Page 358 - 375 **DOI:** *https://doij.org/10.10000/IJLSI.11721*

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 3 | Issue 3

2020

Alliance of Indian Constitution and Indian Evidence Act with Cyber Laws

ANANTA AGGARWAL[1]

ABSTRACT

Cybercrime is developing and untangling at an alarming rate. As the users or servers of social media platform and digital workstation workers are increased the crime in the virtual world, that is cybercrime world. Cybercrime circumscribe all the fields as economic, digital stage, political and bank or corporate field.

This paper is an in – depth study of various modes of Cybercrimes in the world and the cross-country models of Cybercrime and Cyber security. This paper also gives a study about Information Technology Act, 2000 which is framed to adjudicate and justify the legislations about cybercrime and its punishments. Information technology Act, does not include or state the explanation of term define 'cybercrime'. Cybercrime means an illegal activity carried out or be blame to the use of computer or necessaries of a digital device or workstation indulged with them as data, documentation, software, and sites together as task – oriented or operational tool which further call forth for cyber-crime, hacking or dissent services and prohibition for use of services.

The goal for this study and analysis have four – fold: firstly, to explore, study and review the meaning of cybercrime, cyber – attack and cyber – security and to monitor the history and origin of cybercrimes; secondly, to examine and inspect various modes of cybercrimes and cyber – attacks; thirdly, to inspect and fractionate the provisions of Information Technology act,2000 with articles of Indian Constitution, 1950; and fourthly, to look over, research and examine the provisions of Indian Evidence Act, 1872 with cyber laws of India.

The historical genesis of cyber laws laid down its root in 1820. The first cybercrime is transcribed took place in the year 1820, by France textile manufacturer Joseph Marie, the device authorizes the reproduction of a service of procedure in wearing of special fabrics, this resultant in a fear of Jacquard's company's employees that their cultural application and livelihood was at stake, they perpetrate or enactment for course of action of couple to discard Jacquard from furtherance serving of technology. This was recorded as first cybercrime!

The proposition or approach of this paper relating to cyber laws and the field of cyber

[1] Author is a student at Amity Law School, Noida, India.

 [ISSN 2581-9453]

laws is that this research paper contains various modes of cyber-crime and cyber-attack across the world and in the second half or part of the paper there is study and genesis of two most important laws of the country that is Indian Constitution, 1950 and Indian Evidence Act. As it states and has laid a groundwork and structure that how both laws are co-related to cyber laws.

Keywords: *cybercrime, cyber security, information, evidence, digital device, technology*

I. INTRODUCTION

Since the genesis of civilization, man has always inspired by different needs, desires of human being, the development process took place after inception scientific era in India. This helps man to take development in science and technology field to a new greater height, by launching and inventing various digital gadgets and scientific formulas.

Later, in time, there was emergence and unfolding of internet which turn the lives of man upside – down, as it does work in just few seconds which previously took hours or days. It helps in sending message, telephonic conversations, pictures Capturing moments in digital form and many more. In just few days many people of society operate and have control over internet,

But as some big things comes in small packets, the internet is same or look like a coin, which simply means internet is two faced. It also has its negative consequences on the people. As people gradually started misemploying the internet. By doing criminal activities or wrongdoings which are offence in eyes of law which are given or coined as "Cyber Crime"

The virtual world of internet is also called as virtual community or fiber – optic cables and the rules and laws guarding and safe guarding this virtual reality are called as Cyber Laws. Cyber Laws can be portrayed as that part of law that counterpart with bonafide and de jure issues relating to the application of inter network information telecommunication and mechanizations.

We can also say that the cybercrime is a non – profitable crime as to disclose the secrecy and confidential data of a person or a company or organization by hacking its computer system or any other unlawful or mud – slinging way as to cause financial loss to individual or company.

By this we can articulate or bring forward two overhanging spheres or elements of computer crimes or digital crimes that are –

- First sphere, related to illegal activities carried out or be blame to the use of computer and gubbins or necessaries indulged with them as data, documentation, software's, sites together as task – oriented or operational tool which further call forth for cyber-crime, hacking or dissent services and prohibition for use of services.

