INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

 ISSN:2582-6433

DISCLAIMER

 ISSN:2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur.Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time &Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

 ISSN:2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN:2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN:2582-6433

IMPACT OF DATA PRIVACY AND SECURITY IN HEALTH LAW.

AUTHORED BY - MS VARSHA. P
Research scholar, School of Law, VISTAS, Pallavaram, Chennai

Abstract

This paper addresses the problem of privacy from an Indian viewpoint, focusing on the subject's legal, technological, and political facets. A framework that we have developed addresses these issues. Technological advancements include cloud computing, data mining, mobile (Geographic Knowledge Discovery), etc. Recent technological advancements and the dynamic legal field have given rise to new privacy and data protection perspectives. Privacy is the right not to infringe upon another person's rights. Because of technological advancements, privacy has become an issue for everyone, with a focus on data protection. Data protection places a strong emphasis on individual liberty, which is threatened by outside intrusion. Any new phenomenon can use the Constitution to validate its essential legal requirements. Maintaining secrecy is essential in all fields, including the health sciences. The interpretive method was employed in this study because it provides a sense of in-person contact in the healthcare setting and introduces social realities regarding the state of the health society. As a result, patients must provide their consent for the use of their medical information in writing or digitally. The consent form needs to be signed by the patient's doctor, family member, and another trustworthy party. This text delves into the challenges of upholding privacy and confidentiality in the healthcare industry, along with an examination of its significance for both individuals and the community. "Privacy rights are really important. It examines how an individual's right has been affected by the intrusion of data protection in connection with other laws.

Keywords: - Indian Perspective, Data Protection, Healthcare Bringing, Right To Privacy, Legal Requirement, Individual Liberty, Healthcare, Data Mining, Geographic, Maintaining Confidentiality, Cloud Computing, Political Domain.

 ISSN:2582-6433

I. INTRODUCTION

Human society's fundamental and unalienable rights have been reduced to a visible and enforceable document on a national and worldwide level. Certain rights are mentioned explicitly in these agreements, while others are introduced through interpretive tools since they are inextricably linked to other rights. The right to privacy is one of the more significant and widely recognized human rights among all of these. It gives individuals the ability to snoop on others. The right to privacy is mentioned in the United Nations Conventions on the Rights of the Child, the International Covenant on the Rights of Civil and Political Persons, and the UN Declaration of Human Rights. A right to privacy is among the most basic rights of an individual.

This right has been recognized as a crucial component of the freedom of speech and the right to live in freedom in India. Everyone has the right to a "personal domain" free from arbitrary government intervention or third-party monitoring. Despite the widespread acceptance of the need to preserve one's privacy, worldwide protection of human rights mechanisms have not completely defined the exact content of this right. The ambiguity surrounding the nature of this right has made it more difficult to implement and uphold. Since the right to privacy is a qualifying right, interpreting it presents difficulties in defining what defines the public interest and how to organize the private realm.

Depending on the context and viewpoint, the word "privacy" can indicate several things. Perhaps because of our culture and way of life, or because of our excitement about new and rapidly developing technologies, politicians were not compelled to incorporate the subject of privacy when drafting the country's legal framework. We must define privacy before we can talk about e-privacy and data protection from an Indian perspective. The Latin word "Privatus," which means "separate from rest," is where the term privacy originates. It can be defined as the ability of a person or group to withhold information about themselves or themselves and thus only expose certain aspects of oneself.

1.1 The Data Security Concept

Globally, the idea of data protection is becoming increasingly significant. All countries are gradually adopting laws that control the handling and mishandling of personal information as well as adopting security of information principles. The German word "Datenschutz" is where the term "data protection" originates. The idea of data protection is somewhat related to

 ISSN:2582-6433

personal privacy.

Usually, it is reserved for a collection of standards that support more interests than just protecting privacy. For data protection, factors other than privacy are taken into account. Several other, somewhat related concepts have also been brought forth, chief among them being "autonomy," "liberty," & "freedom." The individual must first and foremost determine whether they are entitled to data protection. In this arena, the extent to which such regulations should safeguard particular people as well as organisations is an evolving subject. In terms of safeguarding personal data, the concept of data protection is recognized internationally. Since "data subjects" are only defined as "living individuals," the protection of information through laws is also included in the scope of data protection".

