RAMA UNIVERSITY
www.ramauniversity.ac.in

FACULTY OF JURIDICAL SCIENCES

COURSE:BA.LL.B

Semester : VIII th

SUBJECT: Cyber Law

SUBJECT CODE:BAL-805

NAME OF FACULTY: Dr.Puja Paul Srivastava

Lecture-2

LECTURE 2: Jurisprudence of cyber law

Jurisprudence can be defined as the science and philosophy or theory of the law. Applying jurisprudence to cyber law gives rise to the legal study that concentrates on the logical structure, the meanings and uses of its concepts, and the formal terms and modes of operation of cyber law. Cyberlaw is a very recent concept and if compared with other older branches of the law, is a little structured study.

The term cyberspace was originally coined by a science fiction writer William Gibson to depict data matrices existing in a dark distant future which means the information spaces made by the technology of digital networked computer systems that ultimately connect with the mother of all networks that is the Internet. With the advent of the internet and technology, cyberspace along with a number of crimes related to the same emerged and expanded. As we enter the cyber age, the law on all fronts is struggling to keep pace with technological advances in cyberspace. While there is a prosperous discussion of the nature of cyber law and its challenges, still a

fundamental body of scholarly contributions to the discussion is lacking. The outgrowth of cyber jurisprudence around the world has promoted the emergence of newer dimensions in Law. The focus is on the practical aspect of cybercrime with the initial attempt to extend the known physical society concepts to the virtual space rather than the theory, philosophy, and science of cyberlaw generally. Hence in due course, we need to develop separate Cyber Jurisprudence to deal with future disputes.

The modern jurists have been cautious to endow with the rationale pedestal of jurisprudence to this ruling and now ascertained utmost exact definition of cyber jurisprudence as this describes the principles of legal issues, which exclusively regulates the cyberspace and internet can be termed as cyber jurisprudence with a virtual approach[1]

Jurisprudential Aspects of Cyber Laws

Cyber jurisprudence gives an analysis of the land with land and no border, different from the physical world, they may be virtual from origin and nature. This covers the virtual world with virtual rules and policies, along with the virtual subject matter, virtual contracts, virtual disputes, virtual property, virtual possession, and virtual court.

The existence of an item in the context of a virtual world, such as an e-mail account or an online game, is also a form of virtual property. It emphasizes the composite idea of cyber jurisdiction, cyber court's venue in the cyberspace, and recognize uniform cyber rules and policies at the international level. Framing rules and laws to cover every aspect will be an arduous task since the cyber world has no boundaries.

However, a balance has to be maintained and laws be evolved in order to keep a check on cybercrimes.[2] Whenever a conflict is encountered in implementing existing laws of the real space to Cyber Space, the laws of the real space have prevailed, overtime this tendency is likely to develop into a principle of "Primacy of Meta Space" and become the bedrock of Jurisprudence.[3] However, the principle fails when two laws of the real space itself come into conflict in the Cyber Space.

Applying Jurisprudence to Cyber has three possible outcomes:

- ***There exists no relationship between jurisprudence in general and cyber law in particular:*** Here we return to The Law of the Horse. Everything existing at present is sufficient and determining outcomes with a special view to cyber science is unnecessary. No special philosophy or theory of law is necessary to treat events occurring in cyberspace.

- ***Such a relationship exists but it does not require a new jurisprudence to understand it:*** Here the cyber law is recognized as a special area of the law and acknowledges that current jurisprudential thinking is adequate to apply existing theory to its study and analysis.
- ***A new jurisprudence and a new view of cyberlaw are necessary:*** This concludes that cyber law is a special and unique field of the law and it requires a special and unique philosophical and theoretical treatment of its own.

Eventually, the question of whether is it feasible and necessary to create an extensible jurisprudential approach to law that acknowledges and keeps pace with cyber science without being a set of restrictive and inhibitory guidelines that are both confining and resistant to change should be taken into consideration.

Evolution of Cyber Law

Cyber Crimes

In India, Cyber Crime is not directly defined by either IT Act, 2000, IT Amendment Act, 2008, or any Other Legislation. However, the Offence or Crime has been defined by The Indian Penal Code 1860: as any Offence or Crime in which a computer is used is a Cyber Crime. Cyber or Computer Crimes were defined as unethical, unauthorized, and illegal behavior of Individuals or as Groups relating to the automatic processing and transmission of data use of Computer Systems and Networks.

Cyber Crimes are majorly classified into four types:

1. ***Against Individuals:***
    1. Harassment through E-Mails / Messages
    2. Cyber-Stalking
    3. Propagation of Obscene Material on the Internet
    4. Defamation
    5. Hacking/Cracking
    6. Indecent Exposure.
2. ***Against Property of an Individual:***
    1. Computer Vandalism
    2. Transmitting Virus
    3. Internet Intrusion
    4. Unauthorized Control over Computer System
    5. Hacking / Cracking
3. ***Against Organization:***
    1. Hacking & Cracking
    2. Custody of Unauthorized Information
    3. using Cyber Terrorism in opposition to the Government Organization
    4. Distribution of Pirated Software

4. ***Against Society at large:***
    1. Pornography (especially Child Pornography)
    2. Spoil the Youth through Indecent Exposure
    3. Trafficking

In India, the Cyber Crimes have grown from 9,622 and 11,592 to 12,317 during 2014, 2015, and 2016 respectively.[4] The National Crime Records Bureau (NCRB) and Indian Computer Emergency Report Team (CERT-In) had reported that approximately 80 phishing incidents affecting 20 Financial Organization, 13 incidents affecting various Automated Teller Machines, Point of Sales systems, and Unified Payments Interface (UPI).

