cyber Radicalization on Social Media
nn) Cyber Extortion & Ransomware
oo) Does Sexting Pose Any Problems?
pp) What are the Legal Issues Concerning Sexting?
qq) Cybercrime regulation

COURSE CURRICULUM

PART 6:- CYBERCRIMES IN BANKING SECTOR

a) Instance of online financial fraud
b) Get rich quick schemes in online financial fraud
c) Online financial frauds as Cybercrime and their economic impact
d) Is online financial fraud a crime
e) Massive increase in financial frauds and advent of Darknet
f) Mass marketing online frauds
g) Pyramid schemes of online financial fraud
h) Salient features of online financial fraud
i) Figures about growing instances and impact of online financial fraud
j) Increasing Cybersecurity breaches & online financial frauds
k) European Union law on online financial fraud
l) Australian law on online financial fraud
m) Chinese law on regulating online fraud
n) Tips to avoid becoming victims of online financial frauds
o) Tips for corporate to avoid online financial frauds

PART 7:- CYBERCRIME INVESTIGATIONS AND CYBER FORENSICS

a) Cybercrimes investigations and cyber forensics

PART 8:- CONSUMER PROTECTION AND DIGITAL ECOSYSTEM

a) Consumer protection and digital ecosystem

PART 9:- ARTIFICIAL INTELLIGENCE AND LEGAL CHALLENGES

a) Artificial Intelligence And Netizens
b) Artificial Intelligence & Professionals
c) Importance of Artificial Intelligence
d) What is Artificial Intelligence?
e) Other Definitions of Artificial Intelligence
f) Statistics about Artificial Intelligence
g) TCS Survey about Artificial Intelligence
h) Artificial Intelligence as an agent
i) Treating Artificial Intelligence as a company
j) Ethical principles and Artificial Intelligence
k) Legal liability for company owning or licensing Artificial Intelligence
l) Enforcement of legal liability of Artificial Intelligence
m) Important cases pertaining to Artificial Intelligence legal liability
n) Liability under law of torts and Artificial Intelligence
o) Artificial Intelligence contracts and legalities
p) Artificial Intelligence & Legal Challenges
q) Application of Artificial Intelligence & Artificial Intelligence Law
r) Further Application of Artificial Intelligence & Legal Issues
s) Facts & Figures About Artificial Intelligence

COURSE CURRICULUM

t) Additional Artificial Intelligence Statistics
u) AI as a legal entity
v) Company's legal features and their applicability to AI – Part 1
w) Company's legal features and their applicability to AI – Part 2
x) AI & Ethics
y) Legal Profession – AI & Ethics
z) Morality & AI
aa) Morality Question in AI
bb) Privacy Norm & Their Incorporation in AI
cc) Privacy Violation by AI
dd) Applicability of Existing Privacy Law & AI
ee) Data protection in AI
ff) Applicability of existing data protection laws in AI
gg) Responsibility of keeping AI secure
hh) Human monitoring of AI cyber security
ii) Misuse of AI
jj) Malicious use of AI
kk) Regulating malicious use of AI

PART 10:- ARTIFICIAL INTELLIGENCE AND LEGAL REGULATION

a) Need for Artificial Intelligence Law
b) Legal definition of Artificial Intelligence in Nevada
c) Applicability of legal person parameters to Artificial Intelligence
d) Artificial Intelligence and human intelligence
e) Need For Legally Defining Artificial Intelligence
f) US Legal Definition of Artificial Intelligence
g) New Artificial Intelligence Law on Recruitment
h) Preamble of Illinoi Artificial Intelligence Law
i) Disclosure of the Use of Artificial Intelligence Analysis
j) Duty to Explain Artificial Intelligence Working
k) Obtaining Prior Consent For Being Evaluated by Artificial Intelligence
l) Discretions to Employees Using Artificial Intelligence
m) Position Of Illinoi Artificial Intelligence Law
n) Grey Areas Of Illinoi Artificial Intelligence Law
o) Other Deficiencies Of Illinoi Artificial intelligence Law
p) White House Artificial Intelligence Principles 2020
q) Significance Of White House Artificial Intelligence Principles 2020
r) AI Definition by John McCarthy
s) No Need for specific regulation of AI
t) Treating of AI as a legal entity
u) FaceApp – an AI legal case study
v) Impact of AI
w) Need for broad legal AI framework
x) AI Liability & Legalities
y) Introduction to China's AI Governance Principles
z) China's AI Governance Principles
aa) China's Judgment on AI Written Articles Being Copyright Protected
bb) China's AI Powered Judge
cc) Projected Figures About AI Impact
dd) Future Ahead For AI Law

COURSE CURRICULUM

PART 11:- CYBER SECURITY BREACHES AND REGULATION

a) Protecting Critical Information Infrastructure
b) New Approaches for Securing Critical Information Infrastructure
c) Cyber Security Breaches & Legalities
d) Cyber Security Breaches
e) Equifax Cyber Security Breach
f) Important Cyber Security Breaches
g) Increasing frequency and cost of IoT cybersecurity breaches
h) Cybersecurity Breaches on Darknet
i) Increasing Cybersecurity Breaches and Legal Issues
j) Grave Figures About Cybersecurity Breaches
k) Dealing with cybersecurity breach
l) Cybersecurity breaches & legal issues
m) Corporate Liability for Cybersecurity Breaches
n) Cyber security breaches and regulation

PART 12:- CYBER SECURITY AND CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

a) Cyber security and Critical Information Infrastructure protection

PART 13:- CYBER SECURITY AND LEGAL CHALLENGES

a) New York Cyber Security Regulations – Pathbreaking and Impactful
b) Ohio Cyber Security Safe Harbor Legislation- Salient Features & Significance
c) South Carolina Insurance Cyber Security Law – Salient Features & Impact
d) European Cyber Security Framework – Scope & Impact
e) Cyber Security Breaches & Legalities
f) Vertical Specific Cyber Security Guidelines
g) Cyber security laws and applicability for professionals
h) Important Cyber Security Breaches
i) IoT & Legal Challenges
j) IoT Statistics
k) How IoT impacts your privacy
l) Breach of medical IoT devices
m) Privacy challenges on Internet of Things
n) California Internet of Things Cyber Security Law – Dawn of a New Era
o) Internet of Things and professionals
p) Duty to protect Cybersecurity in IoT devices
q) United Kingdom report on consumers IoT products and associated services
r) Intermediary liability & IoT
s) Defining IoT user rights on Cybersecurity
t) Jurisdiction & Attribution in IoT
u) Data protection & Internet of Things (IoT)
v) Traceability and unlawful profiling on IoT
w) Monitoring of data transmission on IoT
x) Cyber security and legal challenges

COURSE CURRICULUM

PART 14:- DATA PROTECTION LEGAL FRAMEWORK IN INDIA

a) Data protection legal framework in India

PART 15:- CONCLUSION

a) Some Broad Trends – New Cyber World Order
b) Emerging Trends Only Illustrative in Nature
c) Trends emerging in blockchain cases around the world
d) Facts About Darknet
e) Growing Facts & Figures

Cyberlaw Univ

SHORT COURSES

COURSES.CYBERLAWUNIVERSITY.COM

HOW DID CYBERLAW BEGIN?

ABOUT THE COURSE

In this course, the students will have an overview of the importance and significance of Cyberlaw as a discipline of legal study. The students will further get to know how Cyberlaw as a discipline evolved given the early advent and growth of the Internet and the World Wide Web. The students will further get to understand of how early developments in Cyberlaw jurisprudence were remarkably shaped up and influenced by the UNCITRAL Model Law on Electronic Commerce and UNCITRAL Model Law on Electronic Signatures and further how these early developments in the beginning era of Cyberlaw gave a foundation head start for the further development and evolution of Cyberlaw as a legal discipline.