Because an organization is not an identifiable individual and the information about it is not personal data, a corporate entity, such as a corporation with limited liability, does not have a right to access any data about itself. Therefore, issues with authority relevance related to data privacy are considered contentious. The one who, whether or not they are an official actor, will protect it out of obligation. The two main parts of the protection of data for non-governmental organizations are as follows: first, an additional constrained definition based on the idea that businesses, particularly smaller ones, should be covered by laws since information about them may inadvertently reveal information about their controllers and owners. Second, since there is a broader meaning, organizations are entitled to the same legal protections regarding information kept about them as individuals are. Different countries have different laws around the concept of data protection. The sophisticated protection of data Law of the European Union.

1.2 Status of the Constitution

The Indian constitution has a few clauses on "Right to Life & Personal Liberty" or "Freedom of Speech & Expression," among other things. These laws impact one of the fundamental rights: the right to privacy. The right to privacy has also been demonstrated time and time again to be a fundamental freedom. The conceptual framework of this proposal also has connections to the newly developed discipline known as "data protection." Data security and privacy are interdependent and tied to one another. A person's freedom of data protection is closely related to their "information". The reading of the country's top court's interpretation in conjunction with the constitution's provisions to understand how rights are expressly outlined about privacy.

 ISSN:2582-6433

It looks at the several ways that data protection is covered by laws. Ultimately, it presents a case for tackling data protection issues from a rights-based perspective. According to Sir John Simmons, "Human rights are rights that are borne by all persons [at all times and in all locations], fundamentally by virtue of their humankind as a whole, addressing the maintenance of human rights. “They will have the characteristics of universality, in the freedom [from social or legal understanding], naturalness, inalienability [from social and legal comprehension], non-forfeit ability, and imprescriptibility," he adds. An explanation of human rights can only fully convey the notion that everyone has the right to assert their freedoms”.

As a result, the idea of protecting human rights includes data protection. The independence and applicability of information security are critical to a person. Data protection also leads to the right to privacy. The most significant and insightful debate focuses on the differences between data protection and privacy. Under specific regimes, a number of interconnected domains are represented by specific connections or shadows. It includes the right to exclude management of the access to one's own domains, just as confidentiality does, which extends much beyond the mere description components of seclusion, solitary living, and the influence of others. Although they are not synonymous, solitude, isolation, and privacy are related concepts. The court's action to establish this evolving right is likewise being highlighted as a matter of right.

1.3 Examining the Correct Based Method

The many laws are the only way to examine the right-based approach to the "data protection" issue. The aim of this methodology is to examine the current state of the "data security" framework in India. The processing of information, business process, call center, accountancy, and other business processes are all being outsourced at an exponential rate as a result of the growing relevance of data protection and the development of internet-enabled services. But as technology advances, legislation must also change to keep up with the innovation.

As a result, data protection examines the extent to which Indian laws, particularly those pertaining to the Indian Constitution, safeguard personal and corporate information and data. Since the Indian Constitution is the "basic and ultimate source" through which all other laws get their legitimacy and effect, emphasis is placed on the protections afforded by it. In order to explore constitutional component concerns, these three must be brought up,

(1) Interest parties' privacy rights in actual and virtual spaces.
(2) Article 19 (1) (a) mandates of information freedom.

 ISSN:2582-6433

(3) Article 21 mandates the right of people at large to know.

II. DATA PROTECTION AND PRIVACY

It clearly addresses in the context of numerous points of view, the rights to privacy, information, and knowledge as well as electronics governance, trade secrets, and proprietary information. This research has been done to support the relationship with rights. Furthermore, the lack of equilibrium between data and information processing is another flaw in this study.

The only way to justify the right-based approach is to debate it with the other laws listed below:

2.1 Privacy Rights & Data Protection

The terms "right to privacy" and "data protection" are becoming more interchangeable. Only until the invasion of privacy is ended can "data preservation" be achieved. Technical advancement and privacy law have long been intimately related, with the protection of information in particular. The "instantaneously photos and publications companies that have entered the sacred precinct of private and local life" are lamented by Warren and Brandeis in their groundbreaking 1890 article "The Right to Privacy," along with the threat posed by several technological innovations that could fulfill the prophecy that "what whispers in the closest shall be proclaiming from the house-tops." This is when the privacy issue began. This is being established in the field of "data protection" these days. The concept of "data protection" includes several facets. The various facets of safeguarding data as a right, such as the right to access data banks, the right to verify their accuracy, the right to update and rectify them, the right to the confidentiality of sensitive data, and the right to give permission for its distribution, collectively make up the new right to privacy. Thus, as a right-based strategy in this case, the relationship between "Data Protection" and "Privacy" status is quite acceptable.