- Second sphere, relate to protection of data, and information which is used by unsanctioned and illicit ways which encompass property law, company laws, privacy laws and intellectual property laws.

This research paper deals with various mode cybercrimes and further explored the overlapping and alliance of cyber laws with constitution of India and Indian Evidence Act provisions.

History of Cyber Laws[2]

Internet fraud consistency scheme serving webchats', chatrooms, email, to put forward fictitious goods and services to consumers or to telecast false information. Cyber fraud has the capability of hampering the economic and civil enlargement of any nation, Cyber fraud distrust the good and righteous values.

The first cybercrime is transcribed took place in the year 1820, by France textile manufacturer Joseph Marie, the device authorizes the reproduction of a service of procedure in wearing of special fabrics, this resultant in a fear of Jacquard's company's employees that their cultural application and livelihood was at stake, they perpetrate or enactment for course of action of couple to discard Jacquard from furtherance serving of technology. This was recorded as first cybercrime!

II. VARIOUS MODES OF CYBER-CRIME ACROSS WORLD[34]

(A) Social Engineering and Phishing -

1. Cyber-criminal ensures that to target or dig out those people who easily post their personal information on social media. In this type of cyber – crime criminals attack those users who have actually do not think and have a simple psychological and intellectual thought process as they can be easily be fool or get manipulate and can exploit them. The process is that they send messages from their friend's ID for urgent financial help and user does transaction in

[2] Cyber Laws Overview, https://taxguru.in/wp-content/uploads/2012/10/cyber-laws-overview.pdf, (last visited Feb. 15, 2021)
[3] Regner Sabillon, Jeimy Cano, Victor Cavaller, Jordi Serra, Cybercrime and Cybercriminals: A Comprehensive Study, Vol-4. No-6, International Journal of Computer Networks and Communications Security, 165, 166-171 (2016)
[4] Tariq Rahim Soomro, Mumtaz Hussain, Social Media – Related Cybercrimes and Techniques for Their Prevention, vol.24, no.1, Sciendo, 9, 11-13 (2019)

minutes being a foolish and stupid. This led to fraud and wrongful gain.

2. It is criminal offence using social engineering and technical subterfuge to break – in consumer's personal identity details and financial credentials.

(B) Credit Card Fraud -

It is an identity theft fraud where illicit or wildcat people uses credit card information of an individual and do purchases and withdraw cash from card. This is done by tracing or by unguarded and forbidden ways for acquiring confidential information from different sites.

(C) Cyber – Crimes against women

1. Cyber Stalking

- It is done through social networking sites. Stalking further cause's mental and emotional torture to the person.
- Cyber Stalking is a heinous crime, which is to keep a close track on each step pf user and try to get intimidate by sending her sexual content and try to make out with her. This can only be stopped by a police complaint in cyber cell or department of police.

2. Cyber Hate Speech

This is giving a hate speech related to a famous personality, individual, political or religious organization or a company on social media platform. This causes defamation and disrespect to the user. This further led to the contempt and discourtesy to the user on the social media platform.

3. Cyber Bullying

It includes directions of communication network to harass and mental torture the person. It later gives rise to distribution or sending of nasty images, call recordings or videos of cyber bashing to mock the person and lampoon the individual.

4. Cyber Stalking

- It is done through social networking sites. Stalking further causes mental and emotional torture to the person.
- Cyber Stalking is a heinous crime, which is to keep a close track on each step of user and try to get intimidate by sending her sexual content and try to make out with her. This can only be stopped by a police complaint in cyber cell or department of police.

5. Cyber Grooming

This is a mechanism which pedophile a relationship between person and attacker which foster to sexual molestation or blackmailing. This can be avoided by not interacting and chatting with strangers on social media platforms.

(D) Cyber extortion

Attacker's nag and oppress victim and victim in order to avoid cybercrime he has to fulfill his demand or pay him in cash or kind. As to remove cyber – threat or stop cyber – attack the attacker also indulge individual in high – risk and dangerous task.