COURSE CURRICULUM

- Introduction
- Beginning of the Internet
- Power of the Internet
- Anonymity on the Internet and Legal Vacuum
- Definition of Cyberlaw
- Ambit of Cyberlaw-converted
- Applications of Cyberlaw-converted
- Cyberlaw constantly evolving-converted
- Origin of Electronic Commerce and it's enabling Legal Framework
- UNCITRAL Model Law on Electronic Commerce
- Article 5 & 6 UNCITRAL Model Law on Electronic Commerce
- Article 7 UNCITRAL Model Law on Electronic Commerce
- Article 8 - Requirements for original e-records
- Article 9 - Admissibility and evidential weight of data message
- Article 10 - Retention of data messages
- Formation and Validity for e-contracts
- Attribution of data messages
- Article 15 - Time and Place of dispatch and receipt of data messages
- UNCITRAL role in coming up with model laws
- UNCITRAL model laws and differences
- Definition of e-signature
- Electronic signature and legal requirements
- Other issues covered by UNCITRAL Model Law on e-signature
- UNCTAD global Cyberlaw tracker
- Conclusion

EMERGING TRENDS IN CYBERLAW BY CYBERLAW EXPERT

ABOUT THE COURSE

In this course students will get to have an overview of the importance and significance of cyber law as an evolving legal discipline and will further be exposed to various emerging trends, developments that are likely to contribute to the further growth of cyber law jurisprudence. Advent of new technologies and new phenomenon has ensured that new legal approaches are required. How these newly emerging thrust areas are impacting the further growth and evolution of cyber law jurisprudence is the main subject of the present course.

COURSE CURRICULUM

- Introduction
- Cyberlaw Definition and Concept
- Four Stages of Cyberlaw Evolution
- Emerging Developments - An Introduction
- Cyber Security Breaches & Legalities
- Vertical Specific Cyber Security Guidelines
- Artificial Intelligence & Legal Challenges
- AI Liability & Legalities
- IoT& Legal Challenges
- IoT Statistics
- Blockchain & Cyber Legal Challenges
- Quantum Computing & Cyberlaw
- Cyber Sovereignty & Legal Challenges
- Data Localisation & Balkanisation
- Fake News Challenges
- Misuse of Social Media
- Increasing Cybercrime Challenges
- Darknet and Related Challenges
- Big Data & Data Protection
- Outerspace & Cybersecurity
- Privacy Issues
- Norms of Behavior in Cyberspace
- Emerging Trends Only Illustrative in Nature
- Cyberspace Statistics
- Emerging Trends in Cyber Security Law Pre & During COVID-19
- Conclusion

CYBERLAW FOR YOUR DAILY LIFE

ABOUT THE COURSE

In this course, students will get broad overview of why Cyberlaw is important and how Cyberlaw applies to your day-to-day activities. This course will help you understand the cyber legal ramifications of various issues and challenges that you face in your day-to-day basis when you use digital or cyber ecosystem.

This course will empower students to understand how cyber legal ramifications of various situations that they face on daily basis in cyberspace. The students will further be able to understand the legal nuances pertaining to various activities done in cyberspace and how they can navigate themselves day-to-day legal situation so as to be on the right side of the law also protect your legal interest.

COURSE CURRICULUM

- Defining Cyberlaw Practically
- Why knowing Cyberlaw Is Important For Your Daily Life?
- Due diligence By Internet Users
- Examples Of Cyberlaw Impacting Your Daily Life
- Corporate Communication Devices and Their Users
- Need To Respect Data Confidentiality
- Cybercrime Regulation and Digital Users
- Your Response To A Ransomware Attack
- Ransomware As A Cybercrime & Legal Nuances
- Understanding Cyber bullying And Identity Theft
- Increasing Cybersecurity breaches and Legal Issues
- Different National Cybersecurity Laws
- Artificial Intelligence And Netizens
- Legality Of Blockchain
- Blockchain Contracts And Legal Nuances
- Blockchain Ledgers – How Much Legal?
- Concept Of Smart Contracts
- Understanding Legal Aspects of Smart Contracts & Blockchain
- Conclusion

DR. PAVAN DUGGAL MANTRAS ON CYBERLAW FOR PROFESSIONALS

ABOUT THE COURSE

In this course, the students will get to appreciate the growing dependence on electronic data and the internet and the need for professionals to be knowing about cyber legal frameworks in today's context. In any and every professional working in whatever profession, needs to know about cyber legal ramifications of their activities in the electronic ecosystem as also in cyberspace, otherwise, they could potentially be exposed to a lot of undesirable legal consequences, both civil and criminal.

Further, the societal and reputational aspects of such ignorance of cyber legal requirements could massively and prejudicially impact a professional's reputation and business prospects, both in the present and also in the future. Hence, in this course, professionals will be sensitized on what all they need to know about Cyberlaw jurisprudence. How Cyberlaw is impacting their day-to-day professional activities and what all they need to be careful of while doing activities in the electronic format.

COURSE CURRICULUM

- Introduction
- Professionals on social media and legal ramifications
- Knowing Cyberlaw as professionals
- Defining Cyberlaw for professionals
- Illustrations of how Cyberlaw impacts professionals
- Cyberlaw early developments and UN Model Laws
- Legality of electronic format and electronic authentication
- E-commerce and e-governance legally enabled
- Retention of electronic records by professionals
- Regulating cybercrime
- Regulating data intermediaries and service providers
- Civil and criminal liability for cyber acts by professionals
- Professionals and corporate devices and laptops
- Data held by professionals and connected duties
- Ownership and handling of corporate data
- Personal data of professionals on official devices and legalities
- Deletion of corporate data by professionals
- Misuse of confidential data / trade secrets
- Electronic incriminating evidence and anonymity
- Avoid publication of incriminating online content
- Duty of confidentiality of data
- Reporting cyber frauds and cybercrimes by professionals
- Avoiding falsification of electronic records by professionals
- Respecting intellectual property rights in electronic data
- Protecting professional data
- Duty of compliance with evolving cyber laws
- Cyber security laws and applicability for professionals
- Artificial Intelligence and professionals
- Internet of Things and professionals
- Complying with cyber legal practices
- Due diligence by professionals
- Digital future for professionals
- Conclusion

GLIMPSE OF CYBERLAW THROUGH COURSES BY DR PAVAN DUGGAL

ABOUT THE COURSE

In this course, the students will have a broad overview of the growing significance of Cyberlaw in our day-to-day lives. The students will further get to know about what all issues and aspects that are increasingly covered under the evolving Cyberlaw jurisprudence.

The students will further be able to understand more about these important components of evolving Cyberlaw jurisprudence by illustrations of various specific courses on Cyberlaw which have been offered by Cyberlaw University.

Cyberlaw University is the world's only University that is dedicated to online education pertaining to Cyberlaw and its awareness. The courses offered by Cyberlaw University have been crafted and developed keeping in mind your specific requirements.

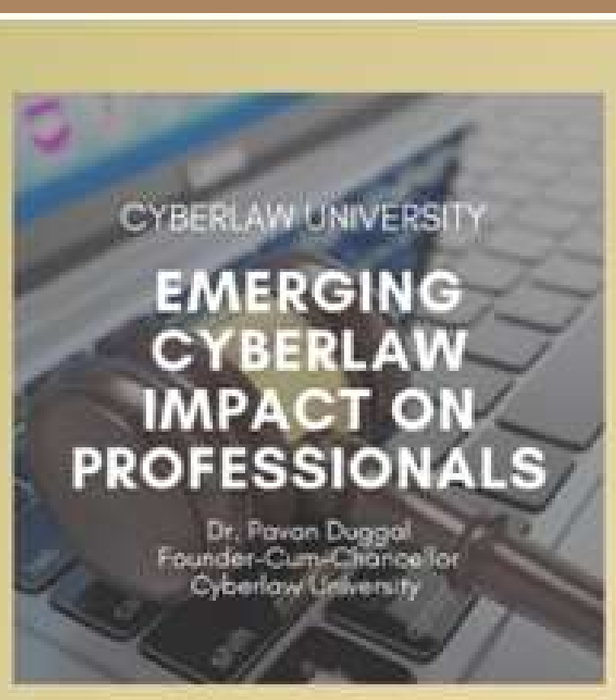
This course enables you to embark upon a journey of discovery of what all is covered under the evolving Cyberlaw jurisprudence, by having glimpse of various courses offered by Cyberlaw University.

COURSE CURRICULUM

- Introduction
- Why Cyberlaw is Important for Us
- Cyberlaw Constantly Evolving
- Cyberlaw Holds You in Good Stead
- Cyberlaw For Your Daily Life
- Relation Of Cybercrime & Cyberlaw
- Regulating Cybersecurity - All You Need To Know
- Discover Artificial Intelligence Law
- Analysis Of Internet Of Things And Law
- What Is Blockchain Law?
- Mystery Of Darknet Law
- New Cyber World Order Post COVID-19
- A Complete Guide To Cyberlaw, Cybercrime & Cybersecurity In Coronavirus Age
- Work From Home Legal Strategies During Coronavirus
- How To Deal With Online Financial Frauds?
- Conclusion

EMERGING CYBERLAW IMPACT ON PROFESSIONALS

ABOUT THE COURSE



In this course, the students will get to appreciate the growing dependence on electronic data and the internet and the need for professionals to be knowing about cyber legal frameworks in today's context. In any and every professional working in whatever profession, needs to know about cyber legal ramifications of their activities in the electronic ecosystem as also in cyberspace, otherwise, they could potentially be exposed to a lot of undesirable legal consequences, both civil and criminal.

