Lex Valorem

Indian Journal of Law and Contemporary Issues

"Where Value is Law"

E-mail - indianjournaloflawandci@gmail.com

LEX VALOREM : INDIAN JOURNAL OF LAW AND CONTEMPORARY ISSUES

VOLUME I , ISSUE I

October 2020

Lexvaloremijlci.com

DISCLAIMER

EDITORIAL BOARD

ABOUT US

Lex Valorem is set up in the year 2020 in Varanasi, India with the sole intention of delivering value added legal services to all.

Lex Valorem: Indian Journal of Law and Contemporary issues is a peer reviewed law journal that aims to provide a platform to all the budding lawyers, researchers and advocates for their original work. The journal follows the principle "Where value is law" and the members of the journal work towards striving value in all fields of law.

Lex Valorem is not just confined to the walls of publishing research papers but also legal updates, case analysis and other areas of legal interest.

PRIVACY LAWS IN INDIA

Author –
Gaurav Lasiyal

Student
Amity Law School, Noida

Table of Contents

S.No Topic

ABSTRACT

Cyber Crime is the most modern form of crime in the era of science and technology. Unlike other crimes, Cyber Crime is rapidly expanding in the present time through extensive use of internet and other computer technologies. It is not particularly defined in any legislation, but it can be understood as a crime which involves around a computer and a network system. Cybercrime covers a wide range of different attacks such as Cyber extortion, Cyber warfare, spreading Computer viruses or Malware, Internet fraud, Spamming, Phishing, carding (fraud), child pornography and intellectual property rights violation etc.

Cyber Crime is mainly violating and affecting the privacy of the individuals through internet network. India has legislations namely Information Technology Act 2000, Indian Penal Code 1860, to deal with cybercrimes but lacks the aspect of dealing privacy. There is no comprehensive legislation in our country which deals with cyber crimes. Cyber crime has entered into popular demonology and today no one can claim to remain in affected by it as individuals, business organizations, governments & states all are in the net. While privacy is seems intuitive to most people in India, its legal codification, complexity of protection not possible. Constitutional right to privacy exists as an ancillary right under Article 21 but not absolute. It gives a right to privacy to the individuals but not incorporate every offence through it. The Supreme Court of India has, intermittently and unconvincingly, recognized a limited right to privacy in certain situations.

HYPOTHESIS

The hypothesis actually to be tested is usually given the symbol H0, and is commonly referred to as the null hypothesis; the null hypothesis is assumed to be true unless there is strong evidence to the contrary – similar to how a person is assumed to be innocent until proven guilty. The other hypothesis, which is assumed to be true when the null hypothesis is false, is referred to as the alternative hypothesis, and is often symbolized by HA or H1.

H0: Privacy Laws is important in the physical world and not in digital world.

H1: Privacy Laws is important in both physical and in digital world.

RATIONALE

The rationale of this paper is to discuss how protection of privacy in physical and digital world can be secured.

METHODOLOGY

This research paper is solely based on the doctrinal research method through the secondary sources that include books, online sources like judicial pronouncements, websites, articles, statutes, reports; e-books all of which when used have been properly cited in footnotes.

OBJECTIVE

The paper focuses on conceptual analysis of concept of right to privacy both in physical and digital world. The paper further focuses on the legislative efforts to protect privacy and discuss the judicial nuances. The paper further focuses whether right to privacy is a right in a real sense or not?