(E) Cyber Intrusion and Data Breaches

- Cyber intrusion is done by stealing someone's personal data and attachments from social media platforms and other networking sites and using that information for their dangerous and corrupt plans.
- Data breach is a commotion wherein information is stolen or misappropriation from a system without the knowledge and endorsement of the owner. Stolen data is sensitive, confidential and of national security.

(F) Malware Attack

1. Venomous and nasty software that is installed by various fraudulent ways. The various sub – categories of malware –

i. Virus – Treacherous code that recreate itself and require execution in a way to destroy the system.

ii. Worm – Self – reproducing code that transmits through network without any interference and information of owner.

iii. Trojan Horse – This gets conceal within a valid application and gets activated within a few seconds of its installation and create backdoors, delete files and disable the internet service from the system.

iv. Ransom ware – Shakedown malware that hide and bolt users' information in order to blackmail and earn money.

2 Virus is a malware that spread by injecting its copy to become and intrinsic of another part. There is transmission of virus from system to system. Worms also cause a similar damage. They recreate their functional copies and damage the system.

3 A 'bot' is a type of malware which hackers bring into play to operate and administer an infected or contaminated system or networks connected and is managed under a single

hacker.

4. Social media accommodate an excellent platform for spreading viruses and malware. Producers of adware, malware and viruses conceal their death – dealing programs in links, attachments and messages which are an easy go task in any of the networking sites. Once the costumer replies to it, the virus enters the system and start ruining the system without any information to user.

(G) Hacking

- Hacking is reconstructing, violating and invading a hardware and software of a digital device which is not his personal property and he is not his creator. Hackers are individual who cater in such programming skills which provide them high level knowledge and can have command in handling the entire set up.
- Hacking – Hacking is to get hands on knowledge of computer and security or 'self – expounding' about computers and security. People who are held responsible for attacking and destroying computers or any digital device are known as "hackers".

Various categories and sub – groups of Hacking are:

- White Hats – individuals who work under restrictions and guidelines of 'hacker ethic' as not to cause harm or for security purposes.
- Gray Hats – the phrase was profound by Lopht. These hackers are best acknowledged as old school hacking groups. They work as security consultants.
- Black Hats – hackers are provoked by anger, power and hatred. They do not give a second thought or hesitate before stealing or dismantling a network in which they trespass or invade.

Sub – groups of Hacking:

- Elite – they have information, knowledge and skills of top most grade of hacking. This status is gained by popular hackers, maneuvers and endured phase.
- Script Kiddies – this is most disdain group within the hacking community. As they are youngest and most unskilled hackers and serve those cat paws which are established by elite hackers.
- Cyber – Terrorist – They use stenography and cryptology for swapping details, documents and directions. They are motivated by social and political groups as to disrupt the security system or grasp the information of other nation's security or other

national policies. This operation is done to target or bull's eye on a specific military operation of a nation to cause threat or damage to defense system of a country and further relates to cyber – terrorism.

- Disgruntled (ex) Employees – One of the most threatening and publicized groups. These people lose their corporate sector jobs or work, and take retaliation or do tit for tat by hacking their system and entering viruses or worms in their systems.
- Virus Writers – These hackers' enterprise the weakness of other hackers and then code or phrase these methods to do foible in their systems.
- Hacktivist – These people attack political, social or religious agendas of groups as to deficit their website and establish a denial of services feature to disgruntle the functions of website.
- Suicide Hackers – Individuals motivate to slope down the deprecatory infrastructure for radical causes who are afraid for going jail. They have links with suicide bombers and can lead to cyber – terrorism.
- Spy Hackers – These hackers' contract for stealing or capturing trade secrets of a company and to become a part of corporate world and for gain of cash, these hackers do these odd jobs.