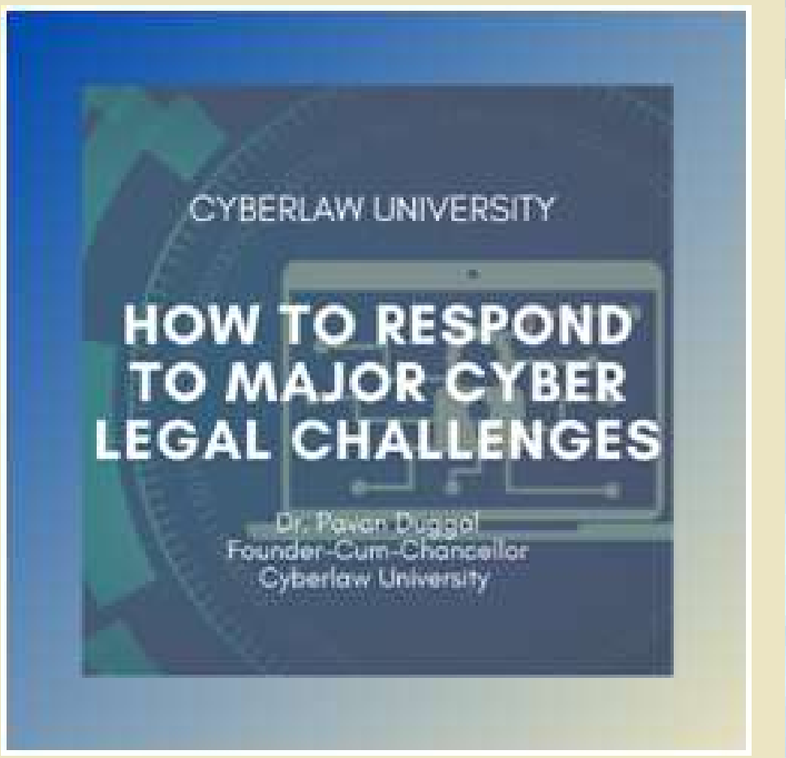
Further, the societal and reputational aspects of such ignorance of cyber legal requirements could massively and prejudicially impact a professional's reputation and business prospects, both in the present and also in the future. Hence, in this course, professionals will be sensitized on what all they need to know about Cyberlaw jurisprudence. How Cyberlaw is impacting their day-to-day professional activities and what all they need to be careful of while doing activities in the electronic format.

COURSE CURRICULUM

- Introduction
- Legality of electronic format and electronic authentication
- E-commerce and e-governance legally enabled
- Retention of electronic records by professionals
- Regulating data intermediaries and service providers
- Civil and criminal liability for cyber acts by professionals
- Ownership and handling of corporate data
- Personal data of professionals on official devices and legalities
- Electronic incriminating evidence and anonymity
- Avoid publication of incriminating online content
- Reporting cyber frauds and cybercrimes by professionals
- Avoiding falsification of electronic records by professionals
- Respecting intellectual property rights in electronic data
- Protecting professional data
- Duty of compliance with evolving cyber laws
- Cyber security laws and applicability for professionals Artificial Intelligence and professionals
- Internet of Things and professionals
- Digital future for professionals
- New Cyber World Order
- Emerging Trends in Cyber Security Law Pre & During COVID-19
- Conclusion

HOW TO RESPOND TO MAJOR CYBER LEGAL CHALLENGES

ABOUT THE COURSE



In this course, students would get to appreciate various nuances pertaining to different cyber legal challenges that they face doing their activities in cyberspace and the digital ecosystem. The students would further get to appreciate legal nuances connected therewith such challenges and what are the most appropriate and efficient response mechanisms that need to be adopted while dealing with such cyber legal challenges.

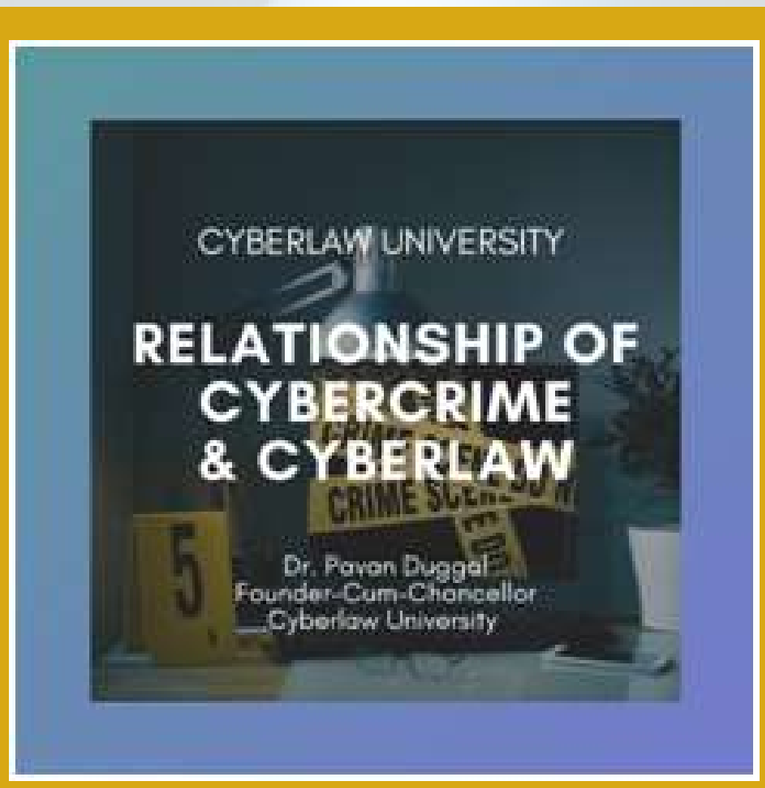
This course will increasingly inform students of how to be more empowered while responding in appropriate and legal manner to various cyber legal challenges. This course will enable the students to have lifelong learnings and that they need to keep in mind various cyber legal challenges while doing activities on the internet and also in cyberspace.

COURSE CURRICULUM

- How to deal with Cyber Bullying And Identity Theft?
- How to respond to Fictitious Page Of Yourself On Social Media?
- Your Response To Defamatory Tweets
- How to Deal With Cyber Defamation?
- How to meet with Revenge Porn Challenges?
- Revenge Porn And Cyber Legal Nuances
- Understanding Legal Challenges Concerning Non Consensual Pornography
- Can You Get Your Personal Data Removed From The Web?
- Do you have a Right To Be Forgotten?
- Does Sexting Pose Any Problems?
- What are the Legal Issues Concerning Sexting?
- Ramifications of Your Acts On Social Media
- Do you have any Duty concerning Data held by You?
- Legal Aspects concerning Corporate Communication Devices
- How to deal with Misuse Of Confidential Data / Trade Secrets?
- Should you be Complying With Cyber Legal Practices?
- Legal ramifications of deleting Corporate Data
- Conclusion