2.2 The Right to Information and Data Protection Act of 2005

"The practical framework of rights access to information for citizens that safeguards info under the oversight of government agencies in order to promote transparency and accountability... for matters concerned therewith or incidental thereto" is the claim made in India's Right to Information bill. This is the Act of 2005's preamble, and Section 2(j) defines the term "right to information." The question of whether or whether the "data" that was retained by the public authority is now relevant. It's really unclear if the digital data described in Section 2(j) clause (iv) is being maintained correctly or not.

 ISSN:2582-6433

In this Act, "data protection" refers to the treatment of personal information as a right. In Bannett Coleman's v. the Union of the Nation, the court identified that "freedom of expression and speech involves within its boundaries the right of all citizens to read and be informed" and that "it is indisputable that by the freedom of the press indicated the right of everything citizens to speak out, publish, and express their perceives." The Court held in Indian Express Newspapers (Bombay's) v. Union of India44 that "every member ought to be able to form their opinions and express them to others as an essential aspect of freedom of expression and expression." In summary, the people's right to know is the essential concept at work today".

2.3 The Information Technology and Data Protection (Amendment) Act of 2008

The "Data Privacy" and "Information Technologies Act" are specifically related to each other. The Act's objectives specifically specify the protection of cyberspace relationship matters. It provides protection against specific data breaches involving information from computer systems. Sections of the previously mentioned Act prohibit the unlawful use of computers, systems for computing, and data saved on them. A number of new provisions pertaining to "data preservation" have been included. Data protection is explicitly addressed in the Act's new Sections 43A and 72A. The 2008 Amendment Act is a noteworthy milestone in the fight against the plethora of cybercrimes that exist today. The statutory regulations governing data protection in India have been modified, ultimately giving in to the demands of the US and European countries over the last ten years. Because the service provider disclosed "personal information in violation of contractual obligation," they are currently facing jail time. Furthermore, the offender faces damages if "sensitive personal information" is made available.

2.4 Indian Penal Code and Protection of Data

The Indian Penal Code originally appeared during the British period of Indian administration. Under the chairmanship of Lord Macaulay, the first draft was composed in the 1860s. The "Indian Penal Code's" rules for "data protection" are unable to entirely satisfy every requirement as a result. Indian criminal laws do not specifically address breaches of data privacy. Such infractions will be assumed to be crimes under the Indian Penal Code associated crimes. For example, under section 403 of the Indian Penal Code, it is illegal to dishonestly misuse or convert "movable property" for a person's personal gain.

2.5 National Security & Protection of Data

In the current global environment, "national security" and "data protection" are extremely

 ISSN:2582-6433

important concepts. Every nation's criminal justice and national security organizations are extremely important for "data protection." For example, in 2013 it was reported that a person named Snowden, or Edward Snowden, had leaked United States government documents about privacy. This story raises the question of whether or not a person has any privacy at all. What level of privacy will be maintained if data is accessible to the public and can be accessed by anyone?

2.6 The Intellectual Property & Data Protection Law

When it comes to computer-related database activity, the equality of "data protection" and "intellectual property law" must be examined from a rights-based perspective. It is acknowledged that the Indian Copyright Act's section B imposes liability on anyone who knowingly uses a copy of an infringing computer program on a computer. An individual's intellectual property rights are determined by their "labour, skill, and judgment" aspects. The owner's right must be protected if any literary, dramatic, musical, artistic, or cinematographic works are sanctioned by the law. However under the Copyright Act, it can be challenging to distinguish between the protection of databases and data preservation.

2.7 Corporate responsibilities & safeguarding information

The relationship between "corporate affairs" and "data protection" is also based on a sound foundation. The corporate world is significantly impacted in several ways. Data processing, sharing, disclosure, and access are all crucial. In the business world, the custody of the data processor or controller has been crucial. Private organizations can at times be asked to share or not share.

2.8 Protecting Consumers & Data

The company's internal obstacles relationship with its customers are crucial to explaining the "data protection" issue. The Calcutta High Court ruled in Shakankarlal Agarrwalla v. State Bank of India that a banker had a duty of secrecy. In accordance with Lord Halsbury's laws of the nation of England, "unless the banker is required to do so by order of a court or circumstances that give rise to a statutory obligation of communication or safeguarding of the banker's own interest requires it, the banker will not disclose to third person without first the express and implied permission of the consumer either the contents of the client's account or any of his deals with the bank or any other information relating to the customer gained through

 ISSN:2582-6433

the retention of his account."