(H) Cyber – attacks

- -Advanced Persistent Threats (APT) – APT is a combatant process that possesses worldly – wise and knowledgeable levels of expertise and consequential resources to grant opportunities to target its objectives by using variant attack vectors. Its main objective is to reduce an elongated time - span and to adapt efforts or skills for grade of conformity with the costumers. The attack cycle aims at target discovery, data, research and intelligence trumpet.
- Remote Code Execution – This is the procedure to execute malware remotely in order to deceive and take or hold on the system.
- ARP poisoning – Address Resolution Protocol misguide inter – related gadgets of the original MAC machine. It enters the system by popping up a request and create a reply encase which take the piss off and trick a game which make a hole for poison.
- Bluejacking – A message is sent via Bluetooth device without permission of owner, which can also contain sound effect. This prey the control of device in a no – disclosure mode.

- Cookies and Attachments – Cookies can engulf web – browsing history and malicious secretive data. This led to an attack of session hijacking which target main attachments and cause virus and worms' attack.
- Cross – site Request Forgery - This is to create misleading HTML links and redirecting the users to perform some specific instructions.
- DNS poisoning – Domain Name System poisoning is attack to change or reshape the cached DNS results. The major threat is the reproduction of DNS information to Internet Service Provider and cached in the system.
- Evil twin – Rouge access point attack which structure and aligned a new WAP (Wireless Access Point) with same SSID (Service Set Identifier), or free Wi – Fi. This led to theft of confidential data which is done by using public Wi Fi services.
- Spoofing – This attack is done to change IP address and email address as to cancel and secure the attackers identity, through which they can easily delete some important files by taking control of the device.

III. CYBER LAWS OF INDIA

As Cyberspace is a spectral and bodiless dimension that is impossible to regulate and safeguard using conventional law. The chief or foremost source of cyber law in India is the Information Technology Act, 2000. Most of cyber-crime cases are committed by educated person. So, it is required the deep knowledge about the cyber –crime and its prevention. Also, in India most of the cases found where, crimes are committed due to lack of knowledge or by mistake.

Information Technology Act, 2000[5]

This act lays down legislation and rules and regulations to deal with cybercrimes or computer – oriented crimes and to promote cyber security. This act provides legal remembrance for transactions carried out by mode of electronic devices, electronic data, computer system and other electronic or internet connected spheres.

Important Terms related to Cyber Laws:

1. Address – This is a person's plan or aspire to develop/ originate 'id' to acquire and secure electronic data.

[5] A2000-21.pdf, https://www.indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf, (last visited Feb. 22nd, 2021)

2. Communication Device – Communication devices denotes to electronic gadgets which helps in private digital assistance and impart or transmit both audio and video messages and conversations[6].

3. Computer – A mechanical, automatic, ocular or other turbo and whistle top data processing device or system which implement analytical, reasoning, arithmetic functions by deceive of electronic, automatic, magnetic, stimulus and consist of input, output, processing, storage, computer software or telecommunications functions which are co-related and fining to the computer in a digital workstation or computer network[7].

4. Computer – Network – Computer – Network means entanglement of grid of one or more computers or computer systems or transmitting gadgets through: -

   (i) The utilization of secondary planet or space capsule, microwave, earthbound line, wire, wireless or other communication media and

   (ii) Concluding or a nexus consisting of one or more interconnected computers or workstations whether or not the grid or chain is uniformly structured[8].

5. Computer System – Computer system means a device or assembly or devices, consisting of input and output assistance device and separation of calculators which are not function able and potential of being in coincidence with superficial or extrinsic files, which contain digital workstation, electronic directions and guidelines, input and output data that perform logical, reasoning, mathematical data storage and resurgence, communication control and other functions[9].

6. Data – Data means presentation of knowledge, statistics, factuality, directions, postulations, which are being stimulated or have been structured in a formal manner, and is hell bent to be processed, or processed in a digital device and may be in any form (consisting of computer printouts, Captivating or visual storage media, punched cards and tapes) or stored purposefully in the memory of computer[10].