RELATIONSHIP OF CYBERCRIME & CYBERLAW

ABOUT THE COURSE



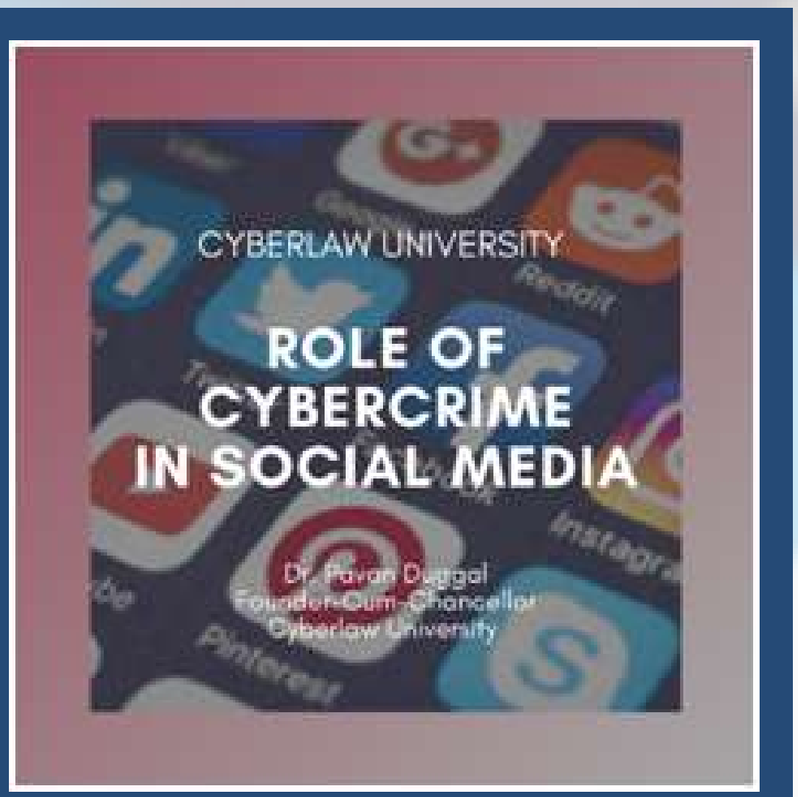
This course gives an overview on cybercrime, which deals with all the criminal activities done either in cyberspace or targeted at computer resources, computer networks and the Internet. This course further gives insights on various categories of cybercrime and further elaborates the various new kinds and manifestations of interpersonal cybercrime and how cyberlaw frameworks are dealing with the same, across the world.

COURSE CURRICULUM

- Introduction
- Cybercrime Origin
- Kinds of Cybercrime
- Inter-Personal Cybercrime
- Various Kinds of Inter-Personal Cybercrime
- Online Child Sexual Abuse
- Cyber Legal Regional Responses to Online Child Abuse
- International Convention Concerning the Rights of the Child
- Online Grooming
- Lanzarote Convention & Online Grooming
- Child Pornography
- Live Streaming of Child Sexual Abuse
- Children Self Generated Sexually Explicit Content
- Cooperation with Private Sector and Way Forward
- Cyber Stalking
- Cyber Harrasment
- European Convention on Human Rights & Cyber Harassment Laws
- Against Cyber Stalking & Cyber Harassment
- Misuse of Cyberlaws for Targeting Critics
- Internet Trolling & Legal Approaches
- Cyber Bullying
- Cyber Bullying & Convention Over Rights of Child
- Laws on Cyber Bullying
- Revenge Porn Case
- Regarding Revenge Porn
- Statistics
- Other Statistics
- Conclusion

ROLE OF CYBERCRIME IN SOCIAL MEDIA

ABOUT THE COURSE



In this course, the students will get to have an understanding of the increasing advent and emergence of cybercrimes on social media. The students will further get to know about the distinct new emerging kinds of cybercrimes that have increasingly arrived on the social media landscape and how the said cybercrimes are appropriately regulated by Cyberlaw frameworks in different parts of the world.

The students will also get to know more about why there is a need for distinct new strategies to be adopted while dealing with cybercrimes on social media and the need for far more capacity building. I hope you enjoyed doing the present course and prepared yourself for the further exciting digital journey ahead. Social media is an integral part of our day-to-day lives and there is no running away from the same.

COURSE CURRICULUM

- Cyber Bullying
- Kinds of Cyber Bullying
- Cyber Bullying by Social Exclusion and spreading rumors
- Legal Regulations of Cyber Bullying
- Cyber Stalking
- Legal Regulation of Cyber Stalking
- Cyber Defamation
- Legalities Regarding Cyber Defamation
- Cyber Nuisance
- Identity Theft
- Legal Regulation of Identity Theft
- Online Pornography & Child Pornography
- Violation of Online Privacy
- Cyber Threats
- Cyber Extortion & Ransomware
- Cyber Hate on Social Media
- Cyber Terrorism & Cyber Radicalization on Social Media
- Deep Fakes
- Trolling on Social Media
- New Kinds of Cybercrime on Social Media Emerging
- Regulating Cybercrime through Cyberlaw
- Need for Reporting Cybercrime on Social Media
- Budapest Convention on Cybercrime
- E-Evidence in Social Media Cybercrime
- Social Media Providers & Their Obligations to Provide Data
- MLATs & Social Media Cybercrime
- Internet Jurisdiction Challenge
- Need for Increasing Capacity Building of Law Enforcement Agencies
- Precaution to Prevent Being Victim of Social Media Cybercrime
- Cybercrime Statistics
- Conclusion

HOW TO DEAL WITH ONLINE FINANCIAL FRAUDS

ABOUT THE COURSE

In this course, the students will get an overview of some of the more important online financial frauds that are existing in cyberspace today. The students will be able to appreciate the peculiar features and characteristics of online financial frauds and will further be able to learn about how legal approaches are being adopted in different countries to effectively trying to regulate online financial frauds.

This course will enable any internet user to be better sensitized about online financial frauds and the connected legal nuances so that they can be better prepared while dealing with any online financial frauds in their day-to-day digital activities and digital lives. The purpose of the present course is to sensitize and empower every online user to be more aware of the different legal, policy and regulatory nuances concerning online financial frauds so that they can be in a much better position to deal with these fraudulent activities as and when faced by them in the coming times.

COURSE CURRICULUM

- Introduction
- Instance of online financial fraud
- Get rich quick schemes in online financial fraud
- Online financial frauds as Cybercrime and their economic impact
- Is online financial fraud a crime?
- Massive increase in financial frauds and advent of Darknet
- Identity theft
- Mass marketing online frauds
- Pyramid schemes of online financial fraud
- Salient features of online financial fraud
- Bangladesh Bank Cyber Heist Case
- Tesco Bank Case
- Figures about growing instances and impact of online financial fraud
- Increasing Cybersecurity breaches & online financial frauds
- Further figures and a grim picture
- Online mortgage frauds
- Credit Card & Debit Card frauds
- Fake charities
- Debt collection frauds
- Misappropriation funds, employee theft and embezzlement
- Phishing
- Innovative approaches of online frauds
- Theft frauds & counterfeit frauds
- Vishing
- Ransomware frauds
- U.S. laws & online frauds
- European Union law on online financial fraud
- Australian law on online financial fraud
- Chinese law on regulating online fraud
- Tips to avoid becoming victims of online financial frauds
- Tips for corporate to avoid online financial frauds
- Conclusion

CYBER DEFAMATION LEGALITIES

ABOUT THE COURSE

In this course, the students will be able to have a broad overview of what constitutes online defamation, what are its salient features and what are the practical legal, policy and regulatory issues concerning online defamation, what practical challenges the entirely new phenomenon of online defamation is beginning to throw up and how there is a need for the legal frameworks to constantly evolve in adopting more proactive approaches while dealing with the newly emerging avatars and manifestations of online defamation.

COURSE CURRICULUM

- Introduction
- Actual world defamation versus online defamation
- Challenges of online defamation
- Freedom of speech versus defamation
- Test of a reasonable man
- Distinctive features of online defamation
- Remedies for online defamation
- Defining online defamation
- Internet jurisdiction and online defamation
- No international law on online defamation
- Electronic evidence and online defamation
- Defamation ingredients
- Damages not effective remedy
- Criminal online defamation
- Role of intermediaries in online defamation
- Principles of reforming defamation law in the internet age
- Online personal attacks and online defamation
- Common law presumption of reputation harm & serious harm requirements
- Need to address new avatars and challenges of online defamation
- Conclusion

REGULATING CYBER SECURITY ALL YOU NEED TO KNOW

ABOUT THE COURSE

In this course, the students will get a broad overview of the various regulatory nuances that are currently evolving at a global level in the direction of regulating cybersecurity. This course will sensitize the practical challenges that are evolving in the direction of regulating cybersecurity and will further inform students of the various approaches and strategies that are now increasingly being implemented by different nation-states in the direction of trying to regulate cybersecurity.

The course will enable the students to have an understanding of how the advent of emerging technologies is having a direct connection with cybersecurity and how there is a need for adopting more proactive approaches in the direction of further growth and evolution of cybersecurity law jurisprudence.

