



A Leading Women's University

**School of Law
Mody University
of Science and Technology**

Lakshmangarh - 332311, Distt. Sikar (Rajasthan) India

Volume

10

**JOURNAL
OF THE
FACULTY OF
LAW**

2021-22

ISSN No. 2347-758X

1. **Privacy and Personal Data In Digital Age: Problems and Challenges**
Prof. (Dr.) S. Sivakumar & Prof. (Dr.) Lisa P Lukose
2. **Privacy an International Concern**
Prof. Satish C. Shastri & Dr. Aditi Sharma
3. **Development of Right to Privacy as a Human Right:
An Excursion from Ancient to Digital India**
Prof. (Dr.) Mohammad Tariq & Ms. Shelja Singh
4. **Justice K.S. Puttaswamy v. Union of India: A Case Exposition**
Dr. R.S. Solanki
5. **Right to Privacy with Reference of Social Media Laws in Nepal**
Dr. Balram Prasad Raut
6. **Data Protection Rights In India: Time To Add Habeas Data Writ In Indian Constitution**
Dr. Vishal Guleria & Dr. Harish Verma
7. **Data Protection in India: Human Rights Perspective**
Dr. Shobhna Jeet
8. **Violation of Privacy Through Surveillance in the Digital Age: A Bird's-eye View**
Mr. Shiv Kumar & Professor (Dr.) Preeti Misra
9. **Privacy: An Essential Pre-requisite in Professional Relationships**
Dr. Money Veena.V.R
10. **General Facet of Right to Privacy and Freedom of Speech**
Ms. Abha Singh
11. **The Impact of Information Technology Act on the Right to Privacy**
Ms. Deeksha Kumari
12. **A Study on Critical Analysis of Right to Privacy and Media Trial in India**
Ms. Poonam Kumari
13. **Right To Privacy: A Study into the Rampant Violation of the Right**
Ms. Megha Middha & Ms. Navna Singh



Editorial Note

The present volume-10 is a potpourri of various articles written by veteran and erudite scholars. It covers myriad aspects of law which are much discussed about now-a-days. Each article is rich with contents and analogical deductions. The authors have demonstrated extensively their skill to treat the subject in its entirety showing the deficiencies of the concerned aspect of the subject and provided innovative but practical solutions. A used range of subjects have been given systematic treatment and have been examined by the learned authors in the light of present day development in the field. Moreover, topics selected by the authors are burning problems of the society and widely deliberated upon in the present day world with special reference to India. The scholars have given a new insight to the problems.

The contributors are renowned scholars and have done a great service to the legal world by their scholarly contribution. Scholarly articles of Prof. (Dr.) S. Sivakumar and Prof. (Dr.) Lisa P Lukose, Prof. (Dr.) Mohammad Tariq, A.M. University, Dr. Balram Prasad Rao, Associate Professor, Tribuvan University, Nepal, Dr. Vishal Guleria, H.M.D. Central University, Dehradun are distinctly distinct as all have advanced their original and cerebral philosophy about the subjects. I pay my deepest gratitude for scholarly their contribution. Other contributors also deserve appreciation for their exploratory articles and dwelling upon the issues of National and International importance.

We hope that present issue of the Journal-10 is a small effort in dealing with and the exploring upon the socio-legal problems prevalent in the society. We hope that present issue will interest you and prove advantageous and useful for all-judicial officials, academicians' research scholars, students and others, equally.

We look forward for your valuable suggestions and solicit your kind cooperation in future in this endeavor which will extemporize it and make this journal more useful.

MUST LAKSHMANGARH



School of Law
Mody University of Science and Technology
Lakshmangarh - 332311, Distt. Sikar (Rajasthan) India

EDITORIAL COMMITTEE

Chief Patron

Hon'ble Shri Rajendra Prasad Ji Mody
Chairman, MUST

Patron

Dr. P K Dashora
President, MUST

Co-Patron

Prof. (Dr.) Rajeev Mathur
Director, MUST

Chief Editor

Prof. Satish C. Shastri
Dean, School of Law

Editor

Dr. R. S. Solanki
Associate Professor & HoD School of Law

Assistant Editors

Dr. Kratika Gupta, Assistant Professor
Ms. Navna Singh, Assistant Professor
Ms. Megha Middha, Assistant Professor

Ms. Sangeeta Jakhar, Assistant Professor
Dr. Aditi Sharma, Assistant Professor
Ms. Pooja Singh, Assistant Professor

Editorial Advisors Board

Hon'ble Justice Dave
Former Chairman
State Law Commission,
Jaipur, Rajasthan

Prof. S. K. Bhatnagar
Vice Chancellor
RML National Law University,
Lucknow

Prof. S. K. Rao
Vice-Chancellor
National Law University, Delhi
New Delhi

Prof. A. P. Singh
Dean, Faculty of Law
GGs Indraprastha University,
New Delhi

Prof. Madhu Shastri
Professor of Law (Rtd.)
University of Rajasthan
Jaipur

Prof. I. G. Ahmed
Dean, Faculty of Law
Sikkim University,
Sikkim

Disclaimer

The information and materials in this journal have been provided for general information purpose only and may not be comprehensive and complete. The views and observation articulated in various articles and independent opinions of the authors and writers and not of editorial board. SOL-MUST has in no way, molded or influenced their line of thinking. SOL-MUST shall be the sole copyright owner of the all published materials. Apart from fair dealing for purpose of research, study or criticism, no part of this journal may be used in any form whatsoever, without prior written permission of the University.

The editors and publisher do not claim any responsibilities for the views, facts and observation articulated by the contributors and for the errors, if any, in the information contained in the journal. The University shall not be responsible for any damages or loss, in whatever mane caused to any person consequent to any action taken on the basis of the journal.



CONTENTS

S.No.	Name of the Article	Page No.
1.	Privacy and Personal Data In Digital Age: Problems and Challenges Prof. (Dr.) S. Sivakumar & Prof. (Dr.) Lisa P Lukose	01-20
2.	Privacy an International Concern Prof. Satish C. Shastri & Dr. Aditi Sharma	21-46
3.	Development of Right to Privacy as a Human Right: An Excursion from Ancient to Digital India Prof. (Dr.) Mohammad Tariq & Ms. Shelja Singh	47-58
4.	Justice K.S. Puttaswamy v. Union of India: A Case Exposition Dr. R.S. Solanki	59-66
5.	Right to Privacy with Reference of Social Media Laws in Nepal Dr. Balram Prasad Raut	67-83
6.	Data Protection Rights In India: Time To Add Habeas Data Writ In Indian Constitution Dr. Vishal Guleria & Dr. Harish Verma	84-104
7.	Data Protection in India: Human Rights Perspective Dr. Shobhna Jeet	105-114
8.	Violation of Privacy Through Surveillance in the Digital Age: A Bird's-eye View Mr. Shiv Kumar & Professor (Dr.) Preeti Misra	115-125
9.	Privacy: An Essential Pre-requisite in Professional Relationships Dr. Money Veena.V.R	126-135
10.	General Facet of Right to Privacy and Freedom of Speech Ms. Abha Singh	136-141
11.	The Impact of Information Technology Act on the Right to Privacy Ms. Deeksha Kumari	142-147
12.	A Study on Critical Analysis of Right to Privacy and Media Trial in India Ms. Poonam Kumari	148-155
13.	Right To Privacy: A Study into the Rampant Violation of the Right Ms. Megha Middha & Ms. Navna Singh	156-165



MODY
UNIVERSITY
OF SCIENCE AND TECHNOLOGY

LAKSHMANGARH ★ RAJASTHAN

A Leading Women's University

ABOUT THE CONTRIBUTORS

Prof. S. Siva Kumar is working as Sr. Professor with the Indian Law Institute, New Delhi. He has been Member of the Indian Law Commission, New Delhi and had the opportunity to officiate as Director, Indian Law Institute. He is a prolific writer and has written more than 15 books. He has a distinction to be the Vice-chairman of the Commonwealth Legal Education Association-Asia (India) (CLEA) and Chairman MILET, India. He is also recipient of many national and international awards. He has been conferred *Honoris Causa* (LL. D) for his immense contribution in the field of Law and Mass Communication. He has also been Executive Member of SAARC Law India Chapter. He has also delivered lectures in many countries and visited prestigious legal institutions including Harvard and Yale universities. He was the member of the International Steering Committee of the Global Alliance for Justice Education (GAJE) to represent South and Central Asia (including the Mid-East) in GAJE. He is the Vice President and Trustee of Commonwealth Legal Education Association (CLEA) – London and the President of CLEA (South Asia). He has been the visiting Professor of various national and international institutions like University of Georgia, USA.

Prof. Lisa P. Lucose is a Professor of law in the GGSIndraprasth University, Delhi. She is also Secretary of the CLEA- Asia (India). She has the privilege to attend and address various National and International Conferences. She has also published articles in many national and international journals and has also 8 books to her credit. She has also been Expert Legal Member, Government of India to review the Geographical Indication Act.

Prof. Satish C. Shastri is the Dean, School of Law; Mody University and has also served University of Rajasthan in various capacities. He has also done his MSL (Master of Studies in Environmental Law) from Vermont School of Law, VT, USA. He has written 10 books in the field of environment and Human Rights. His book *Dwani Pradhushan* has been awarded 'first prize' by the Department of Forest and Environment, Union of India, Delhi. Besides this, he has also published more than six dozen articles in prestigious national and international journals. He has also lectured in many countries like USA, UK, Germany, Bangkok, Canada, China and Nepal. He is also executive member of the SAARC Law India Chapter. He has been a member of the Governing Council of the ILI, New Delhi for about ten years.

Dr. Aditi Sharma is Assistant Professor in School of Law, Mody University. She has authored one book and assisted in writing another book. She has more than 14 articles to her credit on various subjects of Women and Criminal Law, Consumer law and Constitutional law in national and international journals which have been highly appreciated. Her areas of interest are Criminal Law, Constitutional Law and Law of Tort.

Prof. Mohammed Tariq is a Professor of Law in A.M. University Aligarh and has a rich experience of teaching. He has published three books namely; 1. Labour Welfare and Dr. Ambedkar's Vision, 2. Human rights; health and related issues, 3. Human rights; issues & challenges. He has distinction of three awards namely AMP's National Award for Excellence in Education 2021 for exemplary work in the field of education, '*Shikshavidh*' (Educationist) Award and '*Utthan* Award' in the field of Legal Education & Legal Awareness. He is also associated with various Public Service Commissions of the States and the Union Public Commission.

Ms. Shelja Singh is a research Scholar in the School of Law of the Aligarh Muslim University (A Central University), Aligarh.

Dr. R.S. Solanki is Associate Professor and Head of the Law Department in School of Law, Mody University. He has a vast experience of more than 15 years along with advocacy of about seven years. He has also authored three books and 21 research articles and some book chapters. His seven articles have appeared in SCOPUS journals. He is also member of editorial boards of various law journals. He has also participated and presented papers in national and international Seminars/Conferences. Eight research scholars are pursuing their Ph. D. under his guidance and three of them have submitted the thesis. His area of interest is banking and taxation law.

Dr Balram Prasad Raut is an Associate Professor of Law at Nepal Law Campus, Tribhuvan University in Nepal since 2011. He has been practising law as an advocate in Nepal since 2004. He completed his PhD from South Asian University, New Delhi in 2020. He is a Gold Medallist in LL.M. He was awarded *Nepal Biddha Bhushan* (the second highest award for a university degree) from Rt. Hon. Dr Rambaran Yadav, President of Nepal. He has published three dozen research articles in national and international journals in the areas of comparative law, constitutional law and human rights. He recently published a text book of criminal law.

Dr. Vishal Guleria He is presently working as Assistant Professor in the Department of Law, HNBGU (Central University), Uttarakhand. He is having seventeen years of teaching experience. During his tenure, he has taught undergraduate as well as master's level students. He has guided twenty-one LL.M. students and currently two research scholars are pursuing their PhD under his guidance. He is presently working on a Minor Project sponsored by the RCC cell. He has presented research papers in over fifty National and International Conferences/ Seminars. He has also published about thirty- five research papers in reputed journals and has contributed chapter in edited books on various contemporary issues related to law.

Dr. Harish Verma, he is Principal of the Jagran School of Law, Selaqui (Dehradun). His

areas of specializations are human rights, Constitutional Law and Environmental Law. Dr. Verma has published several papers in reputed national and international journals and participated and presented papers in a number of national as well as International seminars and conferences.

Dr. Shobna Jeet, is Associate Professor in School of Legal Studies, K.R .Mangalam University, Gurugram. She has rich teaching experience and has published about 18 research papers. Besides that, she has presented about 20 papers in various national and international Seminars/Conferences.

Sh. Shiv Kumar is currently pursuing his Ph.D. from BBR Ambedkar University (Central University). He has published eight research papers to his credit.

Prof. (Dr) Preeti Misra is currently Dean, School of Legal Studies and Head, Dept. of Human Rights in BBR Ambedkar University (Central University), Lucknow. She has nearly 116 research papers and articles published in different research journals and books of national and international repute touching upon various aspects of human rights on various social, cultural and developmental issues. She has addressed and chaired/co-chaired the sessions in various international Conferences in China, Bangladesh and Thailand. She has got a rich and extensive experience of 22 years of teaching.

Dr.MoneyVeenaV.R., is Assistant Professor at Government Law College, Trivandrum. She has done her PG and Ph.D. from Department of Law, University of Kerala. She has presented papers at international and national seminars and also acted as Resource person in various seminars. She has also published research papers in various peer reviewed journals also.

Ms. Abha Singh is Assistant Professor in the University of Petroleum and Energy Studies, Dehradun. She is also pursuing research from this university. She has attended many national and international seminars/conferences and presented papers in them.

Ms. Deeksha Tewari is working as Assistant Professor in School of Law, IILM University, Gurugram (Haryana). She has also practiced in District and Session Court for some time. Her areas of interest are human rights, constitutional law and corporate law.

Ms. Poonam Kumari is currently pursuing her doctorate degree (Ph.D.) in constitution law

from the Uttarakhand University. She has earned gold medals many times in academics. She is the president and founder of a NGO “Justice for Speechless” to save and the care speechless living beings.

Ms. Megha Midda is an Assistant Professor in School of Law, Mody University for last 3 years. She has also written a book to her credit and published 6 articles in various journals of repute.

Ms. Navna Singh is Assistant Professor in Mody University for last four years and published some articles and book chapters. Her areas of interest are women and Criminal Law, Law of Evidence, Interpretation of Statutes and International Law.

PRIVACY AND PERSONAL DATA IN DIGITAL AGE: PROBLEMS AND CHALLENGES

Prof. (Dr.) S. Sivakumar & Prof. (Dr.) Lisa P Lukose***

Abstract

In the present era of ICT, consumers are concerned about internet security and privacy protection as there are rampant and increasing privacy breaches and data breaches. Privacy rights issues have received great attention in the recent past and are becoming a topic of debate as technology advances. Since most of the security breaches are the result of inadequate security procedures, internet users should have an increased awareness as to the protection of their data and privacy against these unauthorised invasions. Information security system faces new challenges and concerns as technology changes increase the chance of privacy breaches. In addition, our jurisdiction lacks effective legislative measures in this regard.

Keywords: *Privacy, Personal Data Protection, Big Data, Smart Cities, Internet of Things (IoT), Digital Age*

I. Introduction

The right to control and safeguard one's personal information and how it is used is known as privacy in common parlance. The term privacy is often interchangeably used with the word security. Both of them have similar meanings yet there exist certain vital distinctions. It's impossible to discrete one from the other because the concepts of privacy and security are intertwined in today's society. The protection of our personal information is referred to as security. Personal data of an individual can be accessed at multiple locations in the current era of ICT (information, communication and technology). This poses a threat to both privacy as well as security. It is crucial to draw a line between the two concepts as it provides insights as to the protection of privacy in the technological world.

Many consumers are concerned about internet security and privacy of their personal information although the term “information” in general parlance is now more commonly used to describe a unique product or trade item that can be bought, sold, swapped, and so on. The cost of information is frequently several times more than the cost of the systems and technologies on which it is based. Naturally, this emphasizes the importance of safeguarding

* Senior Professor, Indian Law Institute, New Delhi/ Former Member, Law Commission of India.

** Corresponding Author; Professor, University School of Law and Legal Studies (USLLS), GGSIP University, Delhi; Honorary Director, Commonwealth Institute of Justice Education and Research, (CIJER), Greater Noida.

data from unauthorized access, theft, destruction, and other crimes. Many users, however, are unaware that they are jeopardizing their security and privacy while online.

II. Privacy as a general and legal notion

The Indian judiciary and legislature have refrained from conceptually defining the term privacy. Broadly, it can be understood as the condition of being free from public intrusion or letting others have access to their undocumented personal information. Privacy as a legal notion is a very complex and diverse concept. It is one of the cardinal principles of freedom that preserves individual autonomy. However, the absence of a clear, precise, and persuasive definition of privacy is particularly shocking and inexcusable when we consider the large, significant workload that the judiciary has assigned to this concept¹. The quest for a satisfactory definition begins with the examination of essential ideas.

During the early 19th C., Louis Brandeis J. explained the concept of privacy as an “individual's right to be alone,” which shaped the development of privacy law². The philosophy of Immanuel Kant, according to which people should be treated as ends in themselves rather than as means to the aims of others, provided the foundation of the 'dignitary' concept of privacy in Continental Europe.