7. Digital Signature – It means attested and legitimate of any electronic record, by a signer or attester by means of an electronic method or course of action[11]. [sec 2(1)(p)]

[6] IT Act, 2000. sec. 2, § 1, cl. (ha)
[7] IT Act, 2000. Sec. 2, § 1, cl. (i)
[8] IT Act, 2000. Sec 2, § 1, cl. (j)
[9] sec2(l)(l), IT Act, 2000. sec. 2 § 1, cl. (l)
[10] sec 2(1)(o), IT Act, 2000. sec. 2 § 1, cl. (o)
[11] Sec 2(1)(p), IT Act,2000. sec. 2 § 1, cl. (p)

8. Electronic Record – It means data, record, data produce, picture, sound stored, obtained or sent in an electronic form or micro film or digital workstation manufactured micro fiche[12].

9. Secure System – Secure system means workstation hardware, software and course of action that[13]:-

   (a) Are rationale safeguard from unsanctioned eruption seizure and misemploy;

   (b) Anticipate an equitable level of constancy and correct operation;

   (c) Are practically located to function the desired programs; and

   (d) Hold fast and cohere to formally adopt security operation.

Some of Offences under the Act[14]

Section 43: - [Penalty & Compensation] for damage to computer, computer system etc.:

Whosoever without the authority of owner, or who possess the system, extract or get hold of computer, computer system or network: -

(a) Acquire or affiliation approach such computer, computer system or network and resource.

(b) Reproduce, duplicate or distillate any data, database, information from such computer, computer system and network consisting of information or data stored in a detachable storage mode.

(c) Detroit or genesis to be dismantling any computer, computer system, network, data computer data base or any programmers repose in such computer, computer system or network.

(d) Institute or launch or convict to be introduced in any computer contaminated or computer virus into computer, computer system or network.

(e) Disorganize or cause deranges such computer, computer system or network.

(f) Dissent or cause rebuttal of outpouring to any person command or such computer, computer system or network by any medium.

(g) Grant any support to any person to expedite outburst to a computer, computer system or network in contrast of provisions of this Act, rules and regulation stated.

[12] Sec 2(1)(t), IT Act, 2000. sec. 2 § 1, cl. (t)
[13] Sec 2(1) (ze), IT Act,2000. sec. 2 § 1, cl. (ze)
[14] Offence under Chapter XI, IT Act, 2000

(h) Tariff the services 'aid ed' by a person to account of another person by tinkering or exploiting any computer, computer system or network.

(i) Destruct, remove, modify any information inhabit in a computer resource or shrink its value or use or affects it dangerous by any means.

(j) Theft, hide, destruct or modify or causes any person hide, steal or destruct any computer source, code served by a computer resource with an aim to dismantle the system.

Shall be punishable to pay damages by way of reimbursement to person so work on.

Explanation: - For the requirement of this section: -

1. Computer contaminant means any set of computer directions that are framed: -

(a) To change, destruct, transfer or document program residing within a computer, computer system or network.

(b) By any means to seize the normal conduct of computer, computer system or network.

2. 'Computer database' means a depiction of information facts, concepts or directions in text, image, audio, video that are being put together in a standardize method it gave been generated by a computer, computer system or network and motive for use in computer, computer system or network.

3. 'Computer Viruses' means computer specification, data, programme or manual that destruct, breakdown, deface or adversely affect the performance of a computer resource or attract itself to another computer resource and set off when a programme data or instruction is contemplated or some other events of computer resource.

4. 'Damage' means to change, destruct, regroup, any computer resource by any medium.

5. 'Computer Source Code' means jotting down list of programmers, computer commands, design and framework of programme inspection of computer resource in any form.

Section 66 B: Punishment for deceptively encountering seized computer resource or communication –

Whoever deceptively encounter or hold on to any robbed or theft digital workstation resource or communication gadget or device having information or inducement to believe that the appliance to be theft one, shall be liable for detention for term not more than three years or

with fine which can be increase to ten lakh rupees.