COURSE CURRICULUM

- Introduction
- Increasing Cybersecurity Breaches
- Equifax Cybersecurity Breach
- Lack of International Law on Cybersecurity
- Budapest Convention & Cybersecurity
- National Cybersecurity Policies
- The Emerging Discipline of Cybersecurity Law
- Areas of Cybersecurity Law Jurisprudence
- Cyberlaw & Cybersecurity Law
- Cyber Law & Cybersecurity Law
- Cybersecurity Law in Different Countries
- Germany Cybersecurity Law
- Extraterritorial Applicability of Cybersecurity Regulation
- Attribution Cyber
- Attribution Techniques & Challenges
- International Cooperation on Cybersecurity
- Bilateral Cybersecurity Cooperation Agreements
- Features of Bilateral Cooperation Agreements
- Artificial Intelligence & Cybersecurity
- Internet of Things & Cybersecurity
- Quantum Computing & Cybersecurity
- Need For New Proactive Approaches
- Cybersecurity Challenges Galore
- Conclusion

LEGAL CHALLENGES OF CYBER SECURITY

ABOUT THE COURSE

In this course students will learn about the emerging discipline of cyber security law and the distinctive challenges that are currently facing the further development and evolution of cyber security law. Cyber security law is a sub discipline within the broader cyber law umbrella however its growth and evolution is dependent on how it is going to deal with the specific challenges that are currently being posed by increasing cyber security breaches.

This course will enable the students to have an overview of what major issues and challenges are facing cyber security law and how the need to be appropriate tackled in the coming times. With cyber security breaches increasingly becoming the new normal, it is imperative that the issues and challenges pertaining to cyber security breaches need to be efficaciously and holistically addressed by cyber security law.

COURSE CURRICULUM

- Introduction
- Increasing Cybersecurity Breaches
- Equifax Cybersecurity Breach
- Uber Cybersecurity Breach
- Attribution
- Cyber Attribution Techniques & Challenges
- Current Issues Before Cyber Attribution
- Encryption as Challenge
- Regulation of Encryption by Cybersecurity Law
- Jurisdictional Challenges
- Electronic Evidence Challenge
- Protecting Critical Information Infrastructure
- New Approaches for Securing Critical Information Infrastructure
- Darknet & Cybersecurity Breaches
- Lack of International Law on Cybersecurity
- MLATs not Successful
- Bilateral Cooperation on Cybersecurity
- International Cooperation on Cybersecurity
- Cybersecurity Law in Different Countries
- National Cybersecurity Policies & Strategies
- Prevailing Position of Cybersecurity Breaches
- Grave Figures About Cybersecurity Breaches
- Cybersecurity Risks Ahead
- Future Growth of Cybersecurity Law
- Cybersecurity Challenges Galore
- Conclusion

CYBERSECURITY LEGALITIES

ABOUT THE COURSE

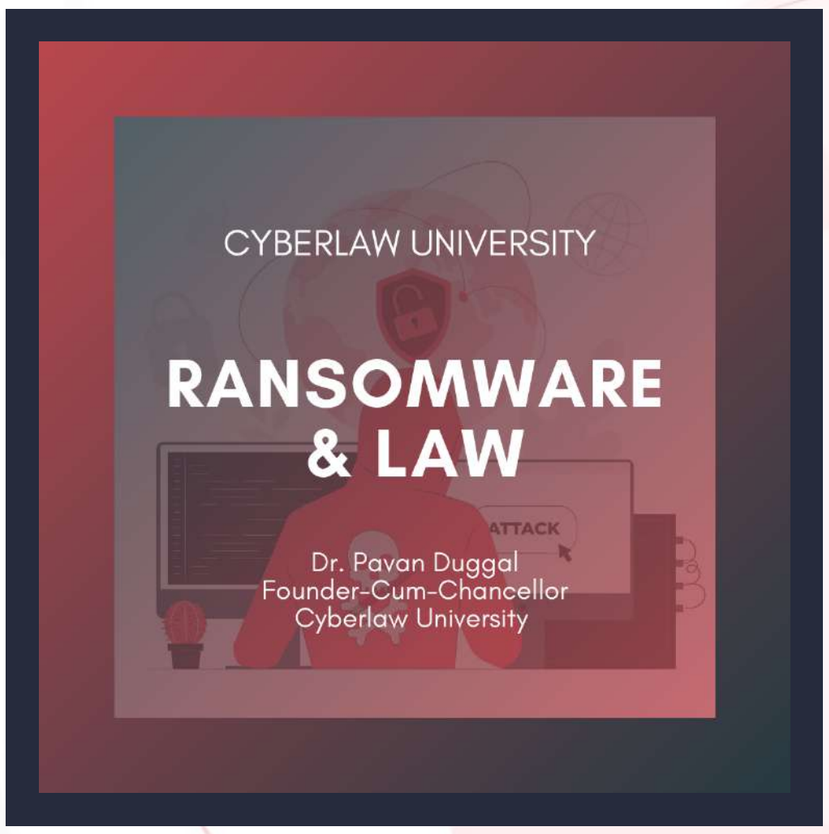
In this course, the students will have a broad overview of the emerging legal and policy issues impacting the protection and preservation of cybersecurity. Cybersecurity breaches are increasingly getting more and more prevalent.

COURSE CURRICULUM

- Introduction
- Data as new oil of data economy
- Kinds of cybersecurity breaches
- Lack of International Law on cybersecurity
- Budapest convention & cybersecurity
- National Cybersecurity Policies & Strategies
- Chinese regulatory approach on cybersecurity
- Chinese cybersecurity law - Features
- Cybersecurity regulation in another countries
- Jurisdictional Challenges
- Cyber sovereignty
- Encryption as Challenge
- Bilateral Cooperation on Cybersecurity
- International Cooperation on Cybersecurity
- Vacuum at International level on cybersecurity regulation
- Cybersecurity in outer space
- Artificial intelligence & cybersecurity
- Internet of things & cybersecurity
- Grave Figures About Cybersecurity Breaches
- Cybersecurity Risks Ahead
- Future Growth of Cybersecurity Law
- Conclusion

RANSOMWARE & LAW

ABOUT THE COURSE



The present course on Ransomware & Law seeks to provide a broad understanding of how ransomware as a phenomenon is constantly increasing and the various legal and policy ramifications thrown up by ransomware attacks.

This course is seeking to give you a bird's eye view of the key important elements concerning ransomware attacks that you need to know in your professional life. The focus of this course is clearly to build capacity to fight the growing menace of ransomware as a predominant cyber security breach vector of today's times.

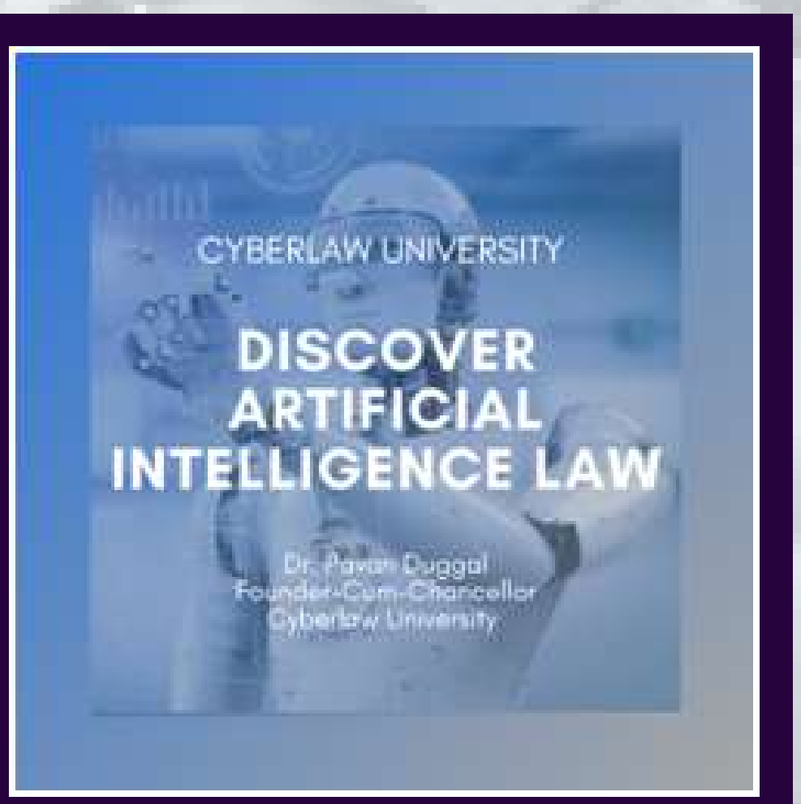
This course would be of value to any stakeholder in the digital ecosystem who is concerned about cyber security and who wishes to understand about the growing paradigm of ransomware attacks and the connected legalities pertaining to ransomware.

