Law Audience Journal, Volume 4 & Issue 1, 10th May 2022, e-ISSN: 2581-6705, Indexed Journal, IF 5.381, Published at https://www.lawaudience.com/volume-4-issue-1/, Pages: 76 to 87,

Title: "Decryption and Protection of Data in Cyberspace: An Overview of Indian Legislations", Authored By: Mr. Sandeep Mishra, Research Scholar, Department of Legal Studies, Dr. Ram Manohar Lohiya National Law University, Lucknow. Email Id: juris.sandeep@gmail.com.

Cite this article as:

MR. SANDEEP MISHRA, "*Decryption and Protection of Data in Cyberspace: An Overview of Indian Legislations",* Vol.4 & Issue 1, Law Audience Journal (e-ISSN: 2581-6705), Pages 76 to 87 (10th May 2022), available at ***https://www.lawaudience.com/decryption-and-protection-of-data-in-cyberspace-an-overview-of-indian-legislations/.***

Law Audience Journal, Volume 4 & Issue 1, 10th May 2022, e-ISSN: 2581-6705, Indexed Journal, IF 5.381, Published at https://www.lawaudience.com/volume-4-issue-1/, Pages: 76 to 87,

Title: "Decryption and Protection of Data in Cyberspace: An Overview of Indian Legislations", Authored By: Mr. Sandeep Mishra, Research Scholar, Department of Legal Studies, Dr. Ram Manohar Lohiya National Law University, Lucknow. Email Id: juris.sandeep@gmail.com.

Publisher Details Are Available At:

https://www.lawaudience.com/publisher-details/

Editorial Board Members Details Are Available At:

https://www.lawaudience.com/editorial-board-members/

Email: ***lawjournal@lawaudience.com, info@lawaudience.com,***
Phone: ***+91-8351033361,***
Website: ***www.lawaudience.com.***
Facebook: ***www.facebook.com/lawaudience***
Instagram: ***www.instagram.com/lawaudienceofficial***
Contact Timings: ***5:00 PM to 9:00 PM.***

Law Audience Journal, Volume 4 & Issue 1, 10th May 2022, e-ISSN: 2581-6705, Indexed Journal, IF 5.381, Published at https://www.lawaudience.com/volume-4-issue-1/, Pages: 76 to 87,

Title: "Decryption and Protection of Data in Cyberspace: An Overview of Indian Legislations", Authored By: Mr. Sandeep Mishra, Research Scholar, Department of Legal Studies, Dr. Ram Manohar Lohiya National Law University, Lucknow. Email Id: juris.sandeep@gmail.com.

Law Audience Journal, Volume 4 & Issue 1, 10th May 2022, e-ISSN: 2581-6705, Indexed Journal, IF 5.381, Published at https://www.lawaudience.com/volume-4-issue-1/, Pages: 76 to 87,

Title: "Decryption and Protection of Data in Cyberspace: An Overview of Indian Legislations", Authored By: Mr. Sandeep Mishra, Research Scholar, Department of Legal Studies, Dr. Ram Manohar Lohiya National Law University, Lucknow. Email Id: juris.sandeep@gmail.com.

ABSTRACT:

"Cyberspace is shorthand for the web of consumer electronics, computers, and communication networks that interconnects the world. Privacy is the desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitude and their behavior to others. There are certain laws in force, which ensures protection to the right to privacy in cyberspace. The present research paper therefore aims at exploring the status of Privacy in Cyber Space in India. India needs to work more for enduring an effective and concrete legislation for data protection. However, while creating the laws, the legislature has to be well aware for maintaining a balance between the interests of the common people along with amicably handling the increasing rate of cybercrime. In continuing the privacy conversation, we must recognize that a vision protective of information privacy and data protection in cyberspace will be singularly hard to maintain".

Keywords: Cyberspace and Privacy; Information Privacy Invasion; Privacy Invasion Tools and Measures; Data Protection Legislation.