Section 66 E: Punishment for infringing privacy –

If an individual motively or deliberately reproduce, bring out the image of sexual organs of any person without his/her permission and acknowledgement, then that person shall be liable for captivity which can increase to three years or with fine not more than two lakh rupees, or both.

Section 66 F: Punishment for cyber terrorism –

A person who –

(A) With aim to menace the unity integrity security or sovereignty of India or to bash terror in people –

(i) Contradict or cause the contradiction of access to any person authority to acquire computer resource.

(ii) Procure hand to acquire a computer resource without permission of owner.

(iii) Direct or cause to direct any computer contaminant.

And by any mode work on or is likely to cause bruise or demise to person or destruct of property, services to the community or censorious information.

(B) Voluntarily creep into a computer resource without knowledge or authority of owner, and acquire data or information that is restrained to use for security reasons in relation to state, public morality, decency, foreign relations, contempt of court, defamation or incitement to an offence of cyber terrorism

Section 67B: Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form: - Whoever –

(a) Communicate, print or broadcast or cause to print or broadcast material in any electronic form which show children seize in sexually explicit act or work.

(b) Compose, text or digital images, store, swap, reproduce, search, spread material in an electronic form depict children in sexual nasty, outrageous exploit manner.

(c) Refine, persuade children to online relationship with one or more children for sexually explicit act or a work that is improper and is a crime and not just.

(d) Ease abusing children online, or,

(e) Store in any electronic mode from own abuse or that of others perpetuates to sexually exploit conduct with children.

Shall be punishable for not more than 5 years and fine not more than 10 lakh rupees for first attempt and for subsequent attempts imprisonment for a term which may increase to 7 years and fine not more than 10 lakh rupees.

Provided that under provision of section 67, section 67A if printing, documenting in a book, newspaper or pamphlet is to be justified and for good faith and used for bona fide heritage or religious purpose is not an offence.

IV. CONSTITUTIONAL PROVISIONS ALLIANCE WITH CYBER LAWS

As digitalization has step in shoes of exercise of accumulating and giving documents in physical manner, everything nowadays is preserved and squirrel away in digital devices or in an electronic medium. The 'right to privacy' is an essential element of human rights and also a fundamental right as articulated in United Nations Declaration of Human Rights and in Indian Constitution, 1950 respectively.

Privacy is best insight or interpreted as a bunch of interest and motives submerge as:

- Administer and influence over information concerning oneself.
- Supervision of approach of information both mental and physical.
- Command over one's capacity to make an essential commitment regarding family and lifestyle in relation to be assertive and flourish different relationships.

The right to privacy was first acknowledged as a fundamental and constitutional proposition in India for the first time in case of Kharak Singh v. Union of India[15] In this case the five Judges bench, holding majority by three Judges dismissed the actuality of a fundamental right to privacy as a segment of right to life and personal liberty[16] but the minority judges discard this interpretation and conclude: -

"The right to personal liberty grabs not only a lawful postulate to be uncoined from boundation exist on his track, but also liberty from intrusion on his individuality. It is a fact our constitution does not practically clarifies a right to privacy as a constitutional right, but he said right is an important segment of personal liberty.

[15] (1964) SCR (1) 332
[16] INDIAN CONST. art. 21

Later in case of Govind v. State of Madhya Pradesh[17], the Supreme Court on the groundwork on Kharak Singh Case, comprehend right to privacy as an embedded constitutional right in Indian constitution. The Apex Court discloses the scope and cave at or peculiarity to the right. As this right is not a sovereign right three tests were stated to guard the enforceability of right. The three tests are: -

(i) Important of right is in uniformity and counterbalance of superiority;

(ii) Necessity and constraints regarding state interest; and

(iii) Urging public scrutiny

In case of People Union for Civil Liberties (PUCL) v. Union of India[18]

The yardsticks or touchstones of case are[19]: -

(i) The right to privacy "is an essential ingredient of life' and personal liberty' embodied and cherished under Article 21 of the Constitution."

(ii) The authority to hold a telephone dialogue or skill session at individual home, and workplace without any intervention is affirmed as "right to privacy" as the nature of telephonic sessions and discussions are private, deep – sealed and sensitive.