COURSE CURRICULUM

- Introduction
- Introduction
- Cyber security missing in cyberspace
- Data – new oil and cyber attacks
- Challenges in collection of incriminating electronic evidence
- Covid-19 legislations
- Major forms of ransomware
- Ransomware as malicious program
- Ransomware as phenomenon
- Ransomware and related perspectives
- Attribution and ransomware
- Growing incidents of ransomware
- Metaverse – The New Internet
- Digital divide, ransomware and cyber breaches
- Ransomware and Artificial Intelligence
- Ransomware and cyber disputes
- Impact of ransomware on data entities
- If your documents gets robbed by ransomware attacker, then how will one get to know that who has done it, and what are the legal steps that need to be taken?
- If a person is in India, and some other person from some other country, and he has engaged himself in an activity of cybercrime with a person situated in India, and the person needs to lodge a complaint, since there are no international laws regarding cybercrime what will be the legal remedy for the same?
- Many different countries are coming with their own laws regarding data security and cyberspace privacy, then it that case is it viable that different countries have different laws in such a globalized world as different countries have different interest and different prospects regarding their law. When we see that cybercrime is increasing because of people indulging more and more into the internet, then what is the minimalistic way of life in cyberspace will be good to be safe.
- Conclusion

DISCOVER ARTIFICIAL INTELLIGENCE LAW

ABOUT THE COURSE



This course will give a brief introduction to the emerging new legal discipline of Artificial Intelligence Law and would sensitize the students to the amazing world of legal complexities thrown up by the advent of Artificial Intelligence. This course will enable the students to have a broad understanding of some of the more significant legal, policy and regulatory issues concerning Artificial Intelligence.

This course will also highlight some of the practical challenges being faced today, in applying actual world laws to the emerging paradigm of Artificial Intelligence. This course further will sensitize the need for coming up with pragmatic, flexible and fresh legal perspectives while dealing with numerous challenges thrown up by Artificial Intelligence.

COURSE CURRICULUM

- Introduction
- Data as new oil of data economy
- Kinds of cybersecurity breaches
- Lack of International Law on cybersecurity
- Budapest convention & cybersecurity
- National Cybersecurity Policies & Strategies
- Chinese regulatory approach on cybersecurity
- Chinese cybersecurity law - Features
- Cybersecurity regulation in another countries
- Jurisdictional Challenges
- Cyber sovereignty
- Encryption as Challenge
- Bilateral Cooperation on Cybersecurity
- International Cooperation on Cybersecurity
- Vacuum at International level on cybersecurity regulation
- Cybersecurity in outer space
- Artificial intelligence & cybersecurity
- Internet of things & cybersecurity
- Grave Figures About Cybersecurity Breaches
- Cybersecurity Risks Ahead
- Future Growth of Cybersecurity Law
- Conclusion

MOULDING ARTIFICIAL INTELLIGENCE LAW IN FUTURE

ABOUT THE COURSE

In this course, students get to have a first-hand exposure to the various artificial intelligence legislations and legal provisions passed across the world. These are legal provisions which have been made as part of existing law so as to enable and regulate artificial intelligence in this. In this course, students will also get to know more about the other existing developments concerning artificial intelligence law, which have already taken place in different parts of the world in which developments are likely to further contribute to the evolving jurisprudence concerning artificial intelligence law.

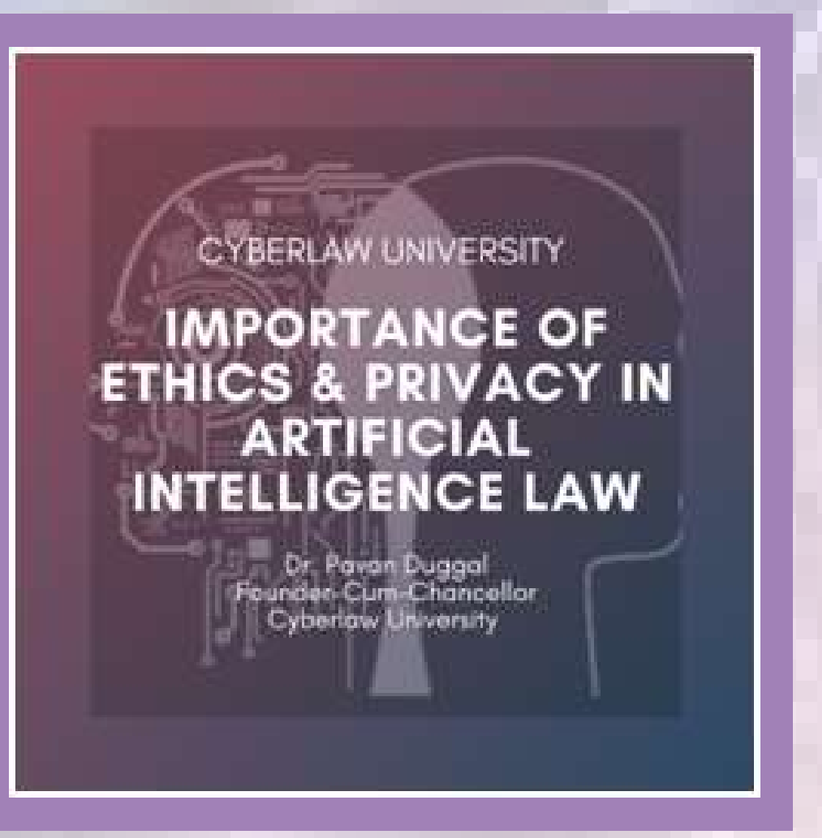
This course will give the students a clear understanding of existing artificial intelligence laws and developments in the actual world in which legal provisions and developments are likely to be the foundational foundation for the further evolution of artificial intelligence law jurisprudence in the coming times.

COURSE CURRICULUM

- Introduction
- Application of Artificial Intelligence & Artificial Intelligence Law
- Further Application of Artificial Intelligence & Legal Issues
- Facts & Figures About Artificial Intelligence
- Additional Artificial Intelligence Statistics
- Need For Legally Defining Artificial Intelligence
- US Legal Definition of Artificial Intelligence
- New Artificial Intelligence Law on Recruitment
- Preamble of Illinois Artificial Intelligence Law
- Disclosure of the Use of Artificial Intelligence Analysis
- Prior Notice Necessary
- Duty to Explain Artificial Intelligence Working
- Obtaining Prior Consent For Being Evaluated by Artificial Intelligence
- Discretion to Employees Using Artificial Intelligence
- Duty Of Destruction Of Videos
- Position Of Illinois Artificial Intelligence Law
- Grey Areas Of Illinoi Artificial Intelligence Law
- Law Lacking Penal Provisions and Opt-out Options
- Other Deficiencies Of Illinois Artificial intelligence Law
- White House Artificial Intelligence Principles 2020
- Significance Of White House Artificial Intelligence Principles 2020
- Introduction to China's AI Governance Principles
- China's AI Governance Principles
- China's Judgment on AI Written Articles Being Copyright Protected
- China's AI Powered Judge
- Projected Figures About AI Impact
- Future Ahead For AI Law
- Conclusion

IMPORTANCE OF ETHICS PRIVACY IN ARTIFICIAL INTELLIGENCE LAW

ABOUT THE COURSE



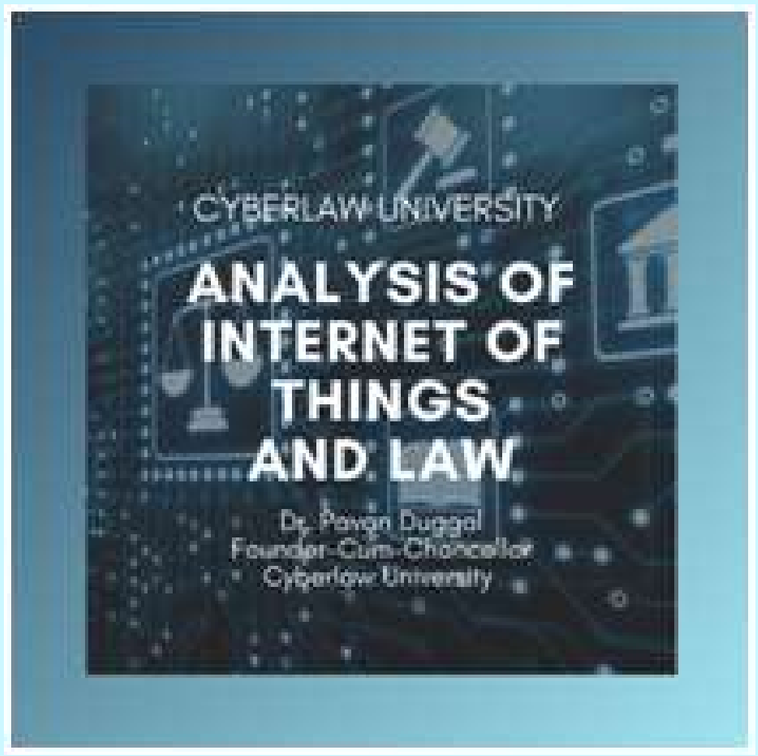
This course provides a holistic perspective of some of the important issues and topics that are gaining significance in the evolving Artificial Intelligence Law discipline. This course deals with the importance of ethical principles and standards in Artificial Intelligence Law, the need for protecting and preserving the individuals' data and personal privacy, need for enabling data protection in the Artificial Intelligence paradigm, the relationship between cybersecurity and Artificial Intelligence and the emerging need of regulating Artificial Intelligence cybercrimes. This course further tries to highlight the directions in which Artificial Intelligence Law as an emerging discipline is likely to evolve, with the passage of time.