I. INTRODUCTION:

Cyberspace is shorthand for the web of consumer electronics, computers, and communication networks that interconnects the world. The Internet users in present scenario are dangerously exposed to the risk of privacy infringement in cyberspace. With the growing use of internet by the citizens of the country, the risk of their being exploited and victimized by infringing their privacy over internet is increasing day by day. This concern is felt more in the case of youth and teenagers who constitute majority of the internet users and are susceptible in understanding the risk of exposing themselves to the cyber world. The social is susceptible in understanding the risk of exposing themselves to the cyber world. The social networking sites which are now used extensively for social interactions between the individuals by uploading their personal content, has further aggravated the issue of 'internet privacy'. There are several ways in which, the privacy of the individual could be violated in cyber space. There are

Law Audience Journal, Volume 4 & Issue 1, 10th May 2022, e-ISSN: 2581-6705, Indexed Journal, IF 5.381, Published at https://www.lawaudience.com/volume-4-issue-1/, Pages: 76 to 87,

Title: "Decryption and Protection of Data in Cyberspace: An Overview of Indian Legislations", Authored By: Mr. Sandeep Mishra, Research Scholar, Department of Legal Studies, Dr. Ram Manohar Lohiya National Law University, Lucknow. Email Id: juris.sandeep@gmail.com.

certain laws in force, which ensures protection to the right to privacy. The Right to Privacy is one of the most cherished rights for the human beings given the nature and the importance of this right. The human beings by their very nature require a space exclusive from interference of any kind. This is necessary for the development of their individual personality.

II. PRIVACY RIGHT: INTERNATIONAL COMMITMENTS:

The fact that the right to privacy finds a special mention in the ancient texts and sources signifies its importance to the societies of all times. This right has received recognition and protection in societies of all times. In modern era, the human rights movements have considerably affected the concept and jurisprudence of legal rights. The right to privacy has found explicit mention in all international instruments concerning human rights.[1] As basic principles for the protection of privacy there are three international treaties that are widely recognized as the basis for the protection of privacy and personal life.

Article 12 of the Universal Declaration of Human Rights of 1948, Article 17 of the ***International Covenant on Civil and Political Rights (ICCPR)***. The OECD guidelines on the Protection of Privacy and Trans border Flow of Data are also of relevance in this aspect.[2] Alan Westin (1967) in 'Privacy and Freedom' defined privacy as the "*desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitude and their behavior to others.*"

III. RIGHT TO PRIVACY: INDIAN SCENARIO:

Privacy is an incident of fundamental freedom or liberty. The right to privacy is one of the basic Human rights. In addition, Courts in India have admitted it a status of fundamental right, though it is not directly provided in the Constitution of India. In ***Justice K.S.***

[1] Art.12 of the Universal Declaration of Human Rights and Art.14 and 17 of the International Covenant on Civil and Political Rights.

[2] http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

Law Audience Journal, Volume 4 & Issue 1, 10th May 2022, e-ISSN: 2581-6705, Indexed Journal, IF 5.381, Published at https://www.lawaudience.com/volume-4-issue-1/, Pages: 76 to 87,

Title: "Decryption and Protection of Data in Cyberspace: An Overview of Indian Legislations", Authored By: Mr. Sandeep Mishra, Research Scholar, Department of Legal Studies, Dr. Ram Manohar Lohiya National Law University, Lucknow. Email Id: juris.sandeep@gmail.com.

Puttaswamy vs. Union of India[3]**,** the Apex court unanimously affirming that the right to privacy is a fundamental right under the Indian Constitution. The verdict brought to an end a constitutional battle that had begun almost exactly two years ago, on August 11, 2015, when the Attorney-General for India had stood up during the challenge to the Aadhaar Scheme, and declared that the Constitution did not guarantee any fundamental right to privacy.[4] Justice D.Y. Chandrachud, while delivering the judgment, has held that "privacy is intrinsic to life, liberty, freedom and dignity and therefore, is an inalienable natural right."[5]

IV. PRIVACY RIGHT AND INTERNET:

The threat to privacy over internet is not a new phenomenon. The developed countries in the world, where the information technology is firmly rooted amongst the masses, have already adopted the security measures by which this problem can be redressed effectively to a considerable extent. The Internet users of these countries normally observe all these security measures while navigating in the cyberspace. The latest McAfee study sheds light on examines the online behavior and social networking habits of Indian tweens and teens. The study stresses the need for more awareness and focus on online safety for youth, the majority of internet users in India are young teenagers who do not understand the risks in exposing themselves to the completely unknown cyber-world[6].