(iii) Any right embodied in Article 21 cannot be impinged or unfeigned except as per the instructions manifested by law, which has too equitable, impartial and rational.

By nine judges' bench, the Supreme Court overrented M. P. Sharma case[20] and gave sanction and constitutionality to right to privacy in Puttaswamy case[21].

The fundamental postulate that "Privacy is the final proposal of statement of righteousness of individual".

The analysis and judgement held in case: -

(a) The breach of 'right to privacy' with autocratic and doctorial course of action would substance to the just, sensible and reasonableness inspection under Article 19.

[17] (1975) AIR 1378
[18] (1997) l SCC 301
[19] Right to Privacy: surveillance in the Post- Puttaswamy Era, https://www.bloombergquint.com/law-and-policy/right-to-privacy-surveillance-in-the-post-puttaswamy-era, (last visited Feb. 13, 2021
[20] (1954) AIR 300
[21] (2017) 10 SCC 1

(b) Privacy expropriation that implies Article 19 freedom would lay the constraints of public ordinance, immorality etc.

(c) Trespassing into someone's personal life and sovereignty under Article 21 will adjoin the fair, sensible and practical approach.

(d) The 'proportionality and legitimacy' test was introduced. This test us four bench of test that requires to be executed before predicament of intrusion in the 'right of privacy'.

The justice Chandrachud and justice Kaul, entangled and detailed the four-bunch test as following: -

(i) Legality: - The actuality and occurrence of law.

(ii) Legitimate Goal: - The law should have attained the admissible and sanctioned state objective. The target conduct must be regulated for parliamentary society for a lawful condition.

(iii) Proportionality: - There should be judicious link between the purpose and the means acquired to accomplish them. The dimension of trespassing or intrusion must be proportionate as per its requirement.

(iv) Procedural Guarantees: - To inspect and examine against the exploit of state obtrusion.

By accumulating the summary of above stated case laws we stipulated the constitutional jurisprudence on privacy in Indian laws, but for the pith of conciseness, here are some touchstones: -

(i) Equitable and rational limitations can be trust on the right to privacy in the engrossment of the sovereignty, public ordinance, foreign states, contempt of court, solidarity of India, libel and slander or surveillance of state to an offence[22].

(ii) Rational limitations cab be urge on the right to privacy for the deliberation of public ordinance and safeguard of the engross of any schedule tribe.[23]

(iii) Right to privacy can be bounded by approach generated by law which plan of action which would have to persuade and reassure the test in guided under Maenka Gandhi Case[24].

[22] INDIA CONST., 1950. art. 19 § 2
[23] Article 19(5) of INDIA CONST., 1950. art. 19 § 5

(iv) The right can be limited if there is an urgent and reliable counterbalance attentiveness, according their superiority.

(v) It can be limited also if there is a curse of action putting the serves on nation interest to be utilized by doing such conduct.

By this way I explained and discussed that how provisions of Indian constitution, 1950 and Cyber laws of India are co-related with each other. Both the Indian Constitution and Cyber laws are independent laws but are at some provision's alliance with each other for the aim to stimulated proper explanation and grant punishments to criminals or wrongdoer.

V. INDIAN EVIDENCE ACT CORELATION WITH CYBER LAW OF INDIA

Cyber-crime is explained as a guilt, offence in which a computerized and an electronic machine is used for conversation between two people. The machine is used as a gadget or appliance of crime, which is the main object or instrument which testing and evidence of crime.

The first electronic and automatic computer evidence was traced in 1984, by FBI (Federal Bureau of Investigation) situated at United State of America.

On 17th October 2000, the Information Technology Act, 2000 was acquainted with the alliance of Indian Evidence Act, 1872 this provide and guard a legitimate structure by giving acknowledgement to electronic records and electronic proof as evidence.

Electronic evidence tries to showcase the actual picture as what is happened conversation between 2 people as audio and video clips and actual occurrence of event.