COURSE CURRICULUM

- Introduction
- Introductory Remarks
- Statistics – ChatBots& Virtual Assistants
- Statistics – Machine Learning
- Other Statistics A
- Other Statistics B
- AI & Ethics
- Legal Profession – AI & Ethics
- Morality & AI
- Morality Questions in AI
- Privacy & AI
- Privacy Norm & Their Incorporation in AI
- Privacy Violation by AI
- Applicability of Existing Privacy Law & AI
- Roles & Responsibilities of AI users
- Need to balance existing privacy legislations with AI
- Data protection in AI
- Applicability of existing data protection laws in AI
- Cyber security & AI
- AI and cyber security laws
- Responsibility of keeping AI secure
- Human monitoring of AI cyber security
- Cybercrime and AI
- Applicability of existing cybercrime legislations to AI
- Need for deterrence in AI cybercrime law
- Attribution of AI cybercrime
- Shutting down AI systems for cybercrimes
- Inequality and AI laws
- Challenges in AI Cyber Crime - Going Forward
- Misuse of AI
- Malicious use of AI
- Regulating malicious use of AI
- FaceApp – an AI legal case study
- Impact of AI
- Need for broad legal AI framework
- Road ahead for AI laws
- Conclusion

ANALYSIS OF INTERNET OF THINGS LAW

ABOUT THE COURSE



This course gives you an introduction of the legal, policy and regulatory issues impacting the Internet of Things. It takes you through a journey to discover the various complex legal issues that Internet of Things is beginning to throw up, including protection of privacy and cyber security and how different legal approaches are evolving to deal with these legalities and related nuances raised by IoT.

COURSE CURRICULUM

- Welcome to the course on IoT& Law
- Introduction
- Positives and Negatives of Internet of Things
- IoT & Statistics
- Statistics & Barcelona case study
- How IoT impacts your privacy?
- Breach of medical IoT devices?
- Internet of Things and Privacy
- Questions regarding Internet of Things and Privacy
- Privacy challenges on Internet of Things
- Difficulties in privacy protection
- California IOT law – Introduction
- Manufacturers' obligations
- Reasonable security features – elements
- Clarifications regarding interpretation of California IOT law
- IoT and Cybersecurity - An Introduction
- Distinction between computers and communication devices on IoT evaporating
- Duty to protect Cybersecurity in IoT devices
- Cybersecurity law & IoT
- United Kingdom report on consumers IoT products and associated services
- Common principles of UK proposed code of practice of security
- Other common principles contd.
- Defining IoT user rights on Cybersecurity
- Jurisdiction & Attribution in IoT
- Increasing frequency and cost of IoT cybersecurity breaches
- Interception, Surveillance and Monitoring in IoT
- Data protection &IoT
- Traceability and unlawful profiling on IoT
- Monitoring of data transmission on IoT
- Conclusion

WHAT IS BLOCKCHAIN LAW?

ABOUT THE COURSE

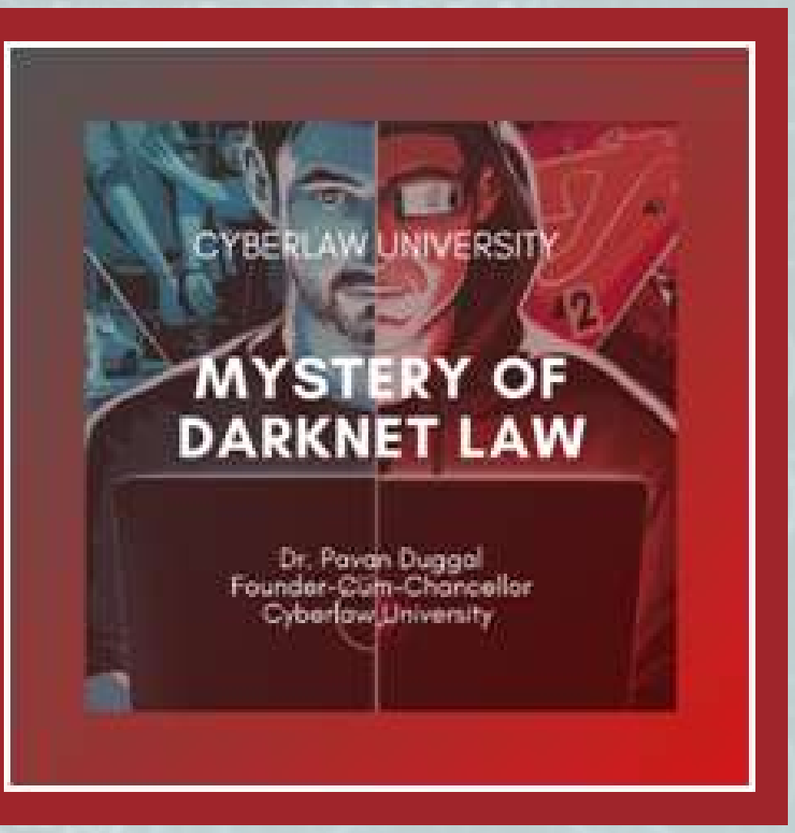
This course gives you an introduction of the legal, policy and regulatory issues impacting the Blockchain. It takes you through a journey to discover the various complex legal issues that Blockchain is beginning to throw up, including protection of privacy, smart contracts and liability of Blockchain service providers and how different legal approaches are evolving to deal with these legalities and related nuances raised by Blockchain.

COURSE CURRICULUM

- Welcome to the course on Blockchain and Law
- Introduction
- Understanding Blockchain
- Characteristics of Blockchain Ledgers
- Blockchain - Statistics
- Additional Blockchain Figures
- Government, Blockchain Pilot Programme
- Is Blockchain Legal?
- Blockchain and cybersecurity
- Challenges of cybersecurity for blockchain
- Additional cybersecurity risks to blockchain
- Existing Cyberlaws and Blockchain
- Malta's Blockchain laws
- Malta's innovative technology
- Malta's Financial Assets Act
- Belarus law on crypto-currency
- Belarus legal recognition of smart contract
- Need for new Legal framework on Blockchain
- Legality of Blockchain, Ledger and Entry
- Nevada Law defining blockchain
- Blockchain Legislation in United States
- Delaware Law on Blockchain
- Blockchain and Privacy
- Liability of Blockchain Service Providers
- Banking - Blockchain and Privacy
- Smart Contracts - An Introduction
- Smart Contract, Blockchain and Legalities
- Trustless trust in blockchain contracts
- Legality of blockchain contracts
- Consent and frustration of blockchain contract
- Projected statistics about blockchain
- Future projections about blockchain
- Trends emerging in blockchain cases around the world
- Conclusion