They often fail to analyze the potential threat that they are under while using the internet for social networking or otherwise. The Privacy concerns in India are thus unaddressed by the internet users and lack of security and legislative measures in this direction are adding to the gravity of this already serious issue. Cybercrime investigations need to take into account privacy concerns while implementing the procedural provisions of the Convention on Cyber

[3] WRIT PETITION (CIVIL) NO 494 OF 2012.
[4] http://www.livelaw.in/supreme-courts-right-privacy-judgment-foundations/
[5] https://thewire.in/171325/justice-chandrachud-judgment-right-to-privacy/
[6] Kul Bhushan, Indian teens and tweens more exposed to online risks, 10 - Nov – 2014, https://www.digit.in/internet/indian-teens-and-tweens-more-exposed-to-online-risks-24415.html

Law Audience Journal, Volume 4 & Issue 1, 10th May 2022, e-ISSN: 2581-6705, Indexed Journal, IF 5.381, Published at https://www.lawaudience.com/volume-4-issue-1/, Pages: 76 to 87,

Title: "Decryption and Protection of Data in Cyberspace: An Overview of Indian Legislations", Authored By: Mr. Sandeep Mishra, Research Scholar, Department of Legal Studies, Dr. Ram Manohar Lohiya National Law University, Lucknow. Email Id: juris.sandeep@gmail.com.

Crime. Cybercrime investigations require more technical expertise and surveillance than conventional crime but it also needs to be ensured that here is protection of fundamental privacy principles both in the national and international law. The absolute protection of privacy on the internet as discussed above is difficult to imagine and achieve. The evolution of the technology and the law for the same is already on the move. The self-restraint by the users on his ***'web-habits'*** is the basic solution which may yield positive results in this direction.

V. THE AADHAAR DATA BREACH CASE (2018):

Aadhaar, which means 'foundation', is a 12-digit unique identity number issued to all Indian residents based on their biometric and demographic data. The ***Unique Identification Authority of India (UIDAI),*** a statutory body that oversees the world's largest biometric identity card scheme, following a report in The Tribune[7] that claimed unrestricted access to any Aadhaar number for a paltry sum of Rs 500. Biometric data, unlike the UIDAI's statement, is not the only privacy concern with this breach. The disclosure of demographic data, such as an individual's name, date of birth, address, PIN, photo, phone number, e-mail, etc., is not any less of a privacy concern. This data forms the basis of many cybercrimes, be it phishing or identity theft. Additionally, obtaining biometric data is getting simpler, such as the extraction of fingerprints from photographs or the spoofing of iris scans.

Obtaining biometric data will be a huge target for cybercriminals, because of the potential of combining it with the troves of other information already illegally available. It is extremely dangerous, therefore, to underestimate the value of the data disclosed in this breach, simply because it did not include biometric data, A data 'breach' is not defined under the Indian Information Technology Act, 2000 or the Aadhaar Act, 2016. However, a data 'breach' is not limited to a technical breach like hacking the security systems of the Central Identities Data Repository (CIDR), as is commonly understood. Gaining unauthorized access to a database – in this case, possibly the CIDR – is very much a data breach and a violation of privacy.