Legislations

The principal source of cyber law in India is the Information Technology Act, 2000 (IT Act) with the primary purpose to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government. This Act penalizes various cyber crimes and provides stringent punishments including imprisonment terms up to 10 years and compensation up to Rs 1 crore. Some of the major Acts got amended after the enactment of ITA:

1. ***The Indian Penal Code, 1860:*** The word 'electronic' was added, thereby treating the electronic records and documents on a par with physical records and documents. The Sections dealing with false entry in a record or false document[5] have since been amended as 'electronic record and electronic document' to bring it within the ambit of IPC.
   Now, electronic records and electronic documents have been treated on par with physical records and documents during the commission of acts of forgery or falsification of physical records in a crime.
   The investigating agencies started filing the cases and charge-sheets quoting the relevant sections from IPC read with the ITA/ITAA in like offense in order to ensure that the evidence and/or punishment can be brought under its scope and be proved under either of these or both the legislation.

2. ***The Indian Evidence Act 1872:*** Before enactment of ITA, all pieces of evidence in a court were in the physical form only and now the electronic records and documents were recognized as the definition part of Indian Evidence Act was amended as "all documents including electronic records".
   Words like 'digital signature', 'electronic form', 'secure electronic record' 'information' as used in the ITA were also inserted after this amendment to be a part of the evidentiary importance under the Act.
   The identification and recognition of admissibility of electronic records as evidence as enshrined in Section 65B of the Act was seen as a significant amendment.

3. ***The Bankers' Books Evidence (BBE) Act 1891:*** Previously banks were required to produce the original ledger, other physical registers, and document during evidence before a Court but now the definitions part of the BBE Act stood amended as: "bankers ' books' include ledgers, day-books, cashbooks, account-books and all other books used in the ordinary business of a bank whether kept in the written form or as printouts of data stored in a floppy, disc, tape or any other form of electromagnetic data storage device"[6].
   This amendment in the provisions in Bankers Books Evidence Act recognized the printout from a computer system and another electronic document as a valid document during evidence, provided, such print-out or electronic document is accompanied by a certificate by a person-in-charge of computer system.

Jurisdictional Cyber Issues

Theories of Jurisdiction

As far a cyber law is concerned, the jurisdiction encompasses several discrete concepts, including jurisdiction to prescribe, jurisdiction to adjudicate, and jurisdiction to enforce.[7] The prescribing jurisdiction is a sovereign entity's authority to make applicable laws to the activities, relations, or status of persons, or the interests of persons in things by legislation, by administrative rule or by determination of a court, by executive act or order and jurisdiction to adjudicate is a sovereign entity's authority to subject persons or entities to the process of its courts or administrative tribunals to determine whether prescriptive law has been violated.[8] There are various theories of jurisdiction:

1. **Territoriality Theory:** It means that a sovereign state has the authority to judge criminal acts that have been committed in its territory. The place where the crime is committed has to be established for this to apply.
2. **Nationality Theory:** Also known as Personality theory, recognizes that a sovereign state can adopt criminal laws that govern the conduct of nationals while outside of its borders. This principle effectively makes it a crime for its nationals to engage in conduct that is not illegal in the place where the conduct is performed. This theory is further dealt with in two ways:
    1. **Active Nationality Theory:** This theory recognizes that a state may exercise criminal jurisdiction over its nationals based on their active nationality and can prosecute and punish its sovereign nationals for committing a crime outside its territory.
    2. **Passive Nationality Theory:** This theory provides for a sovereign to adopt criminal laws that apply to foreign nationals committing crimes against the sovereign's nationals while the sovereign's nationals are outside of the sovereign's territory.
3. **Protection Theory:** This theory provides for a sovereign to adopt a statute that criminalizes conduct that occurs outside of its borders and when that conduct affects the sovereign itself. The sovereign can make it a crime to engage in an act that obstructs the function of government or threatens its security as a state without heed to where or by whom the act is committed.
4. **Universality Theory:** This theory provides for a sovereign to adopt criminal laws applicable to the conduct performed by any person anywhere in the world when such conduct is recognized by nations as being of universal concern.
5. **Derived Jurisdiction Theory:** This theory cannot be treated as an independent basis for jurisdiction. If the state that has jurisdiction, so determines or authorizes a state that has no jurisdiction over certain acts according to its national laws or case law and embodied principles then it may assume jurisdiction. This can be carried out in the form of a formal request or based on an international treaty.

SELF-TEST QUESTIONS

S.NO	Question	Option (a)	Option (b)
1.			
2.			
3.			
4.			
5.			

Answers: 1-(),2-(), 3-(),4-(),5-()