Section 4 – IT Act, 2000

Legitimate admission and endorsement of electronic records –

The law lay out and furnish that information materialistic work and documents ought to be in writing or in photocopied or in typed form, then notwithstanding anything included in the law, such prerequisites must be considered and adjudge to been reserve, serve and gratify if such information or desired document is –

(a) Manifested exhibited and advisable in a technical and automatic digital form and

(b) Ingress or retrieve so as to utilize for an alternative and substitutive citation or source.

Indian Evidence Act –

Sec 65B – Admissibility of electronic records -

[24] (1978) AIR 597

1. Notwithstanding incorporate in this Act, any information accommodated in an electronic record which is typewritten and is inscribed on a photocopied paper, board, scanned, transcribe in an automatic and technological media extract by a computer (herein after digital output) must be judge as a document, if the specification referred in this section are fulfilled in alliance to information and computer in examination and ought to be acquired in proceeding as out of doors any further evidence or structure of original as proof of any tranquity of original and facts mentioned and shaped therein of having direct proof would be justifiable.
2. The necessities or requirements stipulated in reference to sub – section (1) of digital output is: -

   Anvar P. V. v. P K Basheer & Ors.[25]

   (a) Computer was in authorised in supervision of the person assembling the certificate. The electronic record including the subject matter should have been fabricated from the computer as per duration of time gets up which the similar system was periodically served to squirrel away the collect or structured information for the goal of any course of action systematically put forwarded on over that time duration by the person having sanctioned supervision or dominance over the use of digital workstation.

   (b) Subject – matter was fortified in computer conveniently and in the usual courses: -

   The information of the type stimulated in the electronic record or of the cordial from which the matter of procure periodically nourished into the computer in the usual course of the related action;

   (c) Computer was functioning systematically:

   During the subject – matter part of the specified period, the computer was functioning accurately and that even if it was not working accurately for a time span, the disturbance or blown out will not govern either the record or the reliability of the subject – matter; and

   (d) Procreation is conscientious and detailed: - The information stimulated in the record should be proliferation or induction from the information sustained into the computer in the customary course of said action.

State of (NCT of Delhi) v. Navjot Sandhu, SAR Gilani and Ors.[26]

[25] (2014) 10 SCC 473

> In this case the High Court observed that it is not quarrel or debate that the information included in call records is accumulated in enlarged servers which is neither easily movable and nor can be generate in court proceeding. Hence, printout or typed documents get hold from computer/servers by automatic optical process and is authenticated by rational and authoritative official who is for service for dispensing the company, which further lead to attestation or as a proof.

State of Delhi v. Mohd. Afzal & Ors.[27]

In this case the court held that electronic records are acceptable as a proof. If someone provoke or defiance the precision of the computer evidence or the digital record on the groundwork or on base of that particular evidence and utilize or serve that evidence for malfunction and misemploy it by another workstation or causes any misfiring or incorporate the failure in the system, the individual provoking the obstacles must be have some just, fair and reasonable justification for crossing and answering all he possible doubts.

Further, the court observed that mere conceptual and standard perception cannot lay down crystal – clear and mirror – like evidence and it make it unacceptable in the eyes of law.

By this we showcase how both the laws Indian Evidence Act, 1872 and Information Technology act, 2000 alliance with each other. Slowly and gradually at pace of development the Indian courts and people of India are now accepting the digital or electronic records and same are used as evidence in courts. Infact, now due to the COVID-19 virus, there is 'work from home' which in judicial or court proceeding means ONLINE COURTS AND MEDIATION.

VI. CONCLUSION

Cybercrimes and cyber security are connected to each other. India has drafted Information Technology Act, 2000 which lays down legislations against cybercrimes and have also stated its punishments. The alliance between provisions of Indian constitution and Indian evidence Act with cyber laws is to state and laid a groundwork and structure that how both laws are co-related and justify the provisions of Information Technology act,2000.

*****

[26] AIR (2005) SC 3820
[27] 107 (2003) DLT 385