Personal data may only be lawfully collected under very specific circumstances and for a justifiable reason, according to EU law. In addition, individuals or entities that gather and handle your data are required by EU legislation to safeguard it against unauthorized use and to uphold the rights of data owners. The EU countries are quite concerned about the U.S.'s lack of general privacy legislation, which makes it unlikely that the country will guarantee a sufficient level of protection. Despite the administration's concentrated efforts to enact privacy laws addressing a variety of data kinds, the sheer volume of privacy-related measures in Congress raises the possibility that the United States may continue to pursue privacy legislation piecemeal.

AI technology is being quickly embraced by the Indian healthcare sector in an effort to alleviate the lack of qualified doctors and enhance the quality of data in Electronic Health Records (EHRs). In fields like predictive modeling and treatment, artificial intelligence has demonstrated encouraging outcomes. However, India is still in the early phases of developing AI for healthcare applications, and to handle the intricate issues that have not yet received enough attention, a comprehensive healthcare strategy is required. Three major categories can be used to group AI technologies: prescriptive predictive, and description.

Prescriptive AI makes recommendations for possible treatments, predictive AI forecasts future events, and descriptive AI aids in comprehending past occurrences. AI is also able to support human healthcare jobs like speech recognition, neural networks, natural language processing, and catboats. The integration of AI into Indian medical facilities represents a quantum leap in the areas of improved diagnosis, individualized treatment regimens, and effective resource management. AI applications have the potential to completely transform healthcare systems in a nation with an expanding population. Examples of these applications include image identification in diagnostics and predictive analytics for outbreaks of illnesses.

However, as India moves towards a digitally driven healthcare environment, the intersection of AI, data protection, and security becomes a crucial focus point. Protecting the privacy of health data is a major concern because diagnostic imaging, genetic data, and patient records are all digital and hence vulnerable to hacking. It becomes essential to use this extremely sensitive data ethically and protect it by the law to uphold public confidence. To guarantee the highest standards of data privacy, it is imperative to carefully examine and strengthen the

 ISSN:2582-6433

legislative framework controlling AI in healthcare. India is currently struggling to formulate strong data protection regulations. A large attack surface is created by the integration of AI algorithms and the interconnection of healthcare networks, making it vulnerable to cyber assaults.

Breach of cybersecurity puts patient privacy at risk, medical data integrity is compromised, and the accuracy of AI-assisted diagnosis is hampered. The security of these systems is critical as India advances towards the introduction of electronic health records and a Digital Health Mission.

Article 21 of the Indian Constitution defines private as freedom of speech. "Protection of Life and Personal Liberty" states that no one may be deprived of their life or freedom unless a legally prescribed process is followed. One of the essential rights guaranteed by the document known as the Constitution is the right to privacy.

Internationally, privacy is acknowledged in the same way as human rights in a variety of contexts:

- Personal confidentiality
- Personal conduct privacy
- Personal communication privacy
- Personal confidentiality of data

The phrases privacy and confidentiality are not interchangeable. Despite the frequent confusion between the phrases confidentiality, confidentiality, privacy, and information security, each has a distinct meaning and set of uses. Only "discretion when maintaining secret information" is the definition of secrecy."

III. CONFIDENTIALITY OF HEALTH AMID THE COVID-19 EMERGENCY

The privacy of another person was harmed in India by tracking contacts, surveillance, and technical instruments. The pandemic was fully contained via the application of technology. Digital devices are being used for patient databases, tracking, testing, vaccination registering, and tracking efforts. These technologies contain highly confidential data about our movements

 ISSN:2582-6433

and health, including telephone numbers, social security numbers, residential addresses, and vaccination status. A person's long medical history has been disclosed in the middle of the corona. Sharing personal information compromises privacy and has unfavorable outcomes.

It is easy to identify and recognize an individual using personal data because the information or data obtained in this regard by governmental and commercial institutions is widely distributed through social media networks. Maintaining private medical records requires medical privacy above all else. Personal health data should be collected, stored, and distributed with appropriate care to ensure the least amount of interference feasible. Privacy and health go hand in hand in contemporary society. The state should set up appropriate guidelines, rules, and legislation to protect health information. When doing scientific research and producing scientific discoveries, data, and current technology tools should preserve an individual's interests.