INTRODUCTION

In the emerging time the world is going to face a problem of global cyber security which causes cyber contravention and cyber crime, for that many initiative has been taken up by the Developed countries in the ambit of resolution (A/RES/51/162) adopted by General assembly of the united nation regarding the model law on electronic commerce earlier adopted by the united nations commission on international trade law (UNCITRAL). This is true that awareness and knowledge about the cyber crime in developed countries people having more than developing countries. like USA and China has their own law and international treaties on cyber crime for dealing with every aspect and protecting their individuals right and making their citizens safe in their country. Similarly India has laws in the name of IT act 2000 and Act is here to protect and provide a means of redressed even to the owner of a single computer, computer system or computer network located in India which has been violated by any person of any nationality subsequently .it was amended in 2008 with insertion of section 66A which penalize "sending offensive messages" but it does not cover every offence through this IT Act regarding cyber crime also IPC has been amended to accommodate cyber crime of penal nature like outraging the modesty of woman under section(354) through electronic sources subsequently IT Act can be used to accommodate punishment for the crime such a abatement to suicide, theft(stealing money for the bank account holders),cheating of personating (416),criminal intimidation (503),attempt to commit offences(511),forgery 463,making false electronic document(464) and many other sections of Indian penal code are dealing with cyber crimes. Which can be co-related of IT act 2000 .in the light of Indian constitution which gives a right to privacy (Article 21) to its citizen also dealing with this aspect. this is pertinent to various convention on like (Budapest convention)on cyber crime where India could not be a signatory due to privacy concern of its individual .

TO FURTHER ELUCIDATE THE PRIVACY LAWS, WE CAN REFER THE FOLLOWING CASES

I. M.P SHARMA VS SATHISHCHANDRA[1]

Right to privacy was observed first time in the ambit of the constitution. The case related to search and seizers of the document of some dalmia group companies following investigation into its affairs. following, FIR the District magistrate issued warrants and searches were consequently conducted. In the writ petition the constitutionality of the searches was challenged on the ground that they violates the article 19(1)(f) and 20(3).Supreme Court held that the drafters of the Constitution did not intend to subject the power of search and seizure to a fundamental right of privacy.

II. KHARAKSINGH VS UTTAR PRADESH[2]

Again the right to privacy was invoked in this case where the police has arrested kharak singh for dacoit lack of the evidence he was released but police under chapter xx police regulation act were empowered to surveillance of the accused, constitutionality of chapter xx was challenged before court that it violates the article 19(1)(f) and article 21.judge bench held that domiciliary visits at night was unconstitutional, but upheld the rest of the Regulations. More importantly, the bench held that the right of privacy is not a guaranteed right under the Constitution.

III. PUTTASAWMY VS UNION OF INDIA[3]

It was the landmark judgment which we are following today. where the nine judge's bench upheld the right to privacy was constitutionally protected right in India. Retired high court judge puttasawmy challenged the government's proposed scheme for the uniform biometric based identity card which would be mandatory for access to government policy and benefits. Government contented that right to privacy was not guaranteed by the constitution but court reasoned that right to privacy is incident of fundamental freedom and liberty guaranteed

1 1954AIR 300

2 1963 AIR 1295

3 WRIT PETITION (CIVIL) NO. 494 OF 2012

under article 21.On 24th August, 2017 a 9 Judge Bench of the Supreme Court delivered a unanimous verdict in Justice K.S. Puttaswamy vs. Union of India and other connected matters, affirming that the Constitution of India guarantees to each individual a fundamental right to privacy. Although unanimous, the verdict saw 6 separate concurring decisions. Justice Chandrachud authored the decision speaking for himself, Justices Khehar and R.K. Agarwal and Abdul Nazeer. The remaining 5 judges each wrote individual concurring judgments.

IV. SHREYA SINGHAL V/S UNION OF INDIA, 2015[4]

I. It's miles the maximum critical case where the section 66A of the data technology Act 2000 became struck down. It changed into inserted by means of the amendment of 2009 in the act however because of its violative nature changed into struck down by the ideally suited courtroom. The petitioner demanding situations the constitutional validity of the act on the following grounds:

II. It infringes the essential right to free speech and expression and isn't always stored via any of the eight subjects covered in Article 19(2).

III. This section in creating an offence suffers from the vice of vagueness because of which the harmless people are roped in as offenders.

IV. The enforcement of the stated section would honestly be an insidious shape of censorship which impairs a core fee contained in Article 19(1)(a).

V. The stated section infringes the rights of the person beneath Articles 14 and 21 in as a great deal there may be no intelligible differentia among folks who use the net and people who by means of words spoken or written use their mediums of conversation.