[7] Rachna Khaira, Tribune News Service , Jan 4, 2018, http://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html

Law Audience Journal, Volume 4 & Issue 1, 10th May 2022, e-ISSN: 2581-6705, Indexed Journal, IF 5.381, Published at https://www.lawaudience.com/volume-4-issue-1/, Pages: 76 to 87,

Title: "Decryption and Protection of Data in Cyberspace: An Overview of Indian Legislations", Authored By: Mr. Sandeep Mishra, Research Scholar, Department of Legal Studies, Dr. Ram Manohar Lohiya National Law University, Lucknow. Email Id: juris.sandeep@gmail.com.

VI. INDIAN LEGISLATIVE STRUCTURE TO DEAL WITH SURVEILLANCE AND DATA BREACH:

In the report 'Big democracy, Big surveillance: India's surveillance state'[8] published by Open Democracy, India's surveillance programs mostly started following the 2008 Mumbai terror attacks. In India, there is a legislative structure in place that allows the government to undertake surveillance under specific circumstances, such as the investigation and commission of certain crimes. The legal framework for surveillance in India is defined by laws such as the Indian Telegraph Act, 1885, and its rules, the Information Technology Act, 2000, and its rules.

VI.I THE INDIAN TELEGRAPH ACT, 1885:

There are no law exists which mandates or regulates the ***Central Monitoring System (CMS)***. This mass surveillance system is merely regulated under Section 5(2) of the Indian Telegraph Act, 1885, which empowers the Indian Government to intercept communications on the occurrence of any ***"public emergency"*** or in the interest of ***"public safety",*** when it is deemed ***"necessary or expedient"*** to do so in the following instances:

- *the interests of the sovereignty and integrity of India*
- *the security of the State*
- *friendly relations with foreign states*
- *public order*
- *for preventing incitement to the commission of an offense*

However, Section 5(2) of the Indian Telegraph Act, 1885, appears to be rather broad and vague, and fails to explicitly regulate the details of how the Central Monitoring System (CMS) should function. As such, the CMS appears to be inadequately regulated, which raises many questions with regards to its potential misuse and subsequent violation of Indian's right to privacy and other human rights.[9] This provision also gives security agencies and Indian

[8] MARIA XYNOU, Big democracy, big surveillance: India's surveillance state, 10 February 2014, https://www.opendemocracy.net/opensecurity/maria-xynou/big-democracy-big-surveillance-indias-surveillance-state

[9] https://cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about

Law Audience Journal, Volume 4 & Issue 1, 10th May 2022, e-ISSN: 2581-6705, Indexed Journal, IF 5.381, Published at https://www.lawaudience.com/volume-4-issue-1/, Pages: 76 to 87,

Title: "Decryption and Protection of Data in Cyberspace: An Overview of Indian Legislations", Authored By: Mr. Sandeep Mishra, Research Scholar, Department of Legal Studies, Dr. Ram Manohar Lohiya National Law University, Lucknow. Email Id: juris.sandeep@gmail.com.

Income Tax authorities centralized access to the country's telecommunications network and the ability to listen in and record mobile, landline, satellite calls and voice over Internet Protocol (VoIP) and read private e-mails, SMS and mms and track the geographical location of individuals all in real time. It can also be used to monitor posts shared on social media such as Facebook, LinkedIn and Twitter and to track user's search histories on Google without any oversight by the Courts or Parliament.

Tapping is a serious invasion of an individual's privacy as held in ***"People's Union of Civil Liberties vs. Union of India and Anr."***[10] Senior Internet researchers feel that the CMS is chilling in view of its reckless and irresponsible use of the sedition and Internet laws. They feel that it may be used to silence critics, journalists and human rights activists. The right to privacy is guaranteed under the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights to which India is a state party. Article 17 of the Covenant provides that '' (***i) no one shall be subjected to arbitrarily or unlawful interference neither with his privacy, family, home or correspondence nor to unlawful attacks on his honor and reputation; (ii) everyone has the right to the protection of the law against such interference or attacks."***

VI.II THE INFORMATION TECHNOLOGY ACT, 2000:

For quite a long time in India there was no law governing cyber laws involving privacy issues, jurisdiction issues, intellectual property rights and a number of other legal issues. To optimize benefits of ICTs and secure confidence of user's information society should be safe and secured not only through cyber laws per se but also appropriate enforcement mechanisms. In order to formulate strict statutory laws to regulate the criminal activities in the cyber world the Indian Parliament passed the ***''Information Technology Act, 2000"*** to protect the fields of e-commerce, e-governance, e-banking as well as penalties and punishments in the field of cyber-crimes. The Act was further amended in the form of

[10] AIR 1997 SC 568

Law Audience Journal, Volume 4 & Issue 1, 10th May 2022, e-ISSN: 2581-6705, Indexed Journal, IF 5.381, Published at https://www.lawaudience.com/volume-4-issue-1/, Pages: 76 to 87,

Title: "Decryption and Protection of Data in Cyberspace: An Overview of Indian Legislations", Authored By: Mr. Sandeep Mishra, Research Scholar, Department of Legal Studies, Dr. Ram Manohar Lohiya National Law University, Lucknow. Email Id: juris.sandeep@gmail.com.

Information Technology Amendment Act, 2008 (ITAA-2008).[11] Information Technology act does not provide any definition or provision related to data privacy or data breach directly. The S. 69 of the Information Technology Act, 2000 is modeled extensively after Section 5(2) of the Telegraph Act, 1885. Section 69 of the Information Technology Act, 2000 provides for the *"power to issue directions for interception or monitoring or decryption of any information through any computer resource."* ***It lays down certain grounds including:***

i. Sovereignty or integrity of India;

ii. Defence of India;

iii. Security of the State;

iv. Friendly Relations with foreign states;

v. Public order

vi. Preventing incitement to the commission of any cognizable offence

vii. For investigation of any offence.

After recording reasons in writing, the Central Government or State government authorize any officers who can direct any agency of the to intercept, monitor, decrypt, or cause to be intercepted or decrypted any information received, created, stored, or transferred in any computer resource. The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 lay down the procedure for interception, monitoring and interception to be followed by the authorities. In the case of Facebook Inc. vs. Union of India,[12] the Supreme Court had stated that "easy availability of decryption could defeat fundamental rights and that it should be relied on only in special circumstances ensuring that privacy of an individual is not invaded." At the same time, the Supreme Court had also noted that *"the sovereignty of the State and the dignity and reputation of an individual are required to be protected. For purposes of detection, prevention and investigation of certain criminal*

[11] http://www.cyberlawtimes.com/category/cyber-laws/

[12] Facebook Inc. v. Union of India, T.P. Civ. No.(s) 1943-1946/2019

Law Audience Journal, Volume 4 & Issue 1, 10th May 2022, e-ISSN: 2581-6705, Indexed Journal, IF 5.381, Published at https://www.lawaudience.com/volume-4-issue-1/, Pages: 76 to 87,

Title: "Decryption and Protection of Data in Cyberspace: An Overview of Indian Legislations", Authored By: Mr. Sandeep Mishra, Research Scholar, Department of Legal Studies, Dr. Ram Manohar Lohiya National Law University, Lucknow. Email Id: juris.sandeep@gmail.com.

activities it may be necessary to obtain such information. De-encryption and revelation of the identity of the originator may be necessary in certain other cases."

VI.III THE DATA PROTECTION BILL, 2021:

In the year of 2019 Government of India was introduced The Personal Data Protection Bill, 2019 to deal with such problems regarding data privacy and decryption of data. But act does not turn into reality. In the year 2021 again, it was laid down before the parliament and now it is on the hand of joint parliament committee for review and suggestion. This law provides exhaustive provision related to the safety of personal and non -personal data. Hope, after passing of this piece of legislation from parliament so many debates regarding data privacy have been ended up. The data protection bill, 2021 provides a detail provision regarding Right to Forgotten, Data Protection, Protection of data of children, Data Localization, Responsibility of social media intermediaries, Transfer of sensitive and personal data, right of deceased, Data Protection Officer and Data protection Authority and Appellate Tribunal.[13] Parliament will also have to define reasonable restrictions in the case of right to privacy as it involves, already pointed out by intelligence agencies, the issues of national security. With these restrictions, defining privacy is going to be big challenge for the parliamentarians. *"You cannot define right to privacy in absolute terms. Codification of right to privacy right will be a big problem. It will be a challenge for Parliament to accurately define what constitutes privacy*"[14]