IV. CHALLENGES

4.1 Regulatory Challenges

It is very difficult to guarantee the protection of privacy rights in the Indian environment due to the absence of a suitable model for privacy legislation. However, the government uses a few event safeguards or proxy laws in the absence of formal legislation to protect privacy. Several laws, including Article 21 of the Indian Constitution, the IT Act of 2000, the Indian Contract Act of 1872, the Indian Penal Code, the Indian Copyright Act, the Consumer Protection Bill of 1986, the Specific Relief Act of 1963, and the Indian Telegraph Act, indirectly support concerns regarding privacy in India.

The current Indian legislative framework for privacy has the following flaws:

- There is no comprehensive law and the privacy issue is still handled by some proxies; there is no convergence on the subject.
- The data is never categorized as sensitive, private, or publicly available data.
- Absence of a legislative framework discussing who owns sensitive and private data and information.
- There is no set process for generating, processing, sending, and storing the data.
- There are no rules defining data transparency, proportionality, or quality.
- no structure addresses the problem of cross-border information flow.

 ISSN:2582-6433

Such a legal framework gap cannot be ignored in the information age, as it can seriously degrade both individuals and the country.

4.2 Problems with technology

The Indian ICT revolution and globalization have fundamentally altered the nature of information. Information became easier to obtain, carry, and use. These days, being nimble and intelligent is desired not only by the government but also by the corporate and individual sectors. Even though it has accelerated, eased, and improved our lives, it has also revealed some unexpected chaos and exposed our personal lives.

4.3 Social and Political Difficulties

For any technology to be implemented successfully, human resources must provide solid support. We discuss the human element in political problems while discussing stakeholders for a certain technology. People are the most vulnerable element in information security, according to the information technology principle. In the Indian context, humans are essential since they set policies and choose the course that whatever technology will take. Although there isn't a scam that directly affects privacy at this time, and people don't care as much about it as they used to, the adage "prevention is better than cure" applies here.

The majority of BPO's offshore work comes from nations that have codified laws or established legislative frameworks, such as the United States' ECPA and all of Europe's DPA 1998. The reason they conduct business in India is the extremely low cost of investing. They take proper care of their data by international non-governmental organizations like ITIL, ISO, and others. Due to privacy breaches resulting from a breach of trust between two parties, the majority of cases in the family court system are still pending. The media is crucial to democracy because it informs people about government policies and public grievances. However, in today's world, the media intrudes on public life and no one's personal information is kept private for their own gain.

In India, the current regulatory and legal structure about digital health is disjointed and unclear. Furthermore, India has a dearth of legal scholarship about digital health. This is especially difficult because digital health encompasses so many different areas, including business models, data gathering and processing, care delivery, and technology breakthroughs that cause the regulatory framework to become fragmented. It should come as no surprise that there is

 ISSN:2582-6433

concern regarding the extensive digitization of medical services in India given the possibility of data leaks, improper use, and insufficient oversight by private sector entities. Supporters of privacy have taken issue with government-sponsored initiatives. The legal director of the online civil rights organization SLFC.in, Prasanth Sugathan, said, "The lack of data protection legislation should not be an excuse for performing such exercises affecting the freedoms of citizens."

In this article, I critically analyze the ethical and legal concerns related to digital health legislation. I highlight these challenges with India's healthcare digitization project by referencing recent studies, legislation, and policies that the state has adopted.

V. CONCLUSION

The examination of several subjects revealed that diverse viewpoints have seen data protection as a right. The protection of data as a right was acknowledged by all subjects, including the right to security, the right to data, technological advances, the Indian Penal Code, business affairs, and consumer protection. The goal of the issue is to make data protection seem more legitimate in this era of technological liberalization. The protection of individual liberty is being threatened by the ever-expanding scope of technology, which calls for a stronger data protection system. The purpose of this research project is to prove that the right to safeguard data and privacy is a fundamental right that may be treated as such after careful consideration and examination. Only the complete legal need as a right to protect information can be achieved by others interfering with or violating an individual's liberty. A general approach to data protection might be provided by the organizational status of data protection. The various aspects of data protection, such as gathering, processing, storing, protecting, and granting access, should be integrated into a legal framework to grant specific status to safeguarding information as a right. Global knowledge of the proper foundational approach to privacy and data protection must grow to unanimity.

VI. REFERENCES

Blau, B. The adult client's conception of confidentiality in the therapeutic relationship. Professional Psychology: Research and Practice, 16 (3), 375-384.

Briere, J. Trauma Symptom Checklist for Children.

Cheng TL., Savageau JA. Sattler AL., DeWitt TG. (2016). A survey of knowledge, perceptions, and attitudes among high school students.