2. What are the unique offences and punishments beneath the IT Act?

- Section 43A, which deals with implementation of affordable security practices for touchy private facts or statistics and affords for the compensation of the person tormented by wrongful loss or wrongful gain.

4 WRIT PETITION (CRIMINAL) NO.167 OF 2012

- IT Act, section 65,, tampering with pc source documents: Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly reasons any other to conceal, break or adjust any laptop source code used for a laptop, laptop programme, laptop device or computer network, whilst the computer supply code is required to be saved or maintained with the aid of regulation for the being time in force, is punishable with imprisonment up to three years, or with a first-class which may enlarge upto Rs. 2 Lakh, or with each. The object of the phase is to protect the 'highbrow assets' invested inside the laptop. it is an try to protect the computer supply documents past what's to be had beneath Indian Copyright law. That is a cognizable and non- bailable offence. to use this section to the cutting-edge scenario, we need to make sure that the critical components for software of this section are met, which incorporates a person:

1) knowingly or intentionally concealing,
2) knowingly or deliberately destroying,
3) knowingly or intentionally changing,
4) knowingly or deliberately causing others to hide,
5) knowingly or intentionally inflicting every other to spoil,
6) . Knowingly or deliberately causing some other to regulate.

- IT Act, section 66, hacking computer gadget:(1) Whoever with the intent to purpose or knowing that he is probable to motive wrongful loss or damage to the public or any man or woman destroys or deletes or alters any facts residing in a computer aid or diminishes its value or application or influences it injuriously by way of any approach, commits hacking; and (2) Whoever commits hacking shall be punished with imprisonment upto three years, or with high-quality which might also make bigger upto Rs. 2 Lakh, or with both. The segment talks about the hacking hobby.

Again, before applying this provision to the occasions, one might want to test the essential elements of the section-

1) Whoever with goal or expertise.
2) Causing wrongful loss or harm to the general public or anyperson.
3) Destroying or changing any statistics residing in a laptop resource.
4) Or diminishes its fee or utility or.
5) Affects it injuriously via any approach.

- Section 67, publishing obscene data in digital form: Whoever publishes or transmits or causes to be published inside the digital shape, any fabric that is lascivious or appeals to the prurient

interest, or if its effect is such as to tend to deprave and corrupt people who are probable, having regard to all applicable situation, to read see or pay attention the matter contained or embodied in it, can be punished on first conviction with imprisonment of either description for a term which may additionally enlarge to 5 years and with excellent which may additionally make bigger to Rs. 1 Lakh and within the event of a 2d or subsequent conviction with imprisonment of both description for a time period which may additionally extend to ten years and additionally with exceptional which might also expand to Rs. 2 Lakh.

- **The primary case here was state of Tamil Nadu v/s Suhas Katti.** This became a case approximately posting obscene, defamatory and worrying message approximately a divorcee girl on a Yahoo message group. The accused became found guilty of offences below section 469, 509 IPC and sixty seven of IT Act 2000 and convicted to go through RI for 2 years underneath 469 IPC and to pay first-rate of Rs.500/-and for the offence united states509 IPC sentenced to undergo 1 yr easy imprisonment and to pay nice of Rs.500/- and for the offence u.s.67 of IT Act 2000 to go through RI for two years and to pay satisfactory of Rs.4000/- All sentences to run concurrently. The accused has because paid the nice and is lodged at vital prison, Chennai. that is considered the first case convicted beneath IT Act section 67.
- In Avnish Bajaj (CEO of bazzee.com) case, there had been 3 accused, along with the provider company (Avnish Bajaj later acquitted). The sections relied upon were phase 292 (sale, distribution, public exhibition, and so forth. of an obscene item) and phase 294 (obscene acts, songs, and so on, in a public vicinity) of the Indian Penal Code (IPC), and segment 67 (publishing data that's obscene in digital form) of the IT Act. Similarly, the schoolboy faces a rate below phase 201 of the IPC (destruction of evidence), for there is apprehension that he had destroyed the cellular phone that he used in the episode. Those offences invite a penalty of imprisonment starting from 2 to 5 years, in the case of a first time conviction, and/or fines.
- section 72 penalty for breach of confidentiality and privacy: Any individual who, in pursuance of any of the powers conferred underneath the IT Act, guidelines or regulation made there beneath, has secured examine to any electronic file, book, check in, correspondence, information, record or different cloth without the consent of the individual involved discloses such fabric to another character may be punished with imprisonment for a term which may additionally extend to two years, or with quality which may additionally increase to Rs. 1 Lakh, or with both.
- section 72A, which gives for imprisonment for a duration up to three years and/or a pleasant up to Rs. 500,000 for someone who reasons wrongful loss or wrongful advantage with the aid