In legal parlance, the right to privacy has been recognized as an equitable doctrine³ and highly coveted right in a democracy. It is not a common-law right. Privacy is essential to life and liberty, and it is enshrined, as per the judicial interpretations, in the Indian Constitution as one of the fundamental rights. It exists in all people, regardless of class, socio-economic status, gender, or sexual orientation. It is very important in the development of one's character, integrity, and dignity. However, privacy is not an absolute right, but rather a privilege. In order to protect the fundamental human right of privacy, invasion against this solen right must be based on legality, necessity and proportionality. It should be acknowledged that privacy rights must be promoted and safeguarded. This privacy debate has reignited, the need for data privacy laws and the civil right to privacy of every individual, regardless of sexual orientation. By creating conditions for individualization, privacy sets the groundwork for dignity⁴.

Private space is inalienable when it comes to privacy. The demand for privacy, as well as its acknowledgment as a legal right, is a relatively new phenomenon. It is the result of individuality rather than collectivism. Privacy refers to the protection of personal

¹ WA Parent, “A New Definition of Privacy for the Law” 2 Law and Philosophy 305-338 (1983). Samuel Warren and

² Louis Brandeis, “The Right to Privacy” 4 Harvard Law Review, 193-220 (1890).

³ *Kaye v. Robertson* (1991) FSR 62 The court expressed its inability to protect the privacy of the individual and blamed the failure of common law and statute in protecting it.

Also, *Douglas v. Hello Ltd* (2001) 2 All ER 289; *Campbell v. MGN* (2003) 1 All ER 224 (CA).

⁴ Immanuel Kant, *The Moral Law: Kant's Groundwork of the Metaphysic of Morals*, translated and analyzed by H. J. Paton 90-1 (London Hutchinson University Library, 1948).

information from being made public. Privacy is restricted when public acts and information are made public. As a result, privacy limits one's right to know about others. Despite the fact that Indian privacy law is derived from tort law and constitutional law, Indian courts have mostly relied on American case law in creating privacy jurisprudence. The right to privacy as a distinct right has yet to emerge anywhere in the globe. Privacy is a self-contained area in which a person can live a private life and make decisions. Privacy is a self-contained area in which a person can live their own life and make their own decisions without intrusion.

III. Personal data and PDP

Following the footsteps of the Supreme Court after the 'right to privacy judgement', the Central Government established a data protection committee to enact stricter laws that can protect the personal data and privacy of the citizens. A committee chaired by former Supreme Court judge, Srikrishna J. was formed in August 2017, which produced an exhaustive white paper on the significance of protection of data and released a Personal Data Protection Bill, 2018 in July. On the advice of the industrial experts, the Personal Data Protection Bill, 2019 (PDP Bill) was introduced in the Lok Sabha, along with minor changes.

With the subsequent adoption of this Bill, it was expected that the right to privacy, as a basic right, would be reinforced and that persons would be protected from unfair invasions of their privacy. However, the PDP Bill was then brought up before a Joint Parliamentary Committee (for brevity “JPC”) for additional discussion and assessment on December 12, 2019. The committee suggested several changes through a report dated December 16, 2021, along with Data Protection Bill, 2021 (DP Bill)⁵. The JPC report on the PDP Bill has sparked even more controversy given the considerable revisions and deviations from the original PDP Bill.

Recommendations of the Committee

It was suggested that the Bill be renamed as the “Data Protection Bill” since it attempts to govern only the personal data of individuals. The committee accepted to change the name with a caveat that it would encompass both personal and non-personal data. It must be highlighted that the Bill allows the Central Government to obtain anonymized or non-personal data from any data fiduciary in order to better focus service delivery or formulate evidence-based policies. It thus becomes a matter of concern that integrating both personal and non-personal data in the same legislation may dilute the PDP Bill's goals, which were set

⁵ Joint Parliamentary Committee, “Report of the Joint Committee on Personal Data Protection Bill, 2019” (December, 2021) available at: http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf (last visited on March 18, 2022).

out in the first place⁶. Combining personal and non-personal data in the same legislation may undermine the PDP Bill's aims, which were intended to create an outline for the security of personal data solely.

The report also suggests that the Data Protection Authority (DPA) selection committee nominated at the Central Government's request include more technical, legal, and academic expertise, as well as the administrative officers who make up the selection committee as opposed to the PDP Bill that includes members from the Ministry of Legal Affairs and the Ministry of Electronics and Information Technology. This report further suggests adding the restriction to the exemption of 'safeguarding the national interest,' *i.e.*, an exception clause created for the government.

It is recommended that the government only be exempted from the legal provisions after following a just, fair, reasonable, and proportionate method which is in accordance with the spirit laid down by the Supreme Court's ruling in the *Right to Privacy* case⁷.

The PDP Bill made the companies duty-bound to notify personal data breaches if they caused harm to the data principal. The report on the other hand compels the keeping of a log of all types of data breaches, be it personal or non-personal, and regardless of the possibility of damage to the data principal. In addition, it sets a 72-hour reporting deadline for such breaches.

The report seeks to scrutinize social media intermediaries more closely. It has been suggested that no social networking medium be permitted to function in India until the business responsible for the technology at hand establishes a presence in the country. Furthermore, a statutory media regulatory institution, similar to the Press Council of India, might be established to regulate the material on all such media platforms.

The PDP Bill included special safeguards for the protection of children's data. The notion of a guardian as a different category of data fiduciary should be eliminated, according to the report, because it may undermine the goal of protecting children. All data fiduciaries ought to be prohibited from profiling, tracking, or behavioral monitoring of children, or targeted advertising intended at children, as well as processing personal data that may cause serious harm to children⁸. This bar only applied to guardian data fiduciaries.

The concept of data localization was already included in the PDP Bill. According to the report, the government must take along copies of all sensitive and vital personal data that

⁶ Anirudh Burman, "Will India's Proposed Data Protection Law Protect Privacy and Promote Growth?: The Growth of Privacy Regulation and the Bill" *Carnegie Endowment for International Peace* 6-7 (2020), available at: <https://www.jstor.org/stable/resrep24293.4?seq=1> (last visited on March 24, 2022).

⁷ *Justice K.S. Puttaswamy v. Union of India* (2017) 10 SCC 1

⁸ The Personal Data Protection Bill, 2019 (Bill No. 373 of 2019), Cl. 16(5).

is now housed outside of India, and all organizations operating in India should gradually move toward data localization. In addition to data localization, the Report recommends that the Central Government draught a comprehensive data localization policy aimed at creating a suitable structure for local data storage and assisting start-ups in complying with localization requests, all the while taking care of the Government's 'ease of doing business' goals in mind.

While the PDP Bill required a significant data fiduciary to appoint a data protection officer (DPO)⁹, the Report however suggests that the DPO be a senior level officer or key managerial personnel with technical knowledge in the respective significant data fiduciary's field of operations¹⁰.

Dissent to the Report

Several members of the Lok Sabha objected to the report's recommendations. The biggest worry with the Report's recommendations and the Data Protection Bill is that it offers the government a broad authority to immunize any or all of its agencies from the legislation's restrictions. The members that have dissented further point out that the report has no safeguards to ensure that individuals' right to privacy is protected. The report's recommendations have damaged the framework for privacy protection by altering the title of the Bill and broadening its scope. There have been concerns that the JPC's Report's recommendations have strayed from the framework of the PDP Bill.

However, the final decision on the right to privacy depends on the debates and reviews made in the said Bill, which are established on the suggestions of the Joint Parliamentary Committee. Because this recommended legislation will be India's first all-inclusive data protection law, it will be exciting to see how the government plans to amend the PDP Bill to defend individuals' right to privacy along with the balancing of security and interests of the nation. This may however necessitate infringement of privacy in certain cases but it is well within the parameters set by the Supreme Court of India.

IV. Privacy as an eroding notion in the digital world

Privacy in the digital age refers to an individual's ability to shape his or her own online identity and determine when, how, and where to disclose elements of that identity with other people, companies, or other entities. The ability to establish and curate a digital portrait that represents personal preference is the heart of conceptual privacy; in practice, it rests in the power to develop and curate an online identity.

These technologies have the ability to create and store a massive amount of sensitive and personal data about individuals. There are two basic ways to think about this issue:

⁹ *Ibid.*

¹⁰ *Supra* note 6.

through private-sector experience and the impact of government interference, such as monitoring, on personal liberty. Although the cultural and legal ramifications of privacy in government and business environments differ, the technology used in both is frequently similar.

Surveillance technology will continue to progress at a lightning speed, and the judicial system will continue to explore the possibilities of what is legally permissible. The views of the courts globally on these tools and techniques provide a valuable insight into cultural understanding of both technological prowess and the meaning of a digital life. While academics debate how to construct a complex legal framework that defines modern privacy, the digital age has created a thriving ecosystem of privacy-enhancing technologies. From social media to fitness monitors and medical equipment, today's huge assortment of digital technologies reflects the myriad ways people connect with technology on a daily basis.

It is a general observation that international agencies use commercial technology to monitor and gather the data of consumers. Since the consumers are becoming increasingly conscious of technology's surveillance and the accumulation of big data, several multinational corporations have started developing technologies that let users to avoid surveillance, limit companies' ability to access or share user data, or market anonymous features in their products as a selling advantage, even if they don't always work.

For instance, most of the internet browsers have a feature that allows the users to browse 'privately'. Many internet users are requesting built-in privacy-protecting modes of operation for everyday use, as seen by the widespread availability of this setting. These options are excellent for avoiding data about browsing patterns and history from being stored on the device, but it does not keep this information secret from servers or third-party tracking software placed in websites. Private browsing is a type of privacy that allows users to protect themselves from someone who is physically close to them and has access to their personal information. That is simply one facet of what being private entails. Other privacy-protecting software may interfere with tracking technology, limiting or eliminating targeted advertising and marketing.

V. Privacy and personal data: Constitutional contours

Private space is inalienable when it comes to privacy. The demand for privacy, as well as its acknowledgment as a legal right, is a relatively new phenomenon. It is the result of individuality rather than collectivism. The concept of privacy denotes the protection of information that is personal from being made public. Privacy is restricted when public acts and information are made public. As a result, privacy limits one's right to know about others.

Despite the fact that Indian privacy law is derived from tort law and constitutional law, Indian courts have mostly relied on American case law in creating privacy

jurisprudence. The right to privacy as a distinct right has yet to emerge anywhere in the globe. Privacy is a self-contained area in which a person can live a private life and make decisions. Privacy is a self-contained area in which a person can live their own lives and make their own decisions without intrusion. The right to privacy is nowhere been stated in the Indian Constitution. On the contrary during the Constituent Assembly debates, it was explicitly mentioned that the right to privacy would be disastrous. The Supreme Court, on the other hand, has excised such a right as a cingulate right from Part III of the Constitution. The court recognized a limited basic right to privacy as an emanation of articles 19 and 21 in *Govind v. State of M.P.*¹¹. The Supreme Court declared in *Rajagopal v. State of Tamil Nadu*¹² that the right to privacy has constitutional standing. The Supreme Court in *Kharak Singh*¹³ held that police domiciliary visits interfered on the petitioner's right to sleep or privacy and that such infringement was unconstitutional. Under article 21 of the Constitution, a statute adopted by the legislature would be required for the purpose. When the Police Act was formed in *Govind*¹⁴, the same police laws were upheld. As stated in *Board of Revenue, Madras v. R.S. Jhava*¹⁵, freedom from searches and seizures is a part of the right to privacy. It was decided that the executive can only use the power of search and seizure if it is granted by a statute.

Telephone tapping is a major abuse of an individual's right to privacy. The Supreme Court iterated in *Peoples Union for Civil Liberties v. Union of India*¹⁶ that telephone conversations are a vital part of a person's private life. The right to have a private phone conversation in the quiet of one's own home or business is unquestionably a right to privacy¹⁷.

In *Justice K.S. Puttaswamy v. Union of India*¹⁸, also known as the *Privacy* verdict, the Supreme Court interpreted privacy as a penumbral right under article 21 of the Indian Constitution. The Court has categorically declared that *M.P. Sharma*¹⁹ and *Kharak Singh's*²⁰ doctrinal premises are erroneous. It has also specifically overruled the *ADM Jabalpur* decision from the emergency regime. The unanimous decision on privacy reaffirms fundamental constitutional values. With the decision of the *Puttaswamy*²¹ judgement, the

¹¹ AIR 1975 SC 1378.

¹² AIR 1995 SC 264.

¹³ *Kharak Singh v. State of Uttar Pradesh* AIR 1963 SC 1295.

¹⁴ *Govind v. State of Madhya Pradesh*, AIR 1975 SC 1378.

¹⁵ AIR 1961 Mad 504.

¹⁶ AIR 1997 SC 568.

¹⁷ Ibid.

¹⁸ *Supra* note

¹⁹ *M.P. Sharma v. Satish Chandra* (1954) 1 SCR 1077.

²⁰ *Supra* note 13.

²¹ *Supra* note 7.

arguments of three great dissenters, Fazal Ali J., in *A.K. Gopalan*²², Subba Rao J., in *Kharak Singh*²³, and Khanna J. in *ADM Jabalpur*²⁴, were vindicated. *Puttaswamy*²⁵ has brought these three dissenters' brooding spirits to life. The Aadhaar-Permanent Account Number connectivity problem may also be raised as a result of the ruling. As a result, the court's decision was viewed as a setback for the government's efforts to expand the scope of Aadhaar as a required need for a variety of government services. It is argued that the privacy judgment demonstrates the tenacity of our leaders' liberalism. The fact that sexual orientation is part of privacy and is constitutionally protected is a good component of the decision. As a result, *Kaushal's*²⁶ decision upholding section 377 of the Indian Penal Code is seriously defective. Due to a glaring judicial error by the Supreme Court, same-gender intercourse remains illegal in the country. *NALSA*²⁷ and *Puttaswamy*²⁸ together laid the foundation to decriminalize consensual gay sex.

In the *privacy judgment*²⁹, the Supreme Court held that self-determination and the individual's right to make essential decisions about the way to treat one's body are at the core of the Constitution. The case of *Common Cause v. Union of India*³⁰ is the first significant application of these broad concepts to a specific scenario. As a result, *Common Cause*³¹ recognizes the right to die. It is claimed that the *Puttaswamy's*³² influence on the

Supreme Court can be seen in the restoration of Hadiya's marriage³³. *Hadiya*³⁴ has internal freedom of choice, marriage, and autonomy, according to the Court. The freedom to convert has been established by the Supreme Court as a fundamental right of choice.

“Freedom of faith is vital to his/her autonomy; selecting a faith is the substratum of personality”³⁵. The Supreme Court took a hard line against crimes committed in the name of honour, recognizing consenting adults' ability to love and marry as a basic right. “Honour killing guillotines individual liberty and freedom of choice, as well as one's own impression of choice”, the Supreme Court said³⁶. In *Puttaswamy*³⁷, the Supreme Court directed the

²² AIR 1950 SC 27.

²³ *Supra* note 13.

²⁴ 1976 AIR 1207.

²⁵ *Supra* note 7.

²⁶ *Suresh Kumar Koushal v. Naz Foundation* (2014) 1 SCC 1.

²⁷ *National Legal Services Authority (NALSA) v. Union of India*, AIR 2014 SC 1863.

²⁸ *Supra* note 7.

²⁹ *Ibid.*

³⁰ (2018) 5 SCC 1.

³¹ *Ibid.*

³² *Supra* note 7.

³³ *Shafin Jahan v. Asokan K. M.*, AIR 1959 SC 843.

³⁴ *Ibid.*

³⁵ *Shakti Vahini v. Union of India* (2018) 7 SCC 192.

³⁶ *Ibid.*

³⁷ *Supra* note 7.

government to put in place a strong data protection mechanism. The court stated that establishing a system necessitates 'a careful and sensitive balancing between individual interests and justified state concerns of the State'. Personal data should be collected in the public interest, but it should be protected and used exclusively for the purposes for which it was collected³⁸. Above all, the law must establish a properly empowered statutory authority to ensure that the promised protection of citizen data and loss of individual autonomy is implemented³⁹.

VI. International perspective

Vivian Bose J., stated, 'I make no apology for turning to older democracies and drawing inspiration from them, for though our law is an amalgam drawn from many sources, its firmest foundations are rooted in the freedoms of other lands where men are free in the democratic sense of the term'⁴⁰. 'The right to privacy was not recognized as a separate right in the Indian Constitution. However, the privacy rights were protected by a potent international legal framework in the form of the Universal Declaration of Human Rights, 1948 (UDHR) and the International Covenant on *Civil and Political Rights*, 1966 (ICCPR). Right to privacy finds its genesis in the profound political distrust in the state'⁴¹.

The Bill is based on recent privacy protection legislations in other nations, such as the EU General Data Protection Regulation (GDPR) and the Asia-Pacific Economic Cooperation (APEC) Privacy Framework. These regulations are based on earlier privacy protection regimes from the 1970s. In 1973, the US Department of Health, Education, and Welfare published a report that outlined a set of principles that have since been embraced by many countries' privacy policies.

A paper was written in response to fast technical advances in the 1970s, particularly computerization and automated processing by government and private companies. Following that, the report's principal recommendations for example no collection of data without consent, user constraints, data processing transparency, *etc.*, were accepted by organizations such as the Organization for Economic Cooperation and Development. It is debatable if data processing regulations based on 1960s technology are still appropriate in the age of big data. Kenneth C. Laudon, an academic, first pointed out the flaws in the existing framework in 1993.

The Fair Information Practices (FIP) philosophy was founded on the technological phenomenon of the 1960s when the biggest dangers to privacy were a few large-scale

³⁸ *Ibid.*

³⁹ *Ibid.*

⁴⁰ *Bidi Supply Company v. Union of India* (1973) 2 SCC 788.