MYSTERY OF DARKNET LAW

ABOUT THE COURSE



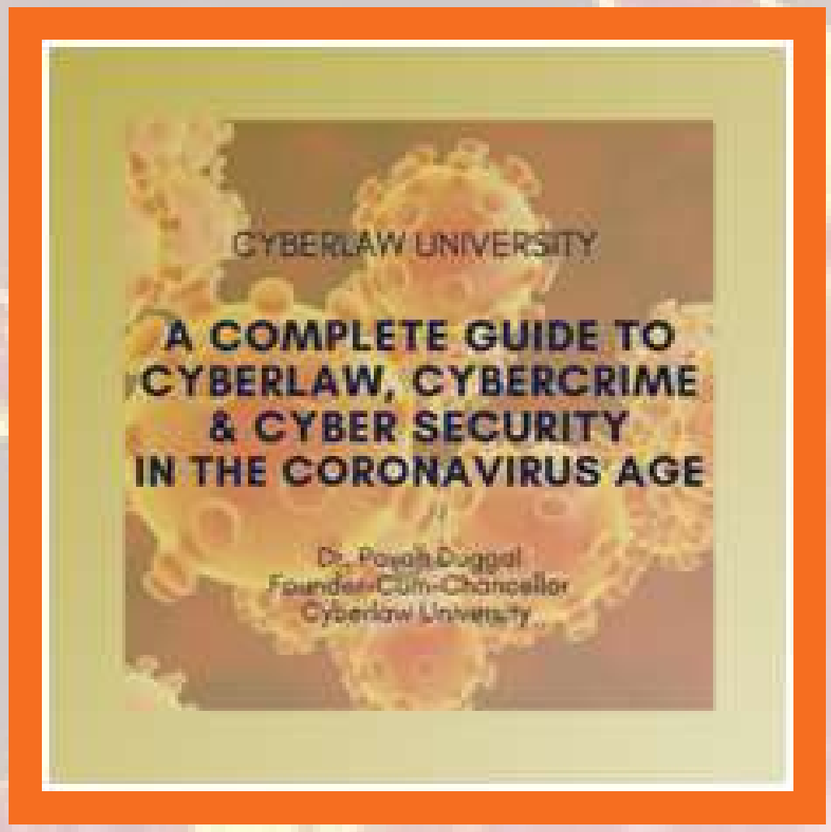
In this course, students will get a broad overview about Darknet being in that portion of the Internet wherein cybercrime is a default economic activity and wherein all kinds of criminal activities and acts are being done. In this course, students will also get to learn about the various practical legal policy and regulatory issues and challenges that the advent of Darknet is beginning to throw up. In this course, students will also learn how the legal jurisprudence pertaining to Darknet is at a very early stage of its development, and how there is a need for coming up with appropriate innovative legal strategies and approaches so as to deal with the emerging legal challenges thrown up by the Darknet.

COURSE CURRICULUM

- Introduction
- Concept of Darknet
- Definition and Features of Darknet
- Facts About Darknet
- Due Care and Caution on Darknet
- Positive use of Darknet
- No International Law on Darknet
- Regulating Cybercrimes on Darknet
- Categories of Darknet Crimes
- Governmental Approaches to Darknet
- Silk Road & Operation Onymous
- Cryptocurrencies on Darknet
- Legality of Darknet Transactions
- Legality of Darknet Contract
- Annonimity on Darknet
- Privacy on Darknet
- Data Protection on the Darknet
- E-Evidence Issues on Darknet
- Darknet Jurisdiction
- Darknet Encryption
- Legal Liability of Darknet Service Provider
- Cyber Terror on Darknet
- Cybersecurity Breaches on Darknet
- Statistics
- Conclusion

A COMPLETE GUIDE TO CYBERLAW, CYBERCRIME & CYBER SECURITY IN THE CORONAVIRUS AGE

ABOUT THE COURSE



In this course, the students will have broad overview of some of the key important Cyberlaw, Cybercrime & Cybersecurity aspects, issues and challenges that are beginning to crop up on the landscape given the advent and further constant spread of the coronavirus contamination.

With increasing reliance on the internet, every person needs to know about the cyberspace challenges and issues that are beginning to emerge in the coronavirus age. Knowing these cyber legal, cyber criminal and cyber security ramifications emerging in the coronavirus age would enable all stakeholders to be better well prepared to deal with these respective challenges and to avoid becoming victim of cybercrime and cyber security breaches.

COURSE CURRICULUM

- Introduction
- Coronavirus Current Figures and Impact on Economic Activities
- Relationship with Cyberspace Activities
- Relationship with Cyberspace Activities
- Coronavirus as an Infodemic
- Massive Increase in Cybercrime and Cyber Security Breaches
- Growing Facts & Figures
- Warning of European Central Bank
- Cyberlaw Developments in South Africa
- Kenya Arrest Over Coronavirus Fake News
- Indian Arrest Over Coronavirus
- Latest Cases on Cybercrime
- Increased Phishing Instances
- Important Cyber Security Breaches and their Characteristics
- Bruno University Hospital Case
- Cyber Attacks on US Health Department
- Cell Phone Surveillance Reported From Israel
- Phishing targeting Hospitals
- Coronavirus Mobile App
- National Cybersecurity Laws
- Increasing Fake News Related to Coronavirus & Its Regulation
- Situation Expected to Worsen
- Practical Tips to be Safe from Cybercrime and Cyber Security Breaches
- Projected
- Trends
- Working
- From Home and connected Issues
- Conclusion

WORK FROM HOME LEGAL STRATEGIES DURING CORONAVIRUS

ABOUT THE COURSE

In this course, the students will have a broad overview of how increasingly employers are resorting to allowing their employees to Work-From-Home, given the advent of coronavirus and how the Work-From-Home concept has brought in far more new distinctive legal and policy challenges which need to be addressed by all stakeholders, whether it be private institutions, organizations, employers as well as employees.

Both from the perspective of employers and employees, this course provides important insights of what needs to be kept in mind by various stakeholders as they go forward in the direction of trying to understand the nuances of Work-From Home in today's times when the coronavirus infection is constantly increasing with each passing day.

COURSE CURRICULUM

- Introduction
- Coronavirus - Advent and Constant Growth
- Coronavirus & Economic Impact
- Work from Home and It's Relevance
- Cybersecurity in Coronavirus Age
- About The Lecture Cybersecurity at Work from Home Premises
- Cybersecurity at Work from Home Premises
- Cybersecurity Challenges and Legal Liability for Companies
- Corporate Liability for Cybersecurity Breaches
- Need for Strong Telecommuting or Work from Home Policy
- Important Elements of Work from Home Policy
- Spelling Up of Employee Expectations
- Precautions By WFH (Work from Home) Employee
- Corporate Responsibility for Health & Safety
- Liability for Employee at WFH Premises
- Salient Principles from Code of Practice 2000
- Working from Home & Child Rearing Interference
- Monitoring of Devices Used in WFH
- Duty to Record Time Keeping
- White House Memo on Telework
- Corporate Declaration on WFH in Exceptional Circumstances
- Employee Benefits as per Local Laws
- Proactive Duties of WFH Employee
- Coronavirus & Cybercrime
- Phishing in Coronavirus Age
- Tips to avoid becoming Coronavirus Phishing Victim
- Coronavirus & Fake News
- Increasing Cybersecurity Breaches in Coronavirus Age
- Conclusion

NEW CYBER WORLD ORDER POST COVID-19

ABOUT THE COURSE

In this course, the students will be able to have a broad overview of some of the key remarkable irreversible challenges that are happening in cyberspace thanks to the advent and outspread of COVID-19. By doing the present course, you will be benefitted in the following manner:

1. **You will get an overview of the deep yet swiped challenges impacting cyberspace during COVID-19 times;**
2. **You will further get to appreciate new**
3. **challenges in cyberspace which are ushering in New Cyber World Order;**
4. **How the New Cyber World Order will impact you and your life;**
5. **What elements you need to keep in mind in order to be prepared for the new cyber age that awaits for us after the**
6. **fight against COVID-19 comes to close;**
7. **You would be able to have far more clarity on interpreting broad manner of emerging trends in cyberspace and how the same are likely to impact digital liberty;**
8. **You would also learn more about the effect of the Ne Cyber World Order on growing cybersecurity breaches and cybercrime.**

COURSE CURRICULUM

- Introduction
- Advent & Outspread of COVID-19
- Internet & Cyberspace
- Impact of COVID-19 on Internet
- New Cyber World Order
- Definition
- Historical Perspectives
- Some Broad Trends – New Cyber World Order
- Consolidation of State Power
- Cyberlaw to play Important Role in New Cyber World Order
- Cyber Security Breaches
- Cybercrimes
- Impact on Digital Liberties
- Migration to Darknet
- Need to be prepared
- New World Awaits Us Post COVID-19
- Conclusion

Cyberlaw Univ

FOR MORE INFO:

www.cyberlawuniversity.com

info@cyberlawuniversity.com

cyberlawuniversity@gmail.com