of disclosing private facts of every other man or woman even as offering offerings under the phrases of lawful contract. A constitutional bench of the supreme court declared 'privacy' as a fundamental proper on 24 August 2017.

3. Aadhaar Act 2016

Aadhaar is unique word itself in the context of the identity which means ‘base’ .Aadhaar Act was enacted by the Indian Government in 2016 as a money bill earlier it was introduce in the Rajya Sabha but along some amendment it was sent back to the Lok Sabha which passed this bill without considering the purposal suggested by the Rajya Sabha. This bill intends to deliver a subsidies to every individual residing in the country by providing a unique number. Essence of this bill is that assign one number to individual shall not be assign to others. As its obligation on the government to verify the identity of the persons as he is receiving the subsidies provided by the government . Government are required them to apply in case people don’t have aadhaar number meanwhile government has to give them alternative for getting subsidies. this act contains 8th chapter and 59 section, which states that how this act should be governed and how Parliament has tried its best to serve people through this scheme but supreme court has to intervene because its provisions violating the basic structure of the constitution aadhaar act was striking on the basic feature of the constitution ‘right to privacy’

- Section 3(2) -as this provision mandate the enrolling agency to inform the person that how it should be used. At the time of enrolment, apprise the individual the manner in which the information shall be used; the nature of recipients with whom the information is intended to be shared during authentication; the subsistence of a right to access information, the procedure for making requests for such access and details of the person or department in-charge to whom such requests can be made.

SOME OF THE IMPORTANT SECTIONS[1] OF AADHAR ACT WERE:

- Section(7)- The above section was the focus of the Aadhaar Litigation. This requires individuals to either generate Aadhaar or his Aadhaar registration number to access social facilities, subsidies, incentives, etc., whose funds are drawn from India's Consolidated Fund. The government released 139 notifications, all of which were under appeal, requiring Aadhaar to get services.
- Section 23(K) - This states that information shall be shared in manner as prescribed by regulation it means it is clear cut violation of the privacy . Though it fails to achieve its goal for which it was enacted
- Section (28)-The problem of security of the information collected through Aadhaar was a major source of concern with the court.

1 Aadhar Act,2016

- Section 28(1)- Provides for the authority to ensure the protection of individuals identity information and authentication records.We shall ensure that the personal identification information and authentication records remain private.
- Section 29(2) -The identity information, other than core biometric information, accumulated or engendered under this Act may be shared only in accordance with the provisions of this Act and in such manner as may be designated by regulations. Even more worrying section 29(4) which permites display the core biometric as per as the regulation.
- Section (57)-State, body corporate, or individual may apply for Aadhaar but in accordance with a law or contract to that effect. It is this clause that offers legislative support for telecom firms, private service providers toobtain the Aadhaar card for identification purposes for individuals.

Even court has orally stated that It shall not be mandatory for availing every service other than governments but still private entity is asking for aadhaar number ,there are several issue before court as government has mandate aadhaar linking with banks and pan card which is not safe for the purpose of privacy as government is taking every and each information about people but if it fails to protect the same than it will jeopardize the safety of citizens .