 ISSN:2582-6433

Daniel Masys& M.D. (2014). It's Only Sensitive If It Hurts When You Touch It

David C. Kibbe, MD &MBA (April 2005). 10 Steps to HIPAA Security. Retrieved from

Donna Cryer, J.D., CEO of CryerHealth and patient advocate, DC Patient. Patients Hold The Ultimate Responsibility Of Selecting The Right Team Member

Dr. Tony Iton. (2013). The California Endowment Health Journalism Fellowships

Edward L.Deci. & Richard M.Ryan (2014). A motivational approach to self-integration in personality. P.45 University of Rochester.

Edward Snowden. (2014). US government spied on human rights workers.

Fr Gemalto. (20 September 2016). Data breach statistics 2016: The first half results are posted on 20 September 2016.Articles: The Importance of Health Care IT Security and Privacy.

Bajpai, Nirupam, and Manisha Wadhwa. "Artificial Intelligence and Healthcare in India." No. 43. ICT India Working Paper, (2021).

Dossetor, J.B. "Beyond the Hippocratic Oath: A Memoire on the Rise of Modern Medical Ethics. Canada:" The University of Alberta Press, 301 p (2005).

Ferrer-Roca, O., and Sosa-Iudicissa, "Handbook of Telemedicine (Third printing). The Netherlands: IOS Press", 297 p. (2002).

Vijai, C., and Worakamol Wisetsri. "Rise of artificial intelligence in healthcare start-ups in India." Advances in Management 14, no. 1 (2021): 48-52.

Yaqoob, Ibrar, Khaled Salah, Raja Jayaraman, and Yousof Al-Hammadi. "Blockchain for healthcare data management: opportunities, challenges, and future recommendations." Neural Computing and Applications (2021): 1-16.

Pandey, Neena, and Abhipsa Pal. "Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice." International journal of information management 55 (2020): 102171.

Vijai, C., and Worakamol Wisetsri. "Rise of artificial intelligence in healthcare start-ups in India." Advances In Management 14, no. 1 (2021): 48-52.

Swati Sinha, "Data Protection Law in India-Needs and Position," Accessed February 21, 2015.

Mr. K.J. Doraisamy v. The Assistant General Manager, State Bank of India and others, (2007) 136 Comp Cases 568 (Mad).

M M S Karki, "Personal Data Privacy & Intellectual Property," Journal of Intellectual Property Rights, Vol 10. (2005): 59-63.

Vaishali Sharma, "You Have Zero Privacy, Get Over It :(Data Protection Law In India, Analysed In A Comparative Framework)", Accessed October 21, 2016.

 ISSN:2582-6433

Maria Grazia Porcedda "Data Protection and the Prevention of Cybercrime: The EU as An Area Of Security? European University Institute, Florence Department of Law," Accessed October 21, 2016.

Dan Jerker B. Svantesson, "Systematic Government Access to Private Sector Data in Australia," 2/4 International Data Privacy Law, (2012).

Denis O'Brien, "The Right of Privacy," Columbia Law Review, Vol. 2, No. 7 (1902): 437-448.

Daniel J. Solove & Paul M. Schwartz, "Privacy, Information and Technology," Wolter Kluwer Law & Business Publisher in New York, (2011), 79-256.

I. N. Walden and R. N. Savage, "Data Protection and Privacy Laws: Should Organizations Be Protected?" The International and Comparative Law Quarterly, Vol. 37, No. 2 (1988): 337-347.

Dr. Amit Ludri, Law on the protection of personal & official information in India, the Bright Law House, New Delhi, 1st Edition, (2010).

Graham Greenleaf and Sinta Dewi Rosadi, "Indonesia's data protection Regulation 2012: A brief code with data breach notification," Privacy Laws & Business International Report, Issue 122, (2013): 24-27.

H L A Hart, "Are There Any Natural Rights?" The Philosophical Review Vol 64, NO 2 (1955): 175-191.

Rebecca Vesely "Cop-friendly Approach to Handling Medical Data," Wired News 12 (September 1997) Accessed March 20, 2014.

Lutha R Nair, "Data Protection Efforts in India: Blind leading the Blind?" The Indian Journal of Law & Technology VOL 4 (2008).

S.K. Sharma, Privacy Law: A Comparative Study (Atlantic Publishers & Distributors: 1994).

Austin, Lisa Michelle, "Privacy law and the question of technology." Ph.D. Thesis, University of Toronto; 2005, ProQuest Dissertations and Theses.

David Flaherty, "Protecting Privacy in Surveillance Societies", University of North Carolina Press, (1989).