⁴¹ Sheetal Asrani; Dann, "The Right to Privacy in the Era of Smart Governance: Concerns Raised by the Introduction of Biometric Enabled National ID Cards in India", 47 JILI 53- 94 (2005).

databases controlled by the Federal and State governments, or by huge financial firms. It was possible at the time for an individual to be aware of all such databases in which they appeared. However, today's large-scale database systems can be run by a personal computer (PC)-based net systems. Individuals have no way of knowing about the entire database systems in which they exist because large-size databases have become so widespread. If technology advancements in the early 1990s pushed core data regulation concepts out of step with commercial realities, the gap is now arguably even greater. The concept of meaningful consent, for example, is considerably more challenging today than it was in 1993. The law is established on the same essential principles that were first laid down in 1973. It was in this background that the national policies of India related to privacy were drafted.

VII. National law and policy: A critical appreciation

There are specific aspects in the PDP Bill that could result in ineffective regulation or significant compliance challenges as a result of the requirements it proposes. Academic literature reveals comparable flaws with data protection rules in other nations. The regulation's ability to fix problems in the data sharing sector and data processing sector is structurally limited. This is specifically true for a country like India, where regulators' capacity across industries is relatively limited. As a result, data protection laws must be formulated to safeguard individuals and society from harm caused by data processing.

A framework created with this goal in mind would result in a better balance of privacy and creativity. The Personal Data Protection Bill, 2019, and the growth of privacy regulation is the latest trend in the Indian privacy law that has been affected by global as well as national trends in the field of constitutional law. Despite the fact that the right to privacy is not officially mentioned in the Constitution, Indian courts have decided that exists as an integral part of the right to life provided by article 21. However, due to the Supreme Court's decision in *Kharak Singh v. State of Uttar Pradesh*⁴², where it was found that a constitutional right to privacy does not exist, there has always been a doubt about the exact nature of the constitutional protection of privacy. Due to two factors, it became necessary to resolve the ambiguity: (1) vociferous claims of loss of privacy in the light of the implementation of the state's project for unique biometric identification (Aadhaar) and (2) simultaneous global developments. The development of digital services in India is not a new trend. It occurred initially due to the telecom revolution and the resultant growth of the Indian IT industry.

This has had two major ramifications. First, because of the proliferation of digital services and platforms, the country is becoming increasingly interconnected. Second, the government has realized that online service delivery is a valuable tool for attaining policy goals including financial inclusion and cash transfer distribution. The implementation of

⁴² *Supra* note 13

Aadhaar has aided the second purpose significantly. The expanding ubiquity of Aadhaar, on the other hand, has been met with a barrage of criticism from a variety of sectors. One concern was that Aadhaar was being utilized for non-social welfare purposes, such as client onboarding by commercial companies. The storing of Aadhaar-related consumer data, such as metadata regarding the authentication location, was alleged to be a severe infringement of privacy.

Another major point of contention was that Aadhaar's widespread use will allow the government to conduct even more extensive monitoring. In 2013, the European Union (EU) proposed a new rule, the General Data Protection Regulation, to standardize and consolidate the EU's existing data protection framework (GDPR). The previous framework for securing personal data was based on the European Data Protection Directive of 1995. It was feared that this legislative framework would result in a fragmented data protection regime across the EU. The GDPR went through several rounds of consultations before becoming law in 2018. This endeavour in the EU to draught a comprehensive data protection policy affected the Indian debate.

The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act, 2016, was the subject of a slew of Supreme Court lawsuits challenging the law that permitted the system: the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act, 2016. The Supreme Court's five-judge bench that considered the petitions stated that, because the petitions claimed infringement of the right to privacy, it was first necessary to examine if the right to privacy existed under the Constitution.

It submitted the case to a Supreme Court bench of nine judges, which ruled in August 2017 that right to privacy did exist under article 21, that the apex court had erred in its decision in *Kharak Singh*⁴³, and that informational privacy was an element of that right to privacy. On two counts, the Supreme Court's decision differed from previous precedent. For starters, it declared unequivocally that the Constitution guaranteed a fundamental right to privacy. The more significant point in the context of this study, however, was that the right to privacy was understood as a right in and of itself, regardless of what privacy it helped safeguard in turn.

In a lengthy line of previous cases, such as the *Kharak Singh* case, privacy was utilised to defend specific interests, such as privacy from nighttime police inspections or privacy from telephone tapping in *PUC v. Union of India*⁴⁴. Instead, the Supreme Court's decision in *Puttaswamy*⁴⁵ viewed privacy as a right worth defending in and of itself. This may have shifted the focus away from the actual harm that a breach of privacy would cause.

⁴³ *Supra* note 13.

⁴⁴ *People's Union for Civil Liberties (PUC) v. Union of India*, (1997) 1 SCC 301.

⁴⁵ *Supra* note 13.

Importantly this understanding of privacy coincided with existing data protection legislation frameworks in other jurisdictions. Meanwhile, in July 2017, the government appointed a committee to research data protection issues and propose legislation in response to calls for a comprehensive data protection law. The committee, led by B.N. Srikrishna J., issued a report outlining the justification for a data protection legal framework, as well as a draught Personal Data Protection Bill, 2018. The report and draught law served as the foundation for the measure that was eventually introduced in parliament. The Bill's major feature is that it establishes a legal framework for collecting and using personal data. The Bill proposes to form a DPA for drafting regulations and enforcing the legal framework, in addition to establishing a set of rights and obligations for the handling of personal data.

The Bill also gives the central government substantive standard-setting powers⁴⁶ and charges the DPA with enforcing them⁴⁷. The Bill's broad applicability is one of its most appealing features. Except for those specifically exempted, it would be applicable to all Indian businesses once adopted. This would cover all the companies that collect data through automated techniques. For example, technology companies banking correspondents, real estate firms, hotels, and restaurants, auto dealers, and e-commerce platforms. The Bill's broad scope warrants a thorough knowledge of its contents and their anticipated consequences. Consent is a crucial feature of the Bill's proposed data protection system⁴⁸. It argues that personal data should only be treated with the consent of a free, informed, and specified person, with the ability to withdraw that consent. Any data processing that occurs without this authorization is a violation that could result in sanctions. The Bill establishes a new category of 'sensitive personal data, which can only be processed with 'explicit consent. Consent must be obtained once the user (also known as the data principal) has been adequately notified about the types of data that will be collected and the reasons for which they will be used⁴⁹.

Users and data collectors (designated as data fiduciaries in the law) must also be provided notice of their obligations⁵⁰. When executing state responsibilities permitted by law, delivering medical or health services during emergencies or epidemics, and providing services during disasters or breakdowns of public order, the Bill exempts specific instances from the notice and consent requirements⁵¹. There are other exclusions from the rules for employment-related purposes. Furthermore, laws can be enacted to enable exemptions from consent requirements for reasons such as prevention and discovery of criminal activity,

⁴⁶ *Data Protection Bill, 2021*, Cls. 35, 37, 86, 93 and 94.

⁴⁷ *Id.* at Cl. 49(1).

⁴⁸ *Id.* at Cl. 11.

⁴⁹ *Id.* at Cl. 7.

⁵⁰ *Ibid.*

⁵¹ *Id.* at Cls. 12, 13, 14.

whistleblowing; mergers and acquisitions, credit scoring, debt collection.

The data fiduciary will be responsible for ensuring that the data is correct⁵² and that it is only kept for as long as it is required for the purposes of data collecting⁵³. It will also be responsible for all of the Bill's compliance requirements. In addition, there are restrictions on how and where data can be used and stored. Data Principles have been endowed with several rights under the Bill⁵⁴. They can ask the data fiduciary to restrict or prevent the continued disclosure of personal data (a topic covered in the Bill's right to be forgotten)⁵⁵; to provide access to certain personal data it has provided to data fiduciaries in a structured, commonly used, and machine-readable format⁵⁶; to have it transferred to any other data fiduciary (right to data portability); and to correct inaccurate data (right to correction and erasure).

Additional responsibilities for data fiduciaries include implementing privacy by design (which requires them to implement business practices that can anticipate, identify, and avoid harm to data principals)⁵⁷; complying with transparency requirements⁵⁸; establishing security safeguards -including methods for de-identifying personal data and encryption, as well as steps to prevent data misuse⁵⁹; and establishing grievance-redressal systems⁶⁰. Additional responsibilities apply to significant data fiduciaries. They must analyze the impact of processing sensitive personal data before doing so, keep records of critical operations in the data life-cycle, perform data processing policy and practice audits, and employ data protection officers. Certain types of data gathering and processing are excluded from certain restrictions under the Bill.

It indicates that the central government may adopt an order exempting any agency of the government from all or any restrictions. Furthermore, elements of the Bill will not apply where data is handled for investigative, legal, domestic, journalistic, statistical, or research purposes. It also suggests some exemptions for small entities' manual processing. The Bill mandates that data fiduciaries maintain some data in India (data localization) and establishes an escalating structure for data storage and processing based on the severity of the information. It proposes three categories of data personal data, sensitive personal data, and vital personal data each with its own set of localization requirements.

⁵² Id. at Cl. 8(1).

⁵³ Id. at Cl. 9(1).

⁵⁴ Id. at Cls. 17- 20.

⁵⁵ Id. at Cl. 20.

⁵⁶ Id. at Cl. 19.

⁵⁷ Id. at Cl. 22.

⁵⁸ Id. at Cl. 23.

⁵⁹ Id. at Cl. 24.

⁶⁰ Id. at Cl. 32.

Personal data can be freely exchanged. The Bill allows for the transfer of sensitive personal data outside of the country for processing reasons alone, as long as the government has provided its approval and users have given their explicit agreement⁶¹. The measure prohibits the transfer of critical personal data (as defined by the central government) beyond the country, except under limited circumstances and after meeting certain criteria. If data fiduciaries fail to comply with specific provisions, monetary fines are contemplated. These can be as much as 4% of the data fiduciary's total worldwide turnover or an amount of 150 million Indian rupees, whichever is greater.

Finally, the Bill intends to make practices that result in the re-identification of personal data illegally⁶². This is a cognizable offence, meaning that an arrest can be made without a warrant and a nonbailable offence. As a result, the proposed Act adopts a broad preventive framework that covers a wide range of data collecting and usage practices. It establishes a number of requirements for firms that collect and utilize customer data, as well as consumer data rights. Because the measure prohibits the gathering of personal data without complying with these requirements, it will apply to both small grocery stores with simple data collection procedures and enterprises that use complex machine-learning algorithms and vast datasets. As a result, the measure will have a considerable economic impact.

Currently, India has a small number of diversified conglomerates, national and international IT corporations, and e-commerce and fintech behemoths competing for customers. Small firms, on the other hand, make up the great majority of businesses. “Of the expected number of 633.92 lakh firms, only 4000 enterprises were largely out of the MSME (micro, small, and medium enterprise) sector, according to the Ministry of Micro, Small, and Medium Enterprises' most recent annual report. Hence small enterprises will make up the vast majority of those affected by the Bill. As a result, it is critical that this Bill safeguard personal data in a way that preserves privacy while allowing for innovation and economic growth in India.

VIII. Privacy and personal data *vis a vis* national security

The Democratic National Committee (DNC) hack in the United States presents a number of serious problems in the realms of cyber security and privacy. This was first and foremost a security issue, as the breach most likely included an external government's attempt at intervening in a presidential election with the goal of manipulating the result. However, this event was also a question of privacy from another perspective. The primary goal of the DNC hack was to divulge “information that the victim wishes to keep private” and to sway its forthcoming decisions by compromising privacy.

⁶¹ Id. at Cl. 34.

⁶² Id. at Cl. 82.

If we believe that there are two questions raised by the recent DNC attack, then the natural tendency to perceive such situations as primarily a security issue might potentially distort the conversation, ignoring privacy concerns. Given the chain of events that led to the breach, the damage to the victim's privacy may merit equal, if not greater, attention than the compromised system itself. We must evaluate the episode as a whole, paying careful attention to the context. Protecting privacy in cyberspace is a difficult issue that necessitates keeping a proper distance from the government while also strengthening the responsibilities of the relevant parties.

The state's basic functions include ensuring the protection of the country and maintaining law and order. Defending the motherland from hostile cyberattacks is unquestionably one of their top priorities. As a result, it is almost self-evident that the state should have the resources to carry out its job. However, there are certain critical limitations to the right means. Firstly, unless in the most extreme circumstances, the state's measures should not interfere with the preservation of the privacy of the individuals. In such cases, the burden of proof should fall on the state, and the scope of the violation of privacy should be the least possible.

In absence of these limitations, the protection of personal information could be jeopardized. Secondly, because preventive actions of the state against a potential offender are basically actions related to a wrong not yet committed, they should be reduced to a bare minimum. It must be agreed upon that between the benefits of crime prevention and the irreversible cost of data breaches, the benefits of avoiding information leaking, or the benefits of avoiding data breaches are more urgent.

If we look at the DNC hack of the United States, at first sight, it appears to be more of a national security issue than a privacy issue. However, overemphasizing national security may overshadow the incident's opposite facet: invasion of privacy. Privacy concerns may be more pressing because any government or entity with adequate power and motivation may be tempted to conduct similarly. In this case, looking for ways to improve privacy protection could be the right lesson to learn.

IX. Information security: Conflict of personal and private interest

The Oxford Learners Dictionary defines the term information security as ways of protecting information, especially electronic data, from being used or seen without permission⁶³. This ability of preserving the integrity and secrecy must be preserved at all times. When any third party, for instance, hackers or other cybercriminals gain access to

⁶³ Information Security, "The Oxford Learner's Dictionaries", available at: <https://www.oxfordlearnersdictionaries.com/definition/english/infosec#:~:text=information%20security,used%20or%20seen%20without%20permission> (last visited on March 15, 2022).

private information, a data security breach occurs. Thus, any individual seeking to maintain their privacy must take adequate steps to safeguard information security. Information technology (IT), operational technology (OT), personal data, and operational data are the tools that collect and store the data of the users. To ensure cyber security, data and information protection must be appropriate. One method to do this is through CIA (confidentiality, integrity, and availability) triad wherein all three elements denote a crucial information security goal.

Confidentiality: The aspect of confidentiality is generally correlated with secrecy and encryption. Confidential information refers to the information that has not been altered by or shared with other people. Confidentiality in this context means that only the users that have been authorised have access to the data. Thus, a breach can occur via diverse ways, some of which include hacking and social engineering.

Integrity: Data integrity implies that the data has not been interfered with and its quality has not been compromised once it is submitted. This provides the assurance that the data has not been tampered with whether intentionally or not. However, there are two places through which data may be jeopardized, one is during the uploading or transmission phase and the second is from the place where the data is stored.

Availability: The element of availability refers to the accessibility of the information to the authorized persons or usability of any system. For this, a proper functioning computer system with adequate security mechanisms is required. It is necessary that such systems are not affected by cyber-attacks power outages, hardware failures, etc. In a cooperative environment which needs constant stability and maintenance, availability becomes an issue. Moreover, there is an added issue that any user of a computer system in such a setting can quickly obtain any information they require. Accessibility in such a setting can be assured through advanced security. Since it is inherently difficult to maintain security in a big corporation, these three constituent elements of data and information protection must be employed while developing such security strategies. A well-structured security policy, resting on different pillars can help in managing the threats to security in an effective manner.

X. Social computing, computing challenges and IoT challenges

Social computing refers to systems that support the gathering, representation, processing, use, and dissemination of information that is distributed across social collectivities such as teams, communities, organizations, and markets. Security risks of social computing include possible legal infringement, corporate disrepute, leakage of confidential information, identity theft. Productivity risk, particularly when staff is permitted to access external social networking sites. Some academics have predicted the onset of the fourth industrial revolution, citing recent improvements in numerous digital

technologies. This technological advancement is aided by numerous breakthroughs in biology, materials, and computation. Among these, the Internet of Things (IoT), a branch of connection that has grown out of the Internet (or world wide web), is wreaking havoc on civilization. The consequences are not simply financial, but also social and political. Being able to digitally connect and perceive physical items and the environment allows us to acquire previously elusive data, allowing us to comprehend and act on situations more efficiently, effectively, and precisely. The Internet of Things' potential impact on productivity, job functions, social inclusion, and global rivalry could both empower and harm current human institutions.

IoT's societal impact

The digital transformation of the world has led to the fourth industrial revolution which is producing smart systems and surroundings. A number of economic trends are expected to emerge. Physical resources can be employed in a more effective and thorough manner, which will support new business models, based on product outcomes and may result in lower demand for specific products. To secure the viability of businesses or livelihoods, ownership of facilities or assets will become less important. Due to enhanced connectivity, improved loyalty, and the emergence of consumer exit barriers, businesses and customers will form deeper relationships, even partnerships.

Because corporations will not be able to recoup their investments in facilities and products in the near future, a more active financial system is required to help businesses maintain their cash flow in the interim. The dynamic interaction of humans and smart systems, on the other hand, has far-reaching consequences that go beyond economics and industry. It has a number of labour, social, security, privacy, financial, and ethical concerns that will cause significant societal changes. Despite their many advantages, machines and systems were designed to accomplish activities that humans did not want to do or were not skilled at, allowing humans to focus on more rewarding labour tasks. The fourth industrial revolution, on the other hand, will tip the scales.

It is no longer true that only humans can perform tasks that require perception, dexterity, and flexibility. In today's smart systems, the equivalency of human senses and neurological systems supports their capacities to perceive, learn, and accomplish complicated tasks that require more than simply physical accuracy and power. Smart systems may already interface and communicate with customers in a simple and effective manner, eliminating the need for specialised people to connect with IT or physical infrastructure. Smart systems can also collaborate and plan ahead of time without the need for human participation or coordination. These developments will put a significant percentage of our workforce at risk, as they rely on and are comfortable performing tasks that machines previously could not.