Though establishing the constitutional provisions of the Aadhaar scheme, the Supreme Court ruled that when you decide to share biometric data, Aadhaar Act does not infringe your right to privacy. Private companies have been barred from using Aadhaar card for KYC authentication purposes but for various other purposes including PAN card and ITR filing you will still require Aadhaar.

Smooth functioning and adjucation managment require individuals to be knowledgeable while there may be a breach and discloser of the their peronal information.

- Section47 describe that best the Uidai or it is approved officer can document a criminal criticism beneath the Act. For this reason, all the criminal consequences prescribed beneath the Act (e.g. for disclosing identity facts below section 37 or for unauthorised get entry to to the crucial Identities records Repository under section38) can best be initiated by the UIDAI, and no longer the aggrieved Aadhaar number holder.

Subsiquently, despite fact that the Act describes civil and crook remedies for aunauthorize get entry to, use, or disclosure via the prescribed authority, the crook remedy isn't always available to the aggrieved Aadhaar quantity holder. Such a person best has recourse to civil regulation, and the fines prescribed under the Act.

Regrettably, a together reading of Sections 28 and section 47 of the Act divulge the assumption of conflict of hobby considering the fact that it may be in UIDAI’s hobby to cover up breaches of privateness. Without the UIDAI’s proactive motion, an man or woman Aadhaar range holder is left without remedy.

- Section 30 prescribe biometric data as “touchy non-public records or records”,as understood in section 43A of the data era Act. The treatment of such statistics beneath the IT Act has been dealt with in element in our previous post. The IT Act itself fails to handle sensitive non-public data or facts in ways that embed privacy issues.

In the end, as stated within the sections above, the supervision mechanism for one of the Aadhaar Act’s maximum arguable sections (section 33), is the charter of an ‘Oversight Committee’. This Committee is tasked with reviewing the disclosures made inside the interest of`country wide protection’, and therefore serves to meet the ‘responsibility’ and ‘security’ ideas of privateness law. However, this 3 member Committee comprises of three government bureaucrats, in particular after the Lok Sabha rejected the Rajya Sabha amendment to consist of both the CVC or the CAG as a part of the Committe

CONCLUSION

1. In my view, “privateness” is a “state of thoughts”. Someone may be amidst a crowd and still experience his privacy isn't invaded. Alternatively he may be sitting in a closed room but filled with anxiety that his privacy is being invaded.
2. “Mental privacy” as a “country of mind” of 1 man or woman is outdoor definition of the physical definition of “right to be left on my own” or “proper to manipulate dissemination of of privateness information”,.
3. It is also out of doors the definition of Cyber privateness as “keeping a certain virtual distance”.
4. It is for every character to claim what are his/her intellectual privateness barriers.
5. Section 66A of ITA 2008 which was scrapped, did have a hyperlink to such idea but the preferrred court docket which dealt with the Shreya Singhal Case did now not apprehend it.
6. Most Cyber Stalking sufferers have a mental situation where what isn't “privacy Invasion” for maximum can be taken into consideration via them as “privacy Invasion”. this is a “Deemed privacy Invasion” and could be a issue to be taken into consideration within the “nation of the thoughts” definition.
7. Under this idea privateness boundaries might be specific from a man and woman, Boy and girl, buddy and Stranger, from a relative to a non relative, from a metropolis bred character to a Villager and so forth.
8. Using one yard stick for all might now not be an excellent idea.
9. Without being capable of define “privacy” any try and supply a “proper” and call it “essential” seems to be a fruitless exercising. I've established a scientific eight-fold direction for analysing laws from the point of view of issues of privacy. We’ve used this framework to examine two laws: The IT Act, 2000, and the Aadhaar Act, 2016. Both those laws have critical disasters in enshrining privacy. These laws thus impede India’s emergence as a mature democracy.

BIBLIOGRAPHY

ACTS

- The Constitution Of India
- The Indian Penal Code ACT NO. 45 OF 18601
- The Information technology ACT, 2000

LINKS

- https://indiankanoon.org/
- https://www.casemine.com/
- https://uidai.gov.in/my-aadhaar/get-aadhaar.html
- https://cybercrime.gov.in/