VI.IV NATIONAL CYBER SECURITY POLICY, 2013:

Another significant step taken by the government of India for ensuring cyber security and controlling cyber-attacks in India is the National Cyber Security Policy 2013, unfortunately the reactions of cyber experts over the policy in terms of privacy protection are not encouraging. The need of incorporating stringent provision in this policy to deal with privacy infringement effectively is expressed by the individuals concerned.

[13] https://sflc.in/summary-jpc-recommendations-personal-data-protection-bill-2019
[14] Prabhash K Dutta, August 24 2017, http://indiatoday.intoday.in/story/right-to-privacy-fundamental-right-parliament/1/1032794.html

Law Audience Journal, Volume 4 & Issue 1, 10th May 2022, e-ISSN: 2581-6705, Indexed Journal, IF 5.381, Published at https://www.lawaudience.com/volume-4-issue-1/, Pages: 76 to 87,

Title: "Decryption and Protection of Data in Cyberspace: An Overview of Indian Legislations", Authored By: Mr. Sandeep Mishra, Research Scholar, Department of Legal Studies, Dr. Ram Manohar Lohiya National Law University, Lucknow. Email Id: juris.sandeep@gmail.com.

VII. UNIFIED LICENSE AND MONITORING SYSTEMS:

The government has launched some application and programs for sharing and monitoring of collected data for emergency use. Authorized government agencies may track and share data with the help of Unified license and monitoring systems such as the ***Central Monitoring System (CMS), the National Intelligence Grid (NATGRID), Crime and Computer Tracking Network System (CCTNS), Lawful Intercept & Monitoring (LIMS) System***.

VII.I NATIONAL INTELLIGENCE GRID (NATGRID):

The Ministry of Home Affairs first proposed the creation of a ***National Intelligence Grid (NATGRID),*** which will give 11 intelligence and investigative agencies real-time access to 21 citizen data sources to track terror activities. These citizen data sources will be provided by various ministries and departments, otherwise called "provider agencies", and will include bank account details, telephone records, passport data and vehicle registration details, among other types of data.

VII.II CRIME AND CRIMINAL TRACKING NETWORK & SYSTEMS CCTNS:

The ***Crime and Criminal Tracking Network & Systems (CCTNS)*** would facilitate the sharing of databases among 14,000 police stations across all 35 states and Union Territories of India, excluding 6,000 police offices which are high in the police hierarchy. Rs. 2,000 crore (around USD 320 million) has been allocated for the CCTNS, which is being implemented by the National Crime Records Bureau under the national e-governance scheme. Apparently, sharing data and linking databases is not enough to track criminals and terrorists.

VII.III LAWFUL INTERCEPT & MONITORING SYSTEMS (LIMS):

In September 2013 it was reported that the Indian government has been operating Lawful Intercept & Monitoring (LIM) systems, widely in secret. In particular, mobile operators in India have deployed their own LIM systems allowing for the so-called 'lawful interception' of calls by the government. And possibly to enable this, mobile operators are required to provide subscriber verification to the Telecom Enforcement, Resource and Monitoring