Nations should not fall into the trap of choosing a technology-driven, data-driven, and user-centric approach to the Fourth Industrial Revolution i.e., Digital Fusion with the Internet of Things, but rather a service-driven, data-driven, and user-centric strategy. Efforts must be taken to ensure that our transition to the next stage of society is done safely and securely.

XI. BD and BDA challenges

Big data (BD) and data analytics are two sources of BDA. Big data is the storage and analysis of large amounts of complicated data using a variety of technologies. These technologies include, but are not limited to map reduce, artificial intelligence, and machine learning, all of which require significant computational capacity to evaluate enormous datasets gathered from multiple sources.

The science of evaluating raw data to obtain valuable information using analytical methods such as mining or predictive analytics and descriptive analytics is known as data analytics. Data analytics, which encompasses procedures like as data inspection, cleansing, transforming, and modeling, can assist in discovering trends and patterns in data to aid decision-making. As a result, BDA is built on the foundation of big data and data analytics. In highly competitive contexts, BDA can increase services, mass customization, digital marketing, and overall performance of the supply chains (SC).

The use of big data analytics (BDA) in the industry has risen dramatically in recent years. Organizations today collect user data (e.g., data collecting) on a continual basis in order to improve their business efficiencies and processes. Managers, policymakers, and executive officers are now routinely embracing technology to transform this plentiful raw data into valuable, illuminating information, with significant volumes of stored data or data-related electronic transactions being used in support of decision making.

The need for BDA capability in organizations is recognized as a data-driven tool to enable informed decision-making. Managers prefer data-driven judgments to trusting their intuitions in today's highly dynamic corporate environment organizational and technological capabilities for extracting value from data are being developed by businesses, giving them a competitive advantage over their competitors. Analysts, on the other hand, encounter substantial difficulties in recognizing the potential for deriving value from the obtained data or information. The value derived from data is determined by the organization's ability to capture, store, and analyze data using modern analytic tools and methods such as big data analytics (BDA). Indeed, different information and communication technologies for the management of supply chains (SC) that generate vast volumes of data have sparked substantial interest in the previous decade.

The review work provides detailed applications of BDA in the supply chain. Also examine the future implications of BDA in supply networks. BDA was discovered to improve supplier performance management, demand forecasting, and safety stock reduction. Furthermore, big data may play an important role in determining supply chain sustainability. Despite the fact that the big data phenomenon is widely regarded as the most recent worldwide sensation, its rise was not hastened. Many businesses are hesitant to employ BDA technologies because of behavioural and organizational challenges, as well as a lack of awareness of the potential benefits.

The perspective of technology for rationalizing financial gains, social media, and its applications in supply chain management have all received a lot of attention in the BDA arena. However, there is currently little research on identifying the barriers to BDA implementation in underdeveloped nations such as India. Furthermore, no previous research studies in the Indian manufacturing SC have investigated the mutual influence of the major hurdles to BDA adoption using a multi-criteria decision-making approach.

XII. Other gray areas

Smart cities

Governments all around the world are in the midst of technological advancements and have started developing 'smart cities. The information and communications technology (ICT)-infused infrastructures assist in observing and navigating the maintenance of the city, by keeping a check on air quality index, movement of people, the consumption of energy, etc. Clearly, these operations require and generate a large amount of data.

In this context, personal data comprises of information that has been collected from city registrations, surveys conducted by the government or corporations, and information available through social media, in addition to the large figures generated by monitoring systems. These data are increasingly being aggregated and connected to develop composite measures of city well-being, economic vitality, and safety. Most of the data is made available to the general public by the governments. This raises concerns on the accessibility of the public over private data. However, the main discussion should be centered on what privacy framework is suitable for linking disparate data sets. It has been suggested by some people that big data will help in making a city more prosperous while others believe that it will lead to a data-driven environment that prohibits deviance and controls originality. These 'Orwellian city data politics' as well as the subject of how particular data gathering and analysis procedures have harmful societal impacts receive little attention. It has been claimed that the pervasive collecting of data on all city operations could lead to the creation of 'panoptic' cities. The panoptic schema, without disappearing as such or losing any of its properties, was destined to spread throughout the social body, its vocation was to become a

generalized function. We are neither in the amphitheater, nor on the stage, but in the panoptic machine, invested by its effects of power, which we bring to ourselves since we are part of its mechanism⁶⁴.

XIII. Conclusion

Due to globalization and the subsequent rise of information technology, there has been a considerable upsurge in the number of internet users. This has led to an increase in the utilization of IT to acquire and collect the personal data of consumers. This has a severe repercussion, both positive as well as negative on the privacy of the individual. With the advent of the internet, people have been endowed with ease and accessibility in various aspects of their life. However, at the same time their privacy has been increasingly put at risk. The dissemination of sensitive personal data such as exposing of information related to credit card, hacking of bank's network are only the tip of the iceberg. There are various other concerns that have arisen recently due to the rapid advance in technology. With each development, there are many potential privacy dangers and risks. For instance, the ICT-enabled infrastructures of smart cities have led to a panoptic environment. The legal system needs to keep up with these rapid advancements. One way to achieve it is through an effective legislation.

⁶⁴ Michel Foucault, "Discipline and Punishment: The Birth of the Prison" (Pantheon Books, New York 1977).

PRIVACY AN INTERNATIONAL CONCERN

Old Wine in a New Bottle?

Prof. Satish C. Shastri* & Dr. Aditi Sharma**

Abstract

The right to privacy is a fundamental human right under international law. The right to privacy for an individual is the right to hide or obscure elements of their life from the wider public. In the modern age, the need for privacy is becoming increasingly difficult in light of modern communication companies which seek to make once which was considered private, public. The right to privacy has historically not been at the forefront of discussions within the international community and the United Nations. The focus from the international community is on addressing not only the practices of state sponsored surveillance but also surveillance undertaken by modern communications companies. The ambivalent attitude of the Supreme Court has not been consistent whether to recognised privacy as a right included under fundamental right to life and personal liberty. The evolution and development of right to privacy can be traced in series of judgments conveyed by the Supreme Court of India over the period of time. Recently, efforts have been made by the court to define the tenuous concept of privacy and to recognise privacy as a framework of rights which is applicable in both public and personal domains. The advent of technology has changed the medium of privacy and introduced us with new dimension of privacy i.e., informational privacy. Every individual has information related to his/her in some form or the other in the cyberspace. This information is either in the custody of state or non-state actors and not with the individual. Thereby possibility and dangers related to the misuse and mishandling of information cannot be ignored. Hence, in this research paper an in-depth analysis will be made about mapping the interest implicated to right to privacy related to information.

Introduction

THE CONCEPT of 'Privacy' has been a matter of debate, discussions and deliberations since its inception. However, the recent Judgement delivered by the Supreme Court in the case of *Justice K.S. Puttaswamy (Retd) v. Union of India*¹ has gained more prominence to the concept of Privacy in India as it dealt with the issues related to *aadhaar* database. The *aadhaar* is a database containing intrinsic details of the citizens including their

* Dean, School of Law, Mody University, Lakshamngarh, Sikar, Rajasthan- 332311

** Assistant Professor, School of Law, Mody University, Lakshamngarh, Sikar, Rajasthan- 332311

¹ Justice K.S. Puttaswamy (Retd) v. Union of India (2017) 10 SCC 1.

bio-metric information.² This creates a provision for privacy related to the person's information i.e., informational privacy. It was argued that the compulsory requirement of aadhaar for access to social welfare schemes violates the right to privacy of an individual. As Aadhaar includes bio-metric information and it is connected with bank accounts, permanent account number (PAN) etc., there is every possible chance that the information collected and connected through Aadhaar may get misused and will eventually hamper the framework of interest associated with privacy of citizens.

Concept of privacy

Privacy is a subjective concept which varies from person to person. It originates from the term "*Privatus*" which means separated from the rest of the world. Steven Lukes, in his article on 'The Meanings of "Individualism"' explains that the concept of Privacy is evolved and developed through the perception of "Individualism"³. Individualism is a moral stance, political philosophy, ideology or social outlook that stresses "the moral worth of the individual". The theory of individualism reflects that an individual is an independent entity because the creator has granted life to him/ her and thereby an individual can avail all the freedom including privacy. According to John Locke, privacy is intrinsic to the notion of freedom. As per Locke's views, "a person who operated within the confine of a social contract, but is free within the confines of those contracts"⁴ and only in the state of war he can give this freedom. Privacy allows every individual to be left alone in a core which is sacrosanct. As discussed by Charles Warren and Louis D. Brandeis in the famous article, "The Right to Privacy", "Once a civilization has made a distinction between the 'outer' and the 'inner' man,

between the life of the soul and the life of the body, between the spiritual and the material, between the sacred and the profane, between the realm of God and the realm of Caesar, between Church and state, between rights inherent and inalienable and rights that are in the power of government to give and take away, between public and private, between society and solitude, it becomes impossible to avoid the idea of privacy by whatever name it may be called- the idea of a private space in which man may become and remain himself"⁵.

Privacy is a prerequisite for the enlargement and salvation of personhood. Jeffrey Reiman defined privacy as, "a recognition of one's ownership of his or her physical and

² R. Venkata Rao, Subha Rao (eds), "A Public Disclosure on Privacy An Analysis of Justice K.S. Puttaswamy v. UOI" (NLSIU, Bangalore, 1/2018).

³ Steven Lukes, "*The Meanings of Individualism*" 32 (1) JHI, 45-66(1971), available at: <http://www.jstor.org/stable/2708324>. (last visited on Jan. 1, 2022).

⁴ Bishop, Philip Schuyler, "*Three theories of individualism*" (2007). (Unpublished Graduate Thesis, University of South Florida), available at: <http://scholarcommons.usf.edu/etd/636> (last visited on Jan. 2, 2022)

⁵ Samuel Warren, Louis Brandies, "*The Right to Privacy*" 4 HLR 193 (1890).

mental reality and a moral right to his or her self-determination”⁶. Privacy is the inner sanctum of a person or reservation of private space which is inviolable, but still somewhere it is conditioned by his/her relationship with the rest of the society. As these relationships always carry with them questions to autonomy and free choice of an individual. Further, the pressure of the state and non-state entities design aspects of social existence which force an individual to surrender his choices.

Alan Westin identifies four characteristics of privacy *i.e.*, solitude, intimacy, anonymity, and reserve⁷. According to Westin, “Solitude is a physical separation from others. Intimacy is a close, relaxed, and frank relationship between two or more individuals that results from the seclusion of a pair or small group of individuals. Anonymity is the desire of individuals for times of public privacy. Lastly, reserve is the creation of a psychological barrier against unwanted intrusion; this creation of a psychological barrier requires others to respect an individual's need or desire to restrict communication of information concerning himself or herself”. These characteristics of privacy are so fundamental in an individual's life that it becomes inalienable unless it is affecting the society adversely.

As Salmond has defined right as, “an interest and protected by a rule of right. It is any interest, respect for which is a duty and this disregard of which is a wrong”⁸. Considering the meaning of right expressed by Salmond, right to privacy is every individual's interest and therefore it not only needs to be recognised but also needs to be protected from state's interference as well as from third parties.

Defining Privacy

Of all the human rights in the international catalogue, privacy is perhaps the most difficult to define and circumscribe⁹. Privacy has roots deep in history. The Bible has numerous references to privacy¹⁰. There was also substantive protection of privacy in early Hebrew culture, Classical Greece and ancient China¹¹. These protections mostly focused on the right to solitude. Definitions of privacy vary widely according to context and environment. In many countries, the concept has been fused with Data Protection, which interprets privacy in terms of management of personal information. Outside this rather strict context, privacy protection is frequently seen as a way of drawing the line at how far society

⁶ Jeffery L. Johnson, “*A Theory of the Nature and Value of Privacy*”, 6(3) Public Affairs Quarterly 271-288 (1992), available at: <https://www.jstor.org/stable/40435812> (last visited on Dec. 15, 2020).

⁷ Leon A. Pastalan, “*Privacy as a Behavioural Concept*” 45(2) Social Science 94 (1970), available at: <https://www.jstor.org/stable/41963409> (last visited on Dec. 15, 2020).

⁸ “*Concepts of Law*”, available at: https://shodhganga.inflibnet.ac.in/bitstream/10603/71969/3/03_chapter%201.pdf (last visited on Nov. 6, 2020).

⁹ James Michael, *Privacy and Human Rights*, UNESCO 1994 p.1.

¹⁰ Richard Hixson, *Privacy in a Public Society: Human Rights in Conflict* 3 (1987). See Barrington Moore, *Privacy: Studies in Social and Cultural History* (1984).

¹¹ Simon Davies “*Big Brother: Britain's web of surveillance and the new technological order*”, Pan, London, 1996 p. 23

can intrude into a person's affairs. It can be divided into the following facets:

- **Information Privacy**, which involves the establishment of rules governing the collection and handling of personal data such as credit information and medical records;
- **Bodily privacy**, which concerns the protection of people's physical selves against invasive procedures such as drug testing and cavity searches;
- **Privacy of communications**, which covers the security and privacy of mail, telephones, email and other forms of communication; and
- **Territorial privacy**, which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space.

The lack of a single definition should not imply that the issue lacks importance. As one writer observed, "in one sense, all human rights are aspects of the right to privacy."

Some viewpoints on privacy¹²:

In the 1890s, future U.S. Supreme Court Justice Louis Brandeis articulated a concept of privacy that urged that it was the individual's "right to be left alone." Brandeis argued that privacy was the most cherished of freedoms in a democracy, and he was concerned that it should be reflected in the Constitution¹³.

The Preamble to the Australian Privacy Charter provides that, "A free and democratic society requires respect for the autonomy of individuals, and limits on the power of both state and private organizations to intrude on that autonomy. Privacy is a key value which underpins human dignity and other key values such as freedom of association and freedom of speech. Privacy is a basic human right and the reasonable expectation of every person."¹⁴

Alan Westin, author of the seminal 1967 work "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.

According to Edward Bloustein, privacy is an interest of the human personality. It protects the inviolate personality, the individual's independence, dignity and integrity¹⁵.

According to Ruth Gavison, there are three elements in privacy: secrecy, anonymity and solitude. It is a state which can be lost, whether through the choice of the person in that

¹² Volio, Fernando. *"Legal personality, privacy and the family"* in Henkin (ed) *The International Bill of Rights*, New York: Columbia University Press, 1981.

¹³ Samuel Warren and Louis Brandeis, *"The right to privacy"*, Harvard Law Review 4, 1890 pp 193 - 220.

¹⁴ *"The Australian Privacy Charter"*, published by the Australian Privacy Charter Group, Law School, University of New South Wales, Sydney 1994.

¹⁵ *Privacy as an Aspect of Human Dignity*, [1964] 39 New York U. L.R. 962 at 971.

state or through the action of another person¹⁶.

The Calcutt Committee in the UK said that, "nowhere have we found a wholly satisfactory statutory definition of privacy." But the committee was satisfied that it would be possible to define it legally and adopted this definition in its first report on privacy:

The right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information¹⁷.

The Right to Privacy

Privacy can be defined as a fundamental (though not an absolute) human right. The law of privacy can be traced as far back as 1361, when the Justices of the Peace Act in England provided for the arrest of peeping toms and eavesdroppers¹⁸. In 1765, British Lord Camden, striking down a warrant to enter a house and seize papers wrote, "We can safely say there is no law in this country to justify the defendants in what they have done; if there was, it would destroy all the comforts of society, for papers are often the dearest property any man can have." [Parliamentarian William Pitt wrote, "The poorest man may in his cottage bid defiance to all the force of the Crown. It may be frail; its roof may shake; the wind may blow though it; the storms may enter; the rain may enter - but the King of England cannot enter; all his forces dare not cross the threshold of the ruined tenement."]

Various countries developed specific protections for privacy in the centuries that followed. In 1776, the Swedish Parliament enacted the "Access to Public Records Act" which required that all government-held information be used for legitimate purposes. In 1792, the Declaration of the Rights of Man and the Citizen declared that private property is inviolable and sacred. France prohibited the publication of private facts and set stiff fines in 1858. In 1890, American lawyers Samuel Warren and Louis Brandeis wrote a seminal piece on the right to privacy as a tort action describing privacy as "the right to be left alone."¹⁹

The modern privacy benchmark at an international level can be found in the 1948 Universal Declaration of Human Rights, which specifically protected territorial and communications privacy. Article 12 states:

No-one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks²⁰.

¹⁶ *Privacy and the Limits of Law*, [1980] 89 Yale L.J. 421, at 428.

¹⁷ Report of the Committee on Privacy and Related Matters, Chairman David Calcutt QC, 1990, Cmnd. 1102, London: HMSO, page 7.

¹⁸ The Rachel affaire. Judgment of June 16, 1858, Trib. pr. inst. de la Seine, 1858 D.P. III 62. See Jeanne M. Hauch, *Protecting Private Facts in France: The Warren & Brandeis Tort is Alive and Well and Flourishing in Paris*, 68 Tul. L. Rev. 1219 (May 1994).

¹⁹ Warren and Brandeis, *The Right to Privacy*, 4 Harvard L.R. 193 (1890).

²⁰ *Universal Declaration of Human Rights*, <<http://www.hrweb.org/legal/udhr.html>>

Numerous international human rights covenants give specific reference to privacy as a right. The International Covenant on Civil and Political Rights (ICCPR), the UN Convention on Migrant Workers and the UN Convention on Protection of the Child²¹ adopt the same language.

On the regional level, these rights are becoming enforceable. The 1950 Convention for the Protection of Human Rights and Fundamental Freedoms²², Article 8 states:

- (1) Everyone has the right to respect for his private and family life, his home and his correspondence.
- (2) There shall be no interference by a public authority with the exercise of this right except as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health of morals, or for the protection of the rights and freedoms of others.

The Convention created the European Commission of Human Rights and the European Court of Human Rights to oversee enforcement. Both have been particularly active in the enforcement of privacy rights and have consistently viewed Article's protections expansively and the restrictions narrowly²³. The Commission found in its first decision on privacy:

For numerous Anglo-Saxon and French authors, the right to respect "private life" is the right to privacy, the right to live, as far as one wishes, protected from publicity. In the opinion of the Commission, however, the right to respect for private life does not end there. It comprises also, to a certain degree, the right to establish and develop relationships with other human beings, especially in the emotional field for the development and fulfilment of one's own personality²⁴.

The Court has reviewed member states laws and imposed sanctions on several countries for failing to regulate wiretapping by governments and private individuals. It has also reviewed cases of individuals access to their personal information in government files to ensure that adequate procedures were implemented²⁵. It has expanded the protections of Article 8 beyond government actions to those of private persons where it appears that the government should have prohibited those actions. Presumably, under these combined

²¹ UNGA Doc A/RES/44/25 (12 December 1989) with Annex, Article 16.

²² *Convention for the Protection of Human Rights and Fundamental Freedoms Rome*, 4.XI.1950. <<http://www.coe.fr/eng/legaltxt/5e.htm>>.

²³ Nadine Strossen, Recent US and Intl. Judicial Protection of Individual Rights: A comparative Legal Proces Analysis and Proposed Synthesis, 41 Hastings L.J. 805 (1990).

²⁴ *Xv. Iceland*, 5 Eur. Commn H.R. 86.87(1976).

²⁵ Judgement of 26 March 1987 (Leander Case)

analyses, the court could order the imposition of data protection laws if data was improperly processed to the detriment of the data subject²⁶.

Article 11 of the American Convention on Human Rights sets out the right to privacy in terms similar to the Universal Declaration. In 1965, the Organization for American States proclaimed the American Declaration of the Rights and Duties of Man, which called for the protection of numerous human rights including privacy²⁷. The Inter-American Court of Human Rights has also begun to address privacy issues in its cases.

The Evolution of Data Protection

Interest in the right of privacy increased in the 1960s and 1970s with the advent of information technology (IT). The surveillance potential of powerful computer systems prompted demands for specific rules governing the collection and handling of personal information. In many countries, new constitutions reflect this right.

The genesis of modern legislation in this area can be traced to the first data protection law in the world enacted in the Land of Hesse in Germany in 1970. This was followed by national laws in Sweden (1973), the United States (1974), Germany (1977) and France (1978).²⁸

Two crucial international instruments evolved from these laws. The Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data²⁹ and the Organization for Economic Cooperation and Development's Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data³⁰ articulate specific rules covering the handling of electronic data. The rules within these two documents form the core of the Data Protection laws of dozens of countries. These rules describe personal information as data which are afforded protection at every step from collection through to storage and dissemination. The right of people to access and amend their data is a primary component of these rules.

The expression of data protection in various declarations and laws varies only by degrees. All require that personal information must be:

- obtained fairly and lawfully;

²⁶ Rolv Ryssdal, Data Protection and the European Convention on Human Rights in Council of Europe Data protection, human rights and democratic values, XIII Conference of the Data Commissioners 2-4 October 1991 41-43. (1992).

²⁷ O.A.S. Res XXX, adopted by the Ninth Conference of American States, 1948 OEA/Ser. L./V/I.4 Rev (1965).

²⁸ An excellent analysis of these laws is found in David Flaherty, *"Protecting Privacy in surveillance societies"*, University of North Carolina Press, 1989.

²⁹ Convention of the Protection of Individuals with regard to the Automatic Processing of Personal Data Convention, ETS No. 108, Strasbourg, 1981. <<http://www.coe.fr/eng/legaltxt/108e.htm>>.

³⁰ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. <http://www.odpr.org/restofit/Legislation/Directive/Directive_Contents.html>.

- used only for the original specified purpose;
- adequate, relevant and not excessive to purpose;
- accurate and up to date; and
- destroyed after its purpose is completed.

These two agreements have had a profound effect on the adoption of laws around the world. Over twenty countries have adopted the COE convention and another six have signed it but have not yet adopted it into law. The OECD guidelines have also been widely used in national legislation, even outside the OECD countries.

The European Telecommunications Directive and the European Data Protection Directive In the past three years, the European Union has enacted two directives which will provide citizens with a wider range of protections over abuses of their data. The Directives set a baseline common level of privacy which not only reinforces current data protection law, but which extends it to establish a range of new rights.

The Data Protection Directive sets a benchmark for national law which will harmonize law throughout the European Union. Each EU State must pass complementary legislation by October 1998, though it is more likely that not all will have completed the process until the early part of 1999. The Telecommunications Directive³¹ establishes specific protections covering telephone, digital television, mobile networks and other telecommunications systems.

Several principles of data protection are strengthened under the Directives, namely the right to know where the data originated, the right to have inaccurate data rectified, a right of recourse in the event of unlawful processing and the right to withhold permission to use data in some circumstances. For example, individuals will have the right to opt-out free of charge from being sent direct marketing material, without providing any specific reason. The Data Protection Directive contains strengthened protections over the use of sensitive personal data relating, for example, to health or finances. In the future, the commercial and government use of such information will generally require "explicit and unambiguous" consent of the data subject.

The key concept in the European model is "enforceability." The European Union is concerned that data subjects have rights that are enshrined in explicit rules, and that they can go to a person or an authority that can act on their behalf. Every EU country will have a Privacy Commissioner or agency that enforces the rules. It is expected that the countries with which Europe does business will have to have a similar level of oversight.

³¹ Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector (DIRECTIVE 97/66/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 December 1997). <<http://www2.echo.lu/legal/en/dataprot/protection.html>>.

The Directive imposes an obligation on member States to ensure that the personal information relating to European citizens is covered by law when it is exported to, and processed in, countries outside Europe³². This requirement has resulted in growing pressure outside Europe for the passage of privacy laws. Those countries which refuse to adopt meaningful privacy law may find themselves unable to conduct certain types of information flows with Europe, particularly if they involve sensitive data.

The Telecommunications Directive imposes wide scale obligations on carriers and service providers to ensure the privacy of users' communications. The new rules will cover areas which until now have fallen between the cracks of data protection laws. Access to billing data will be severely restricted, as will marketing activity. Caller ID technology must incorporate an option for per-line blocking of number transmission. Information collected in the delivery of a communication must be destroyed once the call is completed.

Models of Privacy Protection

There are currently several major models for privacy protections. In some countries, several models are used simultaneously.

The regulatory model adopted by Europe, Australia, Hong Kong, New Zealand, Central and Eastern Europe and Canada is that of a public official who enforces a comprehensive data protection law. This official, known variously as a Commissioner, Ombudsman or Registrar, monitors compliance with the law and conducts investigations into alleged breaches. In some cases, the official can find against an offender. The official is also responsible for public education and international liaison in data protection and data transfer. This is the preferred model for most countries adopting data protection law. It is also the model favored by Europe to ensure compliance with its new data protection regime. However, the powers of the commissions vary greatly and many report a serious lack of resources to adequately enforce the laws.

Some countries such as the United States have avoided general data protection rules in favor of specific sectoral laws governing, for example, video rental records and financial privacy. In such cases, enforcement is achieved through a range of mechanisms. The problem with this approach is that it requires that new legislation be introduced with each new technologies so protections frequently lag behind. The lack of legal protections for genetic information in the U.S. is a striking example of its limitations. In other countries, sectoral laws are used to compliment comprehensive legislation by providing more detailed

³² Article 25 of the Directive stipulates that in many circumstances, the level of protection in the receiving country must be "adequate" - an expression which is widely accepted to mean "equivalent". Article 26 lays out certain options for transferring data out of Europe in circumstances where the level of protection is not deemed adequate. These include consent and contracts.

protections for certain categories of information, such as police files or consumer credit records.

Data protection can also be achieved - at least in theory - through various forms of self-regulation, in which companies and industry bodies establish codes of practice. However, the record of these efforts has been disappointing, with little or no evidence that the aims of the codes are regularly fulfilled. Adequacy and enforcement are the major problem with these approaches. Industry codes in many countries have tended to provide only weak protections and lack enforcement. This is currently the policy promoted by the governments of United States, Singapore and Australia.

With the recent development of commercially available technology-based systems, privacy protection has also moved into the hands of individual users. Users of the Internet can employ a range of programs and systems which will ensure varying degrees of privacy and security of communications. Questions remain about security and trustworthiness of these systems. Recently, the European Commission evaluated some of the technologies and stated that the tools would not replace a legal framework.³³

The Technologies of Privacy Invasion

The report found a number of technologies were causing new concerns about the protection of privacy. Many of these technologies were being adopted and implemented outside legal protections.

Identity systems

Identity (ID) cards

Identity (ID) cards are in use in one form or another in virtually all countries of the world. The type of card, its function, and its integrity vary enormously. While a majority of countries have official, compulsory, national IDís that are used for a variety of purposes, many developed countries do not have such a card. Amongst these are the United States, Canada, New Zealand, Australia, the United Kingdom, Ireland, and the Nordic countries. Those that do have such a card include Germany, France, Belgium, Greece, Luxembourg, Portugal and Spain.

ID cards are established for a variety of reasons. Race, politics and religion were often at the heart of older ID systems. The threat of insurgents, religious discrimination or political extremism have been all too common as motivation for the establishment of ID systems which would force enemies of the State into registration, or make them vulnerable in the open without proper documents. In Pakistan, the cards are used to enforce a quota system.

³³ Opinion 1/98: Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS). <<http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp11en.htm>>.

In recent years, ID cards have been linked to national registration systems, which in turn form the basis of government administration. In such systems - for example Spain, Portugal, Thailand and Singapore - the ID card becomes merely one visible component of a much larger system.

With the advent of magnetic stripes and microprocessor technology, these cards can also become an interface for receipt of government services. Thus, the cards become a fusion of a service technology, and a means of identification. At the heart of such plans is a parallel increase in police powers. Even in democratic nations, police retain the right to demand ID on pain of detention.

In a number of countries, these systems have been successfully challenged on constitutional privacy grounds. In 1998, the Philippine Supreme Court ruled that a national ID system violated the constitutional right to privacy. In 1991, the Hungarian Constitutional Court ruled that a law creating a multi-use personal identification number violated the constitutional right of privacy.³⁴

Biometrics

Biometrics is the process of collecting, processing and storing details of a person's physical characteristics for the purpose of identification and authentication. The most popular forms of biometric ID are retina scans, hand geometry, thumb scans, finger prints, voice recognition, and digitized (electronically stored) photographs. The technology has gained the interest of governments and companies because unlike other forms of ID such as cards or papers, it has the capacity to accurately and intimately identify the target subject.

Biometrics schemes are being implemented across the world. Spain has commenced a national fingerprint system for unemployment benefit and healthcare entitlement. Russia has announced plans for a national electronic fingerprint system for banks. Jamaicans are required to scan their thumbs into a database before qualifying to vote at elections. In France and Germany, tests are under way with equipment that puts fingerprint information onto credit cards. The technology is being used in retail outlets, government agencies, child care centres, police forces and automated-teller machines.

An automated immigration system developed by the U.S. Immigration and Naturalization Service (INS) uses hand geometry. In this project, frequent travellers have their hand geometry stored in a "smart" computer chip card. The traveller places a hand onto a scanner, and places the card into a slot. More than 70,000 people have enrolled in the trial. The scheme may ultimately result in a worldwide identification system for travellers.

³⁴ Constitutional Court Decision No. 15-AB of 13 April 1991.
<http://www.privacy.org/pi/countries/hungary/hungarian_id_decision_1991.html>.

The most controversial form of biometrics - DNA identification - is benefiting from new scanning technology which can automatically match DNA samples against a large database in minutes. Police forces in several countries such as the United States, Germany and Canada are creating national databases of DNA. In the United Kingdom and the U.S., police have been demanding that all individuals in a particular area voluntarily provide samples or face being placed under scrutiny as a suspect.

Surveillance of Communications

Nearly all countries have established some form of wiretapping capability over telephone, fax and telex communications. In most cases, these intercepts are initiated and authorized by law enforcement agencies. Wiretapping abuses have been detected in most countries, sometimes occurring on a vast scale involving thousands of illegal taps. The abuses invariably affect anyone "of interest" to a government. Targets include political opponents, student leaders and human rights workers.³⁵

Law enforcement agencies have traditionally worked closely with telecommunications companies to formulate arrangements that would make phone systems "wiretap friendly." Such arrangements range from allowing police physical access to telephone exchanges, to installing equipment to automate the interception.

The U.S. has led a worldwide effort to limit individual privacy and enhance the capability of its police and intelligence services to eavesdrop on personal conversations. The campaign has had two legal strategies. The first made it mandatory for all digital telephone switches, cellular and satellite phones and all developing communication technologies to build in surveillance capabilities; the second sought to limit the dissemination of software that provides encryption, a technique which allows people to scramble their communications and files to prevent others from reading them.³⁶

At the same time, the United States has taken a lead in promoting greater use of electronic surveillance and the weakening of bank secrecy laws. FBI Director Louis Freeh has traveled extensively around the world, promoting the use of wiretapping in newly free countries such as Hungary and the Czech Republic.

Internet and email interception

Over the past decade the Internet has become an important tool for communication and research. The technology is growing at an exponential rate, with millions of new users going on line each year. The Internet is also used increasingly as a tool for commercial transactions. The capacity, capability, speed and reliability of the Internet is constantly

³⁵ U.S. Department of State Singapore Country Report on Human Rights Practices for 1997, January 30, 1998.

³⁶ James Bamford, *The Puzzle Palace*, Penguin Books, 1981.

improving, resulting in the constant development of new uses for the medium.

But this fluid structure has not protected the Internet from interception and control by authorities. Because the medium is new, it often lacks the protections found in conventional telephone systems. Law enforcement and national security agencies throughout the world have moved swiftly to establish default capabilities to intercept and analyze email and Internet traffic. Law enforcement agencies in the United Kingdom have argued that interception of email traffic should be permissible through agreements between police and Internet Service Providers (ISPs), the conduits for Internet traffic. The move has caused alarm, with rights groups demanding that email interception should not be treated differently than telephone interception. In Singapore, all ISPs are operated by government-controlled or related organizations and reportedly provide information on a regular basis to government agencies. In Russia, a proposal that all ISPs place a black box and high-speed link connected to the Federal Security Service is currently being debated.

"Anonymous remailers," which strip identifying information from emails, can stop traffic analysis. They are the Internet equivalent of PO Box addresses. They have also generated opposition from police and intelligence services. In Finland, a popular anonymous remailer had to be shut down due to legal challenges that forced the operator to reveal the name of one of the users.

Encryption has become the most important tool for protection against surveillance. A message is scrambled so that only the intended recipient will be able to unscramble, and subsequently read, the contents. Pretty Good Privacy (PGP) is the best-known encryption program and has over 100,000 users, including human rights groups such as Amnesty International.

The recording of information about specific Internet activities has become one of the biggest emerging threats to Internet privacy. Every time a user accesses a web page, the server holding the page logs the user's Internet address along with the time and date. Some sites place "cookies" on a user's machine to help track people's activities at a much more detailed level. Others ask for the user's name, address and other personal details before allowing access. Internet purchases are similarly recorded. On-line stores value such data very highly, not least for the potential to sell the data on to marketers and other organizations.

Some technical solutions have been devised to counter such activities. "Anonymising" software allows users to browse the Web without revealing their Internet address. "Cookie cutter" programs stop sites from putting cookies on a user's machine, and are now built into most browsers. Anonymous digital cash lets consumers make payments without revealing their identity.

National Security and the ECHELON system

Immediately following the Second World War, in 1947, the governments of the United States, the United Kingdom, Canada, Australia and New Zealand signed a National Security pact known as the "Quadrupartite," or "United Kingdom - United States" (UKUSA) agreement. Its intention was to seal an intelligence bond in which a common National Security objective was created. Under the terms of the agreement, the five nations carved up the earth into five spheres of influence, and each country was assigned particular targets. The UKUSA Agreement standardized terminology, code words, intercept handling procedures, arrangements for cooperation, sharing of information, and access to facilities. One important component of the agreement was the exchange of data and personnel. The link means that operatives from the New Zealand signals intelligence agency GCSO could work from the Canberra facilities of Australia's Defense Signals Directorate to intercept local communications, and pass on the contents to the Australian intelligence agencies without either nation having to formally approve or disclose the interception.

The strongest alliance within the UKUSA relationship is the one between the U.S. National Security Agency (NSA) and Britain's Government Communications Headquarters (GCHQ). The most important facility in the alliance is Menwith Hill, in the north of England. With two dozen radomes and a vast computer operations facility, the base has the capacity to eavesdrop on vast chunks of the communications spectrum. With the creation of Intelsat and digital telecommunications, Menwith and other stations developed the capability to eavesdrop on an extensive scale on fax, telex and voice messages. It is widely believed that Menwith Hill has around 40,000 lines connected to it, through which access could be gained to too much of European and Soviet communications.

A report published in late 1997 by the European Parliament has confirmed that "Project Echelon" gives the NSA the ability to search nearly all data communications for "key words." Messages are not currently analyzed for overall content, nor is the scanning done in real time, but daily reports provide "precursor" data which assists intelligence agencies determine targets. Automatic scanning of voice communications may not be far behind.

A voice recognition system called "Oratory" has been used for some years to intercept and analyze diplomatic phone calls³⁷. The report - "Assessing the Technologies of Political Control" - states, "Within Europe all email telephone and fax communications are routinely intercepted by the United States National Security Agency transferring all target information from the European mainland via the strategic hub of London then by satellite to

³⁷ European Parliament, Scientific and Technological Options Assessment (STOA), An Appraisal of Technologies of Political Control, 6 January 1998. <<http://jya.com/stoa-atpc.htm>>.

Fort Meade in Maryland via the crucial hub at Menwith Hill in the North York moors in the UK." The report sparked a wave of concern in Europe which led on September 14, 1998, to a debate in the European Parliament. A "compromise resolution" framed that day by the four major parties called for greater accountability and "protective measures" over the activities of security agencies.

Video Surveillance

In recent years, the use of video surveillance cameras (also called Closed Circuit Television, or CCTV) throughout the world has grown to unprecedented levels. In the UK alone, between 150 and 300 million pounds per year is now spent on a surveillance industry involving an estimated 200,000 cameras monitoring public spaces³⁸. Most towns and cities are moving to CCTV surveillance of public areas, housing estates, car parks and public facilities. Growth in the market is estimated at fifteen to twenty per cent annually. Many Central Business Districts in Britain are now covered by surveillance camera systems involving a linked system of cameras with full pan, tilt, zoom and infrared capacity. Their use on private property is also becoming popular.

These systems involve sophisticated technology. Features include night vision, computer assisted operation, and motion detection facilities which allow the operator to instruct the system to go on red alert when anything moves in view of the cameras. Camera systems increasingly employ bullet-proof casing, and automated self defense mechanisms. The clarity of the pictures is usually excellent, with many systems being able to read a cigarette packet at a hundred meters. The systems can often work in pitch blackness, bringing images up to daylight level. The technology will ultimately converge with sophisticated software programs that are capable of automated recognition of faces, crowd behavior analysis, and (in certain environments) intimate scanning of the area between skin surface and clothes. The power and capabilities of cameras will continually increase, while the cost and size will decrease. It is reasonable to assume that covert visual surveillance will in some environments be ubiquitous.

The CCTV trend is not confined to Britain. Sweden - once strongly opposed to such surveillance - is considering relaxing its privacy laws to permit public surveillance, while CCTV activity in Norway has prompted specific inclusion of such surveillance in the data protection act. Meanwhile, CCTV activity has grown markedly in North America and Australia to monitor public squares. In Singapore, they are widely employed for traffic enforcement and to prevent littering.

³⁸ House of Lords, Science and Technology Committee, Fifth report, "Digital images as evidence", 3 February 1998, London.

Some observers believe this phenomenon is dramatically changing the nature of cities. The technology has been described as the "fifth utility." CCTV is being integrated into the urban environment in much the same way as the electricity supply and the telephone network in the first half of the century. CCTV is profoundly changing the nature of the urban environment, and is now an important part of the core management of cities. Visual surveillance is becoming a fixed component in the design of modern urban centers, new housing areas, public buildings and even the road system. CCTV images may in the future be viewed as just one more type of necessary data, and considered a "value added" product.

Workplace surveillance

Employees in nearly every country are vulnerable to comprehensive surveillance by managers. Legal protections are generally laxer in such circumstances because surveillance is frequently imposed as a condition of employment. In many countries employers can tap phones, read email and monitor computer screens. They can bug conversations, analyze computer and keyboard work, peer through CCTV cameras, use tracking technology to monitor personal movements, analyze urine to detect drug use, and demand the disclosure of intimate personal data.

The technology being used to monitor workers is extremely powerful. It can analyze "keystrokes" on a terminal to determine whether employees are making efficient use of their time between telephone conversations. Software companies call this process "performance monitoring." Even in workplaces staffed by highly skilled information technology specialists, bosses demand the right to spy on every detail of a worker's performance. Modern networked systems can interrogate computers to determine which software is being run, how often, and in what manner. A comprehensive audit trail gives managers a profile of each user, and a panorama of how the workers are interacting with their machines. The software also gives managers total central control over the software on each individual PC. A manager can now remotely modify or suspend programs on any machine.

The technology being used extends to every aspect of a worker's life. Miniature cameras monitor behavior. "Smart" ID badges track an employee's movement around a building. Telephone Management Systems (TMS) analyze the pattern of telephone use and the destination of calls. Psychological tests, general intelligence tests, aptitude tests, performance tests, vocational interest tests, personality tests and honesty tests are all electronically assessed. Surveillance and monitoring have become design components of modern information systems.

While companies assert that all surveillance is justified, it is clear that not all uses of monitoring are legitimate. Following some organizing activity by a local union, one U.S. employer installed video cameras to monitor each individual workstation and worker.

Although management claimed that the technology was being established solely for safety monitoring, two employees were suspended for leaving their workstations to visit the toilet without permission. According to a 1993 report of the International Labour Office, the activities of union representatives on the floor was also inhibited by a "chilling effect" on workers who knew their conversations were being monitored.

A spate of well publicized cases of similar abuses of visual surveillance has prompted concern in the workplace. A 1991 survey of employees throughout the U.S. revealed that 62 per cent disagreed with the use of video surveillance (including 38 per cent who "strongly disagreed"). Nevertheless, a recent report by the American Management Association revealed that two thirds of American boss's spy on their workers, often through email and phone interception³⁹.

In a report entitled *Job Stress: The 20th Century Disease*, the ILO "points to growing evidence of problems around the world, including developing countries, where corporations are doing little to help employees cope with the strain of modern industrialization." The report also says that "[a] the use of computers spreads throughout the world, workers in many countries are being subjected to new pressures, including electronic eavesdropping by superiors. . ." A 1990 survey of telecommunications workers sponsored in part by the Communications Workers of America revealed that 84 percent of monitored employees complained about high tension as opposed to 67 percent of unmonitored workers. A later study by the U.S. Office of Technology Assessment also found that workplace monitoring "contributes to stress and stress-related illness."⁴⁰

In Britain and the United States, there are few legal constraints on video surveillance, unlike.

the laws of Austria, Germany, Norway and Sweden, under which employers are obliged to seek agreement with workers on such matters.

This situation has been challenged in the European Court of Human Rights. Former British Assistant Chief Constable Allison Halford had complained that following her sex discrimination complaint against the police, her office phone had been bugged. While the British government asserted that this was an entirely lawful and proper activity, Halford maintained that it breached the right of privacy contained in the European Convention on Human Rights. The court agreed, and ruled that the police had acted improperly in bugging Ms Halford's phone⁴¹.

³⁹ American Management Association, *Report on Electronic Monitoring & Surveillance*, 1997.
<<http://www.amanet.org/survey/elec97.htm>>.

⁴⁰ Office of Technology Assessment, *New Technology, New Tensions*, September 1987.

⁴¹ *Halford v. United Kingdom* (Application No 20605/92), 24 EHRR 523, 25 June 1997.

The practice is likely to breach laws which form in the wake of the European Telecommunications Directive. Currently, however, the court's decision appears to do little more than oblige bosses to notify workers that they should have no expectation of privacy on the phone. And accordingly, most businesses are moving to routine monitoring of phone calls.

Location Data, Public Order and Control

When fighting a large-scale crisis such as a pandemic it is important for governments to understand why a threat is emerging, how the threat scenario develops, and whether the general population complies with measures for containment. Governments and research institutions need data to develop insights on these aspects, with location data being particularly attractive as work in the humanitarian sector has shown for many years by now.

When it comes to the use of location data sourced through mobile communication infrastructure and location services specifically, many commentators have been surprised by the fact that the government of the People's Republic of China (PRC) co-developed a mobile phone application informing users whether they have been in close contact with someone infected by COVID-19 (China Launches Coronavirus 'close Contact' App 2020). The insights presented by this app are based on the analysis of location data collected through phone networks, WiFi connections, satellite-based radio navigation system (e.g. GPS, GLONASS, Galileo) and other surveillance assemblages producing data that reveal the location of individuals and crowds. Furthermore, apps with maps to track the disease also became popular very quickly in Hong Kong (Latest Situation of Novel Coronavirus Infection in Hong Kong n.d.), and South Korea (Coronavirus Mobile Apps Are Surging in popularity in South Korea - CNN n.d.). In the PRC, this approach seems to have evolved into the 'Alipay Health Code', a system that classifies residents based on an opaque methodology (Mozur et al. 2020).

Once a survey has been filled out by a user, this data gets combined with other sources such as location data. Once the data has been analysed, a QR code is generated which has one of three colours; green enables its bearer to unrestricted movement, the 'owner' of a yellow code may be asked to stay home for 7 days, and a red QR code results in two-weeks of quarantine.

In the meanwhile, the US government is in active talks with several large technology corporations such as Google and Facebook to explore venues how location data could be used to combat the pandemic, including tracking whether people are keeping one another at safe distances to counter the spread of the virus (Romm et al. n.d.). Google has already used the pandemic to show some of the advantages of omnipresent location tracking (Google Is Now Publishing Coronavirus Mobility Reports, Feeding off Users' Location History n.d.).

Finally, surveillance corporations such as Athena Security and the infamous spyware firm NSO advertise specialized surveillance cameras and dedicated data analysis services using location data to track the spread of the disease based on the movement of individuals and groups (Cox 2020; Israel Spyware Firm NSO Wants to Track and Stop Coronavirus Bloomberg n.d.).

Human Rights and Data Protection

Right now, the temptation is very strong to do “whatever is necessary” (Sevastopulo et al. 2020). Undoubtedly, in times of crisis there is an increased need for governments to monitor and control the public, which might make it necessary to limit individual freedom. Such decisionism characterizes many emergencies. Constitutions and human rights, however, are designed with such crises in mind. Furthermore, the International Covenant on Civil and Political Rights (ICCPR) and on the European level the European Convention on Human Rights (ECHR), are prepared to deal with such situations. Considering such developments from a formal perspective, it is useful to take a look at the legal and institutional framework of the Council of Europe (CoE). This international organization administers and controls one of the most important international human rights treaties guaranteeing individual freedoms, the European Convention on Human Rights (ECHR).

The CoE has established procedures and case-law for times of crisis like the current one (Mokhtar 2004)⁴².

The guide on Article 15 ECHR for derogations in times of emergency has been updated recently on 31 December 2019 (Council of Europe/European Court of Human Rights 2019). States may derogate in situations of:

- war or other public emergency threatening the life of the nation,
- taking measures which are strictly required by the exigencies of the situation,
- and provided that measures are not inconsistent with other obligations under international law.

Furthermore, Article 4 of the ICCPR is similarly worded and beyond that requires state parties to report to all other parties via the UN Secretariat. Certain rights such as the right to life (except in respect of deaths resulting from lawful acts of war), the prohibition of torture and other forms of ill-treatment, the prohibition of slavery or servitude, and the rule of no punishment without law are non-derogable. However, many other rights are subject to derogation, including particularly the right to privacy, freedom of expression, the freedom of movement, as well as the freedom of assembly and association. Such derogations may only

⁴² Ali A, Qadir J, ur Rasool R, Sathiaselalan A, Zwitter A, Crowcroft J (2016) Big data for development: applications and techniques. *Big Data Anal* 1(1):124. <https://doi.org/10.1186/s41044-016-0002-4>

be of temporary nature (Zwitter 2012). Both of these legal frameworks allow states for some flexibility by enabling them to temporarily derogate from some rights⁴³.

Data protection and privacy are human rights that can be derogated from during crisis. They can be temporarily reduced when a public emergency calls for it. What makes this situation even more complicated is the use of data from and by corporate agencies. Only mentioning the issue of over-dominant corporate power in the form of surveillance capitalism briefly (Zuboff 2019), data ownership is in principle a matter of contract law and in many cases a question of terms of use that customers have to accept by default when intending to use a service. Particularly now, private corporations hold the key to using Big Data for tackling the corona crisis. Furthermore, typical data protection frameworks such as the EU General Data Protection Regulation (GDPR) are focused on individual rights and individual consent. Hence, they leave out many aspects of collective autonomy as outlined below. In summary, standard data protection regimes and human rights law provide little protection for privacy and responsible data use during times of emergency.

Potential Concerns

Over the last years much has been written about the balance between security and individual freedom, particularly on the false trade-off between privacy and security (Solove 2011). While a pandemic such as the spread of COVID-19 requires comprehensive measures, we must keep in mind that the use of location data and other (potentially) personally or demographically identifiable data on such scale results in the production of a 'data exhaust' that invariably has consequences. Just because it might be an emergency, does not mean that everything goes⁴⁴.

The arguably under-considered use of location data is surprising at this point when thinking about the unintentional revelation of the location and features of US military bases through the usage of the fitness app 'Strava' by members of the forces (Liptak 2018), or recent work of the New York Times based on the analysis of a comprehensive set of pseudonymized mobile phone records that allowed to identify several prominent and influential individuals upon closer scrutiny (Thompson and Warzel 2019)⁴⁵. No executive powers enshrined in regulatory frameworks were necessary to acquire these datasets and carry out the analysis, which in itself shows that our societies lack appropriate governance frameworks for such practices. Not only effective oversight on the use of such data is missing, it is also open how individuals would be safeguarded against abuse, and which kind of remedies they could use

⁴³ Baharudin, Hariz, and Lester Wong (2020) "*Coronavirus: Singapore app allows for faster contact tracing*". Text. The Straits Times. <https://www.straitstimes.com/tech/singapore-app-allows-for-faster-contact-tracing>

⁴⁴ Boyd D, Crawford K (2012) Critical questions for big data. Inf Commun Soc 15(5):662679. <https://doi.org/10.1080/1369118X.2012.678878>

⁴⁵ Cannataci J (2017) Report of the special rapporteur on the right to privacy. Office of the High Commissioner for Human Rights, Geneva

to defend themselves. Considering this misuse of location data, the Federal Communications Commission in the US on 28 February 2020 proposed a fine of 200 million dollars for mobile phone network operators repackaging and reselling location data (FCC Proposes Over \$200M in Fines for Wireless Location Data Violations 2020).

Furthermore, research over the past years has proven again and again that the combination of the production of unprecedented amounts of data and improving techniques to analyse large data sets are rendering most if not all state of the art practices to pseudonymize/anonymize datasets meaningless, at least as time moves on (Rocher et al. 2019). The United Nations Special Rapporteur on the right to privacy has rightfully highlighted the risks resulting from the combination of 'closed' datasets with 'open' ones (Cannataci 2017)⁴⁶. In our work on Mobile devices as stigmatizing security sensors we have proposed the concept of 'technological gentrification' which describes our lives in environments that are permanently monitored and where those believing in the benefits of omnipresent data render the choices of others de-facto obsolete (Gstrein and van Eck 2018).

While a crisis like the coronavirus pandemic requires dedicated, quick and effective measures we must not forget that data is contextual. One and the same dataset can be sensitive in different contexts, and we need appropriate governance frameworks to make sure that this data is being generated, analysed, stored and shared in legitimate and responsible ways. In light of the COVID-19 pandemic location data might be very useful for epidemiological analysis. In the context of a political crisis, the same location data can threaten the rule of law, democracy and the enjoyment of human rights.

Luckily, some authorities across the world have already reacted to the potential threats resulting from the use of location data in order to tackle the current pandemic (Data Protection Law and the COVID-19 Outbreak n.d.). On 16 March 2020 the European Data Protection Board released a statement in which chair Andrea Jelinek underlines that “even in these exceptional times, the data controller must ensure the protection of the personal data of the data subjects (Olbrechts 2020). Therefore, a number of considerations should be taken into account to guarantee the lawful processing of personal data.”

While these efforts are commendable, it would be preferable to have dedicated legal frameworks, created through democratic processes in parliaments, as well as transparent policies. Given the necessity to act quickly, one might at least expect governmental decrees or executive acts describing the means, objectives and undertaken practices in a detailed manner, rooted in proper legal basis and competences, including the establishment of oversight mechanisms. Instead, the current picture suggests that ad-hoc practices have to be justified by independent data protection authorities which have to compromise their long-

⁴⁶ Chandler D (2015) A world without causation: big data and the coming of age of posthumanism. *Int Stud* 43(3):119

term supervisory objectives for short-term support of the greater good.

Humanitarian Guidelines for Data Responsibility

Because of the lack of legal guidance in many instances, it is important to resort to best practices established in different fields, particularly in the domain of humanitarian action. Over the past decades the humanitarian community has developed extensive expertise on how to deal with data during crisis responsibly. One core player in this field is the United Nations' Office for the Coordination of Humanitarian Affairs (OCHA)⁴⁷. Its Centre for Humanitarian Data worked - together with many experts - on detailed guidance notes that help to deal with data responsibly (Data Policy The Centre for Humanitarian Data n.d.). This particularly concerns best practices in the cooperation between humanitarian, corporate and governmental stakeholders.

The International Committee of the Red Cross and Red Crescent published a detailed handbook on data protection in humanitarian action (Kuner and Marelli 2017). This handbook covers everything from basic data protection principles, to questions of data sharing and data protection impact assessments (DPIA) in humanitarian contexts. Furthermore, Part II covers specific scenarios and data collection methods such as the use of mobile apps, biometrics and cloud services. These guidelines cover largely the same aspects as the OCHA guidelines. These concern particularly the fair data processing of vulnerable data subjects, data minimization as well as data retention and deletion.

Principles of Data Protection in Humanitarian Studies

At this stage it should be emphasized that the academic community has not been idle. A discussion surrounding data ethics has been held quite vigorous over past years. It ranges from questions surrounding the use of “public data” (e.g. social media data), to biases, and includes considerations on nudging (Boyd and Crawford 2012; Zwitter 2014; Zimmer 2010; Chandler 2015). Experts in the field of humanitarian action, innovation governance and data protection have published extensively on utilities and risks of the use of 'big crisis data'. (Latif et al. 2019) A specific use-case has been the domain of crisis mapping, with Ushahidi and Humanitarian OpenStreetMap launching these developments early on (Ziemke 2012)⁴⁸.

Of particular note in the past years has been the Signal Code of the Harvard Humanitarian Initiative (Greenwood et al. 2017). Its purpose is identification, definition and articulation of International Human Rights standards with regards to data and ICTs, as well as their translation into the humanitarian context. Like the principles of the 510 Data

⁴⁷ Checa D, Bustillo A (2020) Advantages and limits of virtual reality in learning processes: Briviesca in the fifteenth century. *Virtual Real* 24(1):151161. <https://doi.org/10.1007/s10055-019-00389-7>

⁴⁸ China Launches Coronavirus 'close Contact' App. BBC News. (2020) sec. Technology. <https://www.bbc.com/news/technology-51439401>

Responsibility, the Signal Code identifies a set of rights held by all data subjects including the protection of DII.

Some specific aspects of the Signal Code should be highlighted: *The right to information* refers to the right of all people to generate, access, acquire, transmit, and benefit from information during a crisis.

The right to protection concerns protection from all harms that can arise from the misuse and unintended consequences of data and ICTs, given that crisis-affected populations are particularly vulnerable⁴⁹. *Privacy and security* as a right refer to internationally recognised legal, ethical and technical standards of data protection and privacy. The right to data agency relates to individual and collective agency with regards to collection, use and disclosure of PII and DII. Finally, *rectification and redress* of data is also a remedy that pertains to groups and individuals. A key element in all these points is not only the abstract existence and observance of these rights, but to enable effective application procedures for individuals and populations affected by crises. In other words, it obliges humanitarians to establish procedures to give effect to these rights and potential claims of affected people.

Eventually, profound questions around the meaningfulness of concepts such as individual consent and the nature of effective pseudonymization and anonymization remain. Unfortunately, it goes beyond the scope of this short piece to explore these in detail, but considerations on 'group privacy' and informational self-determination in the digital age would be potential starting points for such in-depth discussion (Lu et al. 2012; Raymond 2017b; Taylor et al. 2017). It needs to be reiterated that the humanitarian field is working on this subject extensively and with a mindset that is focused on using data responsibly, instead of mere compliance with regulatory frameworks, which need to resort to abstract human rights provisions too quickly since these frameworks themselves are limited in scope and application. Hopefully, this gap can be filled quickly in order to be able to fully focus on the containment of the pandemic, instead of additionally creating worries around the responsible use of data⁵⁰.

Threats to Privacy

The increasing sophistication of information technology with its capacity to collect, analyze and disseminate information on individuals has introduced a sense of urgency to the demand for legislation. Furthermore, new developments in medical research and care, telecommunications, advanced transportation systems and financial transfers have dramatically increased the level of information generated by each individual. Computers

⁴⁹ Coronavirus Mobile Apps Are Surging in Popularity in South Korea - CNN (n.d.) <https://edition.cnn.com/2020/02/28/tech/korea-coronavirus-tracking-apps/index.html>. Accessed 30 Mar 2020

⁵⁰ Council of Europe/European Court of Human Rights (2019) Guide on article 15 of the European Convention on Human Rights. https://www.echr.coe.int/Documents/Guide_Art_15_ENG.pdf.

linked together by high-speed networks with advanced processing systems can create comprehensive dossiers on any person without the need for a single central computer system.

New technologies developed by the defense industry are spreading into law enforcement, civilian agencies, and private companies⁵¹.

According to opinion polls, concern over privacy violations is now greater than at any time in recent history⁵². Uniformly, populations throughout the world express fears about encroachment on privacy, prompting an unprecedented number of nations to pass laws which specifically protect the privacy of their citizens. Human rights groups are concerned that much of this technology is being exported to developing countries which lack adequate protections. Currently, there are few barriers to the trade in surveillance technologies.

It is now common wisdom that the power, capacity and speed of information technology is accelerating rapidly. The extent of privacy invasion - or certainly the potential to invade privacy - increases correspondingly.

Beyond these obvious aspects of capacity and cost, there are a number of important trends that contribute to privacy invasion:

GLOBALISATION removes geographical limitations to the flow of data. The development of the Internet is perhaps the best-known example of a global technology.

CONVERGENCE is leading to the elimination of technological barriers between systems. Modern information systems are increasingly interoperable with other systems, and can mutually exchange and process different forms of data.

MULTI-MEDIA fuses many forms of transmission and expression of data and images so that information gathered in a certain form can be easily translated into other forms.

Technology transfer and policy convergence

The macro-trends outlined above have had particular effect on surveillance in developing nations. In the field of information and communications technology, the speed of policy convergence is compressed. Across the surveillance spectrum - wiretapping, personal ID systems, data mining, censorship or encryption controls -- it is the West which invariably sets a proscriptive pace⁵³.

Governments of developing nations rely on first world countries to supply them with technologies of surveillance such as digital wiretapping equipment, deciphering equipment,

⁵¹ Data Policy The Centre for Humanitarian Data (n.d.) <https://centre.humdata.org/data-policy/>. Accessed 30 Mar 2020

⁵² Simon Davies "Re-engineering the right to privacy: how privacy has been transformed from a right to a commodity", in Agre and Rotenberg (ed) "Technology and Privacy: the new landscape", MIT Press, 1997 p.143.

scanners, bugs, tracking equipment and computer intercept systems. The transfer of surveillance technology from first to third world is now a lucrative sideline for the arms industry⁵⁴.

According to a 1997 report "Assessing the Technologies of Political Control" commissioned by the European Parliament's Civil Liberties Committee and undertaken by the European Commission's Science and Technology Options Assessment office (STOA)⁵⁵, much of this technology is used to track the activities of dissidents, human rights activists, journalists, student leaders, minorities, trade union leaders, and political opponents. The report concludes that such technologies (which it describes as "new surveillance technology") can exert a powerful 'chill effect' on those who "might wish to take a dissenting view and few will risk exercising their right to democratic protest". Large scale ID systems are also useful for monitoring larger sectors of the population. As Privacy International observed, "In the absence of meaningful legal or constitutional protections, such technology is inimical to democratic reform. It can certainly prove fatal to anyone 'of interest' to a regime."

Government and citizen alike may benefit from the plethora of IT schemes being implemented by the private and public sectors. New "smart card" projects in which client information is placed on a chip in a card may streamline complex transactions. The Internet will revolutionize access to basic information on government services. Encryption can provide security and privacy for all parties.

However, these initiatives will require a bold, forward looking legislative framework. Whether governments can deliver this framework will depend on their willingness to listen to the pulse of the emerging global digital economy and to recognize the need for strong protection of privacy.

Conclusion

After introspecting the above discussion about informational privacy, it appears that the right to life and liberty guaranteed under article 21 of Indian Constitution which protects an individual against both state and non-state actors can very well accommodate informational privacy. The advancement in technology helps in generating databases related to individuals, wherein ideally it is the individual who should be in-charge of it, but unfortunately, he is not.

The presence of technology helps to make information about an individual's private life available to others and tends to influence and even to injure the very core of an

⁵³ Simon Davies and Ian Hosein, *"Liberty on the Line"* in Liberating Cyberspace, Pluto Press, London, 1998.

⁵⁴ Big Brother Incorporated, Privacy International site: <<http://www.privacy.org/pi/reports/>>.

⁵⁵ Published by Science and Technology Options Assessment (STOA). Ref: project no. IV/STOA/RSCH/LP/politicon.1

individual's personality i.e., his informational privacy. The current Indian regulatory framework on informational privacy and data protection is not sufficiently adequate to address the growing concerns arising on account of collection, leaking and linking of data. Certainly, there is a need for comprehensive legislation which can deal with various types of privacy and its related issues. Once the Data Protection bill, 2019 gets enacted, we can expect that the media privacy will be regulated carefully in the coming future. As the technology grows at an unimaginable speed, further research on concerns related to protection and regulation of informational privacy is certainly the need of an hour.

DEVELOPMENT OF RIGHT TO PRIVACY AS A HUMAN RIGHT: AN EXCURSION FROM ANCIENT TO DIGITAL INDIA

Prof. (Dr.) Mohammad Tariq & Shelja Singh***

Abstract

Right to privacy is an elementary human right assured by several international conventions and treaties. It is imperative for safeguarding human dignity and is one of the fundamental pillars of a democratic nation. The concept of privacy was entrenched in the rich cultural heritage and social structure of our country. The term has been found in the work of various eminent Indian scholars and other ancient texts. Owing to creative judicial interpretation, in India, it has now acquired a form of Fundamental Right under the aegis of Article 21. This research paper endeavours to find out the inception of right to privacy as a Human Right in affluent heritage of primordial India. It makes an attempt to locate the path which the Right to Privacy as a human right has travelled from ancient to digital era. It also seeks to search the legislative measures concerning privacy and the contribution of judiciary in firmly establishing the Right to Privacy as a Fundamental Right in India. This paper is also an attempt to point out the challenges in the exercise of the Right to Privacy in this modern digital age and the possible solutions for the same.

Keywords: *Privacy, Human Right, Constitution, digital, judiciary*

Introduction

The origin of Right to Privacy in the human society can be traced back from the primitive human society, gradually it passes through the age of transformation of primitive society to modern human society and finally, it has reached the history of privacy in the modern human society¹. The process of development of this right from the primitive society to the modern society has been understood, at the first instance, about the western societies. Actually, it was present in the primitive human societies in every part of the world, both western and eastern². But, the Eastern scholars have not taken such initiatives at the beginning, like the Western scholars to find out the origin and history of this right in the form

* Professor, Department of Law, A. M. U (A Central University) Aligarh (U.P.) E-mail: tariqmtariq@gmail.com

** Research Scholar, Department of Law, A. M. U (A Central University) Aligarh, Email:sheljasingh2607@gmail.com.

¹ Sargam Thapa, *The Evolution of Right to Privacy in India* 10 INT'L J. HUM. & SOC'L SEC. INV'N 53, 54 (2021). Available at: [https://www.ijhssi.org/papers/vol10\(2\)/Ser-1/J1002015358.pdf](https://www.ijhssi.org/papers/vol10(2)/Ser-1/J1002015358.pdf). (last accessed on January 1, 2022).

² *Ibid.*

of a human right in the Eastern world. Due to this reason, most part of the evidences of origin and history of this right in the Eastern society has been lost. India is not an exception to this general situation³. In ancient India, various basic rights including privacy were granted to all humans irrespective of their status, gender or nationality which are now termed as human rights by the western world which takes the credit to originate them. Right to Privacy has been originated in India since the very old period, existed here in the ancient period, lost in the medieval period and revived in the modern period. Therefore, Right to Privacy had been and is very much present in the Indian society. Next part of the study will concentrate on the origin and history of this right in India⁴.

Right to Privacy in Ancient India

Privacy was embedded in the Indian cultural heritage and Indian social structure, as such; it was not alien to India. Various Indian scholars, Eminent writers, *Smritikaras*, commentators and the authors of different epics had defined the term 'Privacy' in their writings⁵.

The Origin of Privacy in the Vedas and Upanishads

Vedas were the first scriptures of ancient Indian society, which propounded the religious as well as legal injunctions. *Upanishads* were created for the analysis and interpretation of the Vedas. Besides Upanishad and other religious texts, Vedas were also concerned with the rules relating to Privacy in ancient India⁶. It was found that, any kind of disturbance or interference was prohibited in matters of religious or spiritual activities. Privacy was always prescribed in these cases.

Privacy was also required to be exercised at the time of the study of Vedas⁷. In this respect, the necessity and consciousness of right of privacy in the primordial India was clearly expressed by a text of the Rig Veda, which is stated below:-

य आस्ते यश्च चरति यश्च पश्यति नो जनः । तेषां सं हन्मो अक्षाणि यथेदं हर्म्यं तथा ६⁸

(“One ought to build such house which may sustain and protect the inmates in all seasons and be comfortable. The passers-by may not see the inmates nor the inmates see them.”)

³ Ravindar Kumar and Gaurav Goyel, *The Right to Privacy in India: Concept and Evolution* 17 (Lightening Source Publishers 2016).

⁴ Rishika Taneja and Sidhant Kumar, *Privacy Law-principles, Injunctions And Compensation* 3 (eastern Book Company 2014).

⁵ Supra note 1.

⁶ <https://lawtimesjournal.in/privacy-as-a-fundamental-right/>. (last accessed on August 2, 2021).

⁷ E. Jeremy Hutton ET.AL., *The Right to Privacy in the United States, Great Britain and India*,” in RICHARD P. CLANDE (ED.), *Comparative Human Rights* 151 (Hopkins University Press 1976)

⁸ (*Rigveda, Mandal 7, Sukta 55, Hymn 6*)

This above-mentioned hymn of “*Rig Veda*” evidently depicts the subsistence of privacy both physical and psychological privacy at home including the existence of family privacy in ancient India. It also in other way, justifies the western view of “Every man's house is his castle” and its Indian counterpart “*Sarva Swa Swa Grihe Raja*”.

Privacy in the Grihya-Sutras

After the end of the Vedic Age, the period of Sutras came into being. There were various types of Sutras at that period. *Grihya-Sutra* was the prominent among them, which promulgated the rights and duties of a house holder in the family life. It contained detailed norms relating to construction of houses in the ancient India. These rules prescribed elaborate norms for preserving privacy at the time of construction of houses in ancient Indian social system¹⁰. The system of separate bed-room and nursery showed the need for privacy in the residential houses in the ancient period, which also reflected the modern psychiatric thoughts regarding the necessity of privacy in a house. Hence, the *Grihya-Sutras* were so advanced that, those can be called the forefather of the modern systems of privacy in the everyday life of human beings¹¹.

Privacy in the Great Epics

Apart from the Grihya-Sutras, elaborate rules regulating privacy in the Hindu period were found in the two Great Epics of India, the *Ramayana* and the *Mahabharata*. The following rules have been found in the Ramayana relating to privacy: The rule that a male stranger should not see a woman was commonly followed in the society as propounded by the Ramayana. Exceptions to this regulation were provided in this shloka, which would otherwise prove the rule:- “*Vyasaneshu na krichheshu na Yudhreshu swayangbare, Na kratton no vivahe va darshanang dushyate striyah*”

(“At the time of calamity, during physical and mental ailment, during war, in *Swayambar*, during performance of religious rites, during marriage ceremony, if a woman is seen by strangers, no wrong is said to have been committed.”)¹²

The next rule prescribed that no one should watch or hear any secret deliberation amid two persons and doing so was prohibited as a 'wrong' and 'capital punishment' was awarded therefore. The following text proves that rule:-

⁹ Justice M. Rama Joice, *Legal and Constitutional History of India: Ancient Legal, •Judicial And Constitutional System* 3 (universal 2004).

¹⁰ Dr. Ram Gopal, *India of Vedic Kalpasutras* https://archive.org/stream/in.ernet.dli.2015.54199/2015.54199.India-Of-Vedic-Kalpasutras-1959_djvu.txt. (last visited on January 2, 2022).

¹¹ Dr.V.M.Apte, *Social and Religious Life in the Grihya Sutras*, https://archive.org/stream/in.ernet.dli.2015.103973/2015.103973.Social-And-Religious-Life-In-The-Grihya-Sutras_djvu.txt. (last visited on January 2, 2022).

¹² (*Ramayana, Yuddha Kand*)

“Yah Shrinoti nireekshedra Savdhyo vavitataba, Vabeda vai muni mukhyasya vachanangyadyavekshase”

(“Regard being had to the words of the sage, let others know that anybody who will over hear our conversations or see us talking shall be killed.”)¹³

In this respect, it is also pertinent to mention that, this rule had received a prominent place in the period of Ramayana. It had universal application without any discrimination. As for example, The younger brother of Rama, Lakshmana violated the above rule for some unavoidable cause. In consequence, he was awarded the punishment by the royal committee headed by the sage Vasistha. Mahabharata was second great epic of India, which came into being after the Ramayana. It contained rules and regulations of every nature relating to human lives and as such, there was a number of rules regarding the Right to Privacy of human beings. Strangers were prohibited to enter into one's house at odd hours by a rule of the Mahabharata. The following text shows the existence of that rule:-

“Na vishravasajjata parasyagehang gachhennarashcheta yano vikale, Na chatvare nishi tishthe nnigurho na rajanyang yoshitang prarthayeeta”

(“One should not visit other's house at odd hours, one should not sit near a cross-road in the night and one should not try to make the King's wife his own.”)¹⁴

According to another rule of Mahabharata, confidentiality would be maintained within the relationship of husband and wife. The following text proves the existence of that rule:-

*“Tvatsyangnidhon yatkaretpatiste yadyapyaguhyang parirakshitavyam”*¹⁵

(“Even a casual conversation with your husband ought to be kept confidential.”)

Privacy in the *Manusmriti*

Manusmriti or the code of Manu was considered as a landmark in the ancient Indian legal history. It was compiled approximately at 200 B.C. The subject matter of Manusmriti was divided into 12 chapters and 2694 verses. it contained elaborate rules relating to every aspect of human lives during that period¹⁶. In this sense, it also contained a number of rules relating to Right to Privacy in ancient India. Killing of a sleeping person was prohibited. The following text clearly explains the rule: *“Na suptang na visannahang na nagnang na nirayudham, Nayuddhamanang pashyantang nap arena samagatam”*.

¹³ (Ramayana, Uttar Kand)

¹⁴ (Mahabharat, Udyog Parv)

¹⁵ (Mahabharat, Aranyak Parv)

¹⁶ Dr. Paras Diwan, *Modern Hindu Law* 33 (allahabad Law Agency 2007).

“One who is sleeping, one who is deprived of his shield, one who is naked, one who is without arms, one who does not participate in the battle and one who is busy fighting with another, should not be killed.”¹⁷

Privacy in the Kautilya's Arthashastra

Kautilya's Arthashastra was the most important and masterly treatise on statecraft of ancient India. The Prime Minister of Maghadha the time of Chandragupta Maurya, Chanakya or Vishnugupta was the author of this great work. It was called an encyclopaedia of statecraft and legal system of the ancient India. This famous work was created sometimes between 322 and 300 B.C.148. It had propounded elaborate rules relating to duties of king and procedures of administration of justice in ancient India. Kautilya realized the necessity of privacy in various spheres of human lives as well as in the administration of justice in the society. Therefore, he had prescribed various norms of Privacy in the Arthashastra¹⁸. Privacy of women was recognized and as such, the women working from home usually worked through the maid servants. More specifically protection was provided to female slaves. They could not be forced to attend their master, when bathing naked, hurting or abusing them or violating their chastity was also prohibited. In all these cases, forfeiture of the value paid for the slave was prescribed as punishment.

Obstructing the Privacy of others during sleeping, sitting, eating, and exercising was punishable. As the Privacy of the women was recognized, sexual intercourse with a woman without the consent and against the will was prohibited¹⁹. Even the Privacy of a Prostitute was recognized and forcing connection with a Prostitute was punishable. Apart from the above-mentioned provisions, Kautilya's Arthashastra had also prescribed Privacy of Information in different aspects of human lives. The following Sanskrit texts will provide the instances of such aspects of Privacy: “*Susiddha moushadhang dharmang grihachhidrangcha maithunam, Kuvuktang kushrutang chaiba matimanna prakashayet*”.

“(The medicine, effectiveness of which has been tested and proved, acts pertaining to religion, defects of one's family, sexual matters, eating prohibited food and hearing insulting words ought not to be made public)²⁰.”

Another rule states that: “*Aayurvitang grihachhidrang mantramoushadha maithune, Danang manapamanocha naba goupayani karyet*”

“(Informations pertaining to the following nine subjects, viz. (a) age, (b) wealth, (c)

¹⁷ Hargovind Shastri, Manusmriti, [rchive.org/stream/in.ernet.dli.2015.103973/2015.103973.Social-And-Religious-Life-In-The-Grihya-Sutras_djvu.txt](http://archive.org/stream/in.ernet.dli.2015.103973/2015.103973.Social-And-Religious-Life-In-The-Grihya-Sutras_djvu.txt). (last visited on January 4, 2022)

¹⁸ R. Shastri, *Kautilya's Arthashastra*, 19 (*chaukhambha prakashan*, 2014).

¹⁹ Govind Mishra, *Privacy and the Indian Legal System*, 12 Del. L. Rev. 62 (1990).

²⁰ R. Pande, *Chanakyaniti Darpan*, p.103, <https://www.hindibookspdf.com/chanakya-neeti-darpan-hindi-book-pdf-download/>. (last visited on January 4, 2022)

defects of one's family, (d) mantra, (e) tested and effective medicine, (f) sexual matters, (g) honour, (h) insult and (i) gifts, ought to be kept secret.)²¹”

Existence of Privacy in the Medieval Period

Along with the other rules and regulations, privacy and human dignity attained a significant position in Muslim Personal Law. The “*Purdah*” or veil was immensely prevalent in the Muslim society, which shows the subsistence of notion of privacy in the form of deeply embedded custom in the Muslim culture. There were express rules relating to Privacy of home in Islamic Law. As the home was the basis of family, thereby for the protection of Family Privacy, Privacy of Home was recognized in Islam.

In this sense, Islamic idea of Privacy of Home was similar with the Western view of Privacy of Family and Home, as articulated in a well-known saying “*a man's home is his castle*”²². A similar view was found in the verses of Quran, which states that:- “*O ye who believe, enter not houses other than your own without first announcing your presence and invoking peace upon the people therein. That is better for you, that you will be heedful ... and if you find no one therein, still enter not until permission hath been given, and if it to said unto; go away, for it is purer for you, Allah knoweth what you do*”²³”

Peeping into the houses of other people was strictly prohibited as amounting to violation of Privacy. In this respect, Prophet Mohammed announced the following rule: “*If a person peeps into somebody else's house without permission, the people of the house will be justified if they injure his eye*”. Privacy of correspondence was also recognized in Islam. In this respect, Prophet Mohammed prescribed in a Hadith as follows:- “*People would be prohibited from reading letters of others and warned that even if a man casts side long glances in order to see a letter of another person, his conduct becomes reprehensible.*” Spying was prevented in Islam, which as a general rule would always be prevented in every society for the protection of privacy²⁴. The modern theorists also consider spying as an instrument for intrusion on privacy and thereby recommend its prohibition. In this sense, this rule of Islam law could be considered as the fore-runner of the Modern rules of Privacy Law that recognized right to privacy as a human right 1400 years back²⁵.

Inception of Right of Privacy as a Human Right in Modern Era

Right of Privacy is nevertheless an elementary human right and it has also been recognized in various international and regional instruments. In the modern age, privacy has

²¹ *Ibid.*

²² I.P.Massey, *Constitutionalization of the Right to Privacy in India*, in B.P.S.SEHGAL (Ed.), *Human Rights in India*, 311 (Deep and Deep Publications 1995).

²³ (QURANXXIV:27,28)

²⁴ Sheikh Showkat Hussain, *Right to Privacy*, 3 J. ISL. & COMP. L. QUA'Y, 107, 108 (1983).

²⁵ Medani Abdel Rahman Tageldin, *Right to Privacy And Abortion: Jurisprudence*, 12 ALIG. L. J., 140, 141 (1997).

acquired a significant place among other basic human rights. The term was first coined by Warren and Louis Brandeis, the American lawyers in their seminal text on “privacy as a tort action” defining privacy as “the right to be left alone²⁶.” At international level, the contemporary privacy yardstick is found in the “Universal Declaration of Human Rights 1948” in which, the right to privacy was specifically recognized as a basic human right for the first time²⁷.

Specifically, shielding territorial and communicational privacy of individuals, Art. 12 of the declaration states that, “No-one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks²⁸.” Same right has been assured by “International Covenant on Civil and Political Rights, 1966” under art. 17²⁹. Same language has been adopted by the “UN Convention on Migrant Workers³⁰” and the “UN Convention on Protection of the Child³¹.” The right is also being recognized at regional level. 1950 The “Convention for the Protection of Human Rights and Fundamental Freedoms, 1950,” also protects the privacy of individual and his family life³².

By and large, it is explicitly recognized by various countries in world in their constitutions. They commonly include provisions regarding protection from trespass of home and secrecy of personal and confidential communications. Several new Constitutions of the nations for instance “South Africa” and “Hungary” comprise definite provisions regarding access and manage personal information of individual. In various other countries such as the United States, Ireland and India wherein privacy as a right is not overtly provided under Constitution, the right has been granted by judicial activism³³.

Modern Indian Jurisprudence

Our Constitution is an amalgamation of the most excellent provisions of the different Constitutions of the world. One of the most significant provisions crafted by our Constitutional framers is Fundamental Rights. They have incorporated almost all the basic rights recognized as human rights by international instruments in the form of Fundamental Rights making them more concrete. Right to privacy as a fundamental right is not explicitly

²⁶ Warren and Brandeis, *The Right to Privacy*, 4 Har. L. Rev. 193 (1890), <https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>. (last visited on January 5, 2022).

²⁷ David Banisar, Simon Davies, *Privacy And Human Rights An International Survey of Privacy Laws And Practice*, available at: <http://gilc.org/privacy/survey/intro.html#fnlnk0025>. (last visited on January, 8, 2022).

²⁸ *Universal Declaration of Human Rights, 1948*, art.12.

²⁹ *The International Covenant of Civil and Political Rights, 1966*, art.17.

³⁰ *International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, 1990*, art. 14.

³¹ *Convention on the Rights of the Child, 1989*, art.16.

³² *Convention for the Protection of Human Rights and Fundamental Freedoms Rome, 1950*, art.8.

³³ S. K. Sharma, *Privacy Law A Comparative Study*, 333 (Atlantic Publishers 1994).

provided under Indian Constitution but by means of judicial interpretation, this right is brought within the realm of fundamental rights by our judiciary. In our modern Indian Jurisprudence, “Right to Privacy” can be discovered in late 1800s when local British court upheld the privacy of a “*pardanashin*” lady.

This jurisprudence is being evolved with the passage of time as a corollary of article 21 although it is not explicitly recognized by our Constitution.³⁴ Article 21 of the Constitution of India states that “No person shall be deprived of his life or personal liberty except according to procedure established by law.” It can be adequately interpreted after a perusal of Article 21 that the term “life” consists of all facet of life vital for a meaningful, inclusive and dignified life and right to privacy is also an essential element of it which has specifically declared as a Fundamental Right by the Apex Court.³⁵ After a long journey, now, right to privacy has been explicitly or implicitly found place in Indian legal regime.

Right to Privacy under IPC The Indian Penal Code contains many provisions making breach of privacy an offence punishable under it. These provisions include:

Disclosing the identity of the victim- Sec. 228A of the Code protects the right of privacy of victims of some specific offences as provided in the code and prescribes a punishment upto two years with fine for the offence of disclosure of such identity to prevent the victim from social stigma³⁶.

Voyeurism- The Code makes punishable watching or capturing the image of any women engaged in any private act under section 354C respecting privacy of women³⁷.

Stalking- Following and contacting any women personally or digitally, in spite of her apparent lack of interest in such interaction is made punishable under the Code under section 354D.

Right to Privacy under Indian Evidence Act & Information Technology Act

This right is also recognized under Indian Evidence Act. Some communications are protected as privileged communications and the breach of their confidentiality is made punishable under the Act³⁸. Apart from this, the Information Technology Act also contains provisions regarding privacy under sections 66E, 72 & 72A and makes the violation of privacy a punishable offence.

³⁴ Beejal Ahuja, *Judicial interpretation of data protection and privacy in India*, <https://blog.ipleaders.in/judicial-interpretation-of-data-protection-and-privacy-in-india/>. (last visited on January, 8, 2022).

³⁵ *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

³⁶ *Indian Penal Code 1860*, sec. 228 A.

³⁷ *Ibid.* sec. 354C.

³⁸ “*Indian Evidence Act, 1872*. Sec. 122: Communications during the marriage, Section 123: Evidence as to affair of state, Section 124: Official communication, Section 125: Information as to the commission of offences, Section 126: Professional communication, Section 128: Privilege not waived by volunteering evidence, Section 129: Confidential communication with the legal advisor.”

Indian Contract Act

The “*Indian Contract Act, 1872*” allow the parties to the Contract to have a confidentiality clause in the contract to protect the data which form part of the contract³⁹.

Apart from this Copyright Act also protects privacy of data in the form of literary, artistic or any other form of intellectual property safeguarding the human right of privacy. There are various other provisions in the form of Acts, Rules and Regulations safeguarding right to privacy in spheres such as health, commercial and legal sectors etc. But there is a strong need of a comprehensive data protection law.

Judicial Contribution

Judiciary has played a vital role in establishing right to privacy as a Fundamental Right. The Punjab and Haryana high court, in *Kanwaljit Kaur*⁴⁰, held that “allowing medical examination of a woman for her virginity amounts to violation of her right to privacy and personal liberty enshrined under article 21 of the Constitution.” The trio of three decisions of Supreme Court in the cases “*M.P. Sharma*⁴¹, *Kharak Singh*⁴² and *Govind*⁴³,” established the doctrinal foundation of privacy as a fundamental right. If we analyse all of these decisions, the *M.P. Sharma* verdict does not give a ruling on constitutional recognition of privacy as a fundamental right. *Kharak Singh*, on the other hand, rightly acknowledges the dignified existence of term 'life' under Article 21 instead of a right to mere “animal existence.” But, it undergoes with an inner contradiction as on one side, the court struck down the regulation that permitted domiciliary visits considering the privacy concern without using this term expressly, it held that there is no constitutional right of privacy as secured in Constitution. These are two absolutely contradicting views that cannot exist together and both of these decisions are overruled by the Apex court in *Puttaswamy Case* in part that state that the privacy is not protected under the Constitution of India. In, *Selvi*⁴⁴, the apex court differentiated amid physical and mental form of privacy. The judgment further linked the 'right to privacy' with right of self-incrimination under 'Article 20(3).' A constitutional bench of 9 judges delivered a judgment unanimously on 'right to privacy' in *Puttaswamy*⁴⁵ case. It affirmed that privacy is a fundamental right of every individual secured by Constitution of India.

There were six separate but concurring judgments in this case. The court discussed various facets of privacy. It struck down some provisions of Aadhaar Act as unconstitutional.

³⁹ *Indian Contract Act, 1872, sec.27.*

⁴⁰ *Surajit Singh Thind v. Kanwaljit Kaur* AIR 2003 PH 353.

⁴¹ *M.P. Sharma v. Satish Chandra* AIR 1954 SC 300.

⁴² *Kharak Singh v. State of U.P.* 1963 AIR SC 1295.

⁴³ *Govind v. State of Maharashtra* 1975 AIR 1378

⁴⁴ *Selvi and others v. State of Karnataka and others* AIR 2010 S.C. 1974.

⁴⁵ *Justice K.S. Puttaswamy v. Union of India* (2017 10 SCC 1).

Justice Chandrachud aptly stated that, “the Constitution must evolve to meet the aspirations and challenges of the present and the future. In an age where information technology governs virtually every aspect of our lives, the courts must impart meaning to the concept of individual liberty, particularly where an overarching presence of state and non-state entities regulates aspects of social existence which bear upon the freedom of an individual. Every individual irrespective of social or economic status is entitled to the intimacy and autonomy which privacy protects”⁴⁶.

Right of Privacy in Digital Age: Issues & Challenges

In today's digital age, the human right to privacy has acquired acute importance as now a day's almost every work has acquired a digital form. Now we are living in the age where a tedious work can be done within a friction of second on a single click. Now, it is no longer required to wait for hours in the lengthy queues of banks and public offices to pay bills and access services. With the advent of internet and its extreme expansion and with the boon of information technology, it has become extremely simple to communicate and access and share information. But, there are pros and cons of everything in this world. With the rapid development of technology, its misuse is also inevitable. Therefore, the right to privacy, as a human has become very significant right in digital space because today, almost everyone's confidential information is somewhere stored in the digital world⁴⁷. Therefore, it has been recognized in many international texts. The General Assembly of United Nations passed a Resolution on “the right of privacy in the digital age,” on 18 December 2013 which provide for protection of privacy on individual in digital form also. As far as the privacy is concerned, “General Comment No. 16”⁴⁸ on “Article 17” regarding “*Right to Privacy*” of “*the International Covenant on Civil and Political Rights, 1966*” highlights:

“The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law.

Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, What personal data is stored in automatic data files, and for what purposes. Every individual should also be able to, ascertain

⁴⁶ *Ibid.*

⁴⁷ Oliver Diggelmann and Maria Nicole Cleis, *How the Right to Privacy Became a Human Right* 14 HUMAN RIGHTS L. REV. 440, 441 (2014). Available at: <https://www.corteidh.or.cr/tablas/r33348.pdf>. (last visited on January 23, 2022).

⁴⁸ <https://privacy.sflc.in/universal/>. (last accessed on January 23, 2022).

which public authorizes or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.”

This is quite important because India is a signatory to this Covenant therefore this human right to digital privacy is available to Indian Citizens also. They are entitled to enjoy their Human Right of Privacy in all spheres of world whether real or virtual. This is a distressing but true fact that this Human right of people which is now a Fundamental Right also is being violated consistently even without their consent. Today, our data is being stored and shared by websites and intermediaries even without our knowledge. When we browse an online shopping website, we start to receive the notifications relating to the objects of our choices. How they know exactly our choices? It is because they store our Data⁴⁹. It is not about the private entities only. Secret surveillance by governmental agencies without any valid reason is also a big threat to human right of privacy. Lack of digital literacy is also a matter of concern. Numerous cases are being reported on a daily basis regarding the fraud happening to people on digital medium via the means of various apps and other technologies⁵⁰. In this digital age, the matter of privacy has not been circumscribed in the four walls of our home but now it needs to be protected in the virtual world too otherwise it can be misused by anybody without our consent. India does not have a comprehensive data protection law. We need a sound legal framework to protect our data privacy on websites, social media and governmental agencies. The “Personal Data Protection Bill” was presented by the Government in 2019 after the recommendation of our Hon'ble Supreme Court in its legendary “Right to Privacy Judgment” to frame a robust data protection law to secure the data of citizens balancing the interests of citizens on one side and the legitimate concerns of State on other side. The bill contains specific provisions for protecting personal data including establishment of a specific authority for data protection.

The bill was sent to a “Joint Parliamentary Committee” for its appraisal and further recommendations. Recently, in December 2021, the committee has submitted its long awaited report with the finalized “Data Protection Bill, 2021” paving a way for a much awaited data protection law that is the need of the hour in our country to protect the right to privacy of citizens⁵¹.

⁴⁹ *Parminder Jeet Singh, Privacy in the digital age*, <https://www.thehindu.com/opinion/op-ed/privacy-in-the-digital-age/article19446279.ece>. ((last visited on January 22, 2022)).

⁵⁰ *