(TERM) cells of the Department of Telecommunications. In the case of the Indian government, the LIM system is deployed at the international gateways of large ISPs. The functioning of these systems is immune to interception by the ISPs and is under lock and key so as to be in the complete control of the government. Though the government has mandated checks for monitoring and protection of user privacy-- it is largely absent. In effect, all Internet traffic of any user is open to interception at the international gateway of the bigger ISP from whom the smaller ISPs buy bandwidth. Since the government controls the LIMs, it directly sends software commands and sucks out whatever information it needs from the Internet pipe without any intimation and information to anyone except to those within the government who send the Internet traffic monitoring commands. This monitoring facility is available to nine security agencies including the IB, the RAW and the MHA. The governments' monitoring system which is installed between the ISPs Internet Edge Router (PE) and the core network has an 'always live' link to the entire traffic which enables the LIM system to have access to 100% of all Internet activity with broad surveillance capability based not just on IP or e-mail addresses, URL's, HTTPs, FHTpc, tele-net or webmail but even through a broad and blind search across all traffic in the Internet pipe using 'keywords' and 'key phrases.[15]

VII.IV CENTRAL MONITORING SYSTEM (CMS):

In addition to LIM systems being installed, the Government of India runs the Central Monitoring System or CMS which is a clandestine mass electronic surveillance program installed by C-DoT, a government owned telecommunications technology development center and operated by Telecom Enforcement Resource and Monitoring (TERM) cells[16]. Rule 419B under Section 5(2) of the Indian Telegraph Act, 1885, allows for the disclosure of "message related information" Call Data Records (CDR) to Indian authorities. Call Data Records, otherwise known as Call Detail Records, contain metadata (data about data) that

[15] Shalini Singh, Govt. violates privacy safeguards to secretly monitor Internet traffic, available at, http://www.thehindu.com/news/national/govt-violates-privacy-safeguards-to-secretly-monitor-internet-traffic/article5107682.ece

[16] https://en.wikipedia.org/wiki/Central_Monitoring_System

describe a telecommunication transaction, but not the content of that transaction. In other words, Call Data Records include data such as the phone numbers of the calling and called parties, the duration of the call, the time and date of the call, and other such information, while excluding the content of what was said during such calls. According to draft Rule 419B, directions for the disclosure of Call Data Records can only be issued on a national level through orders by the Secretary to the Government of India in the Ministry of Home Affairs, while on the state level, orders can only be issued by the Secretary to the State Government in charge of the Home Department.

VIII. CONCLUSION:

The importance of right to privacy for the maintenance of dignity of an individual is beyond explanation. The legislative measures are adopted in India in this regard though seem to be enough on paper but when it comes to implementation, lack of awareness amongst the users, the internet habits of the users in India and lack of expertise amongst the enforcement agencies are presenting serious challenges ahead. In today's privacy politics, the strong medicine of a privacy commission will be politically infeasible until weaker medicine has been tried. In the meantime, most of us could agree that policymakers and academics alike should work to improve public understanding of cyberspace privacy. In continuing the privacy conversation, we must recognize that a vision protective of information privacy in cyberspace will be singularly hard to maintain.

India needed to work more for enduring an effective and concrete legislation for data protection. However, while creating the laws, the legislature has to be well aware for maintaining a balance between the interests of the common people along with amicably handling the increasing rate of cybercrimes. Technological advancements such as micro cameras and video surveillance have had a profound effect on personal privacy. Everyone, be it an individual or an organization has a right to protect and preserve their personal, sensitive and commercial data and information. India at the moment needs a dedicated law protecting

the data and personal privacy of an individual. A national privacy policy is still missing in India. The laws should be made keeping both genders in mind rather than protecting only female rights because in the cyber space both males and females are equal victims. A gender-neutral law is as crucial as a technological neutral legislation.

Protecting the privacy rights of individuals requires a re-conceptualization on both personal as well as professional grounds keeping in mind human privacy in the context of Information and Communication Technologies. For privacy intactness, proper training and awareness, monitoring and auditing, and incident response is required Expression through speech is one of the basic needs provided by civil society. Variance in the scope of freedom of expression, combined with more online communication, has produced concerns about censorship in cyberspace.

Freedom of opinion and expression should be free from any kind of political, commercial or any other influences. It should be applied in non-discriminatory and non-arbitrary manner, also, should be supported by applying safeguards against any kind of abuse, hate speeches, religion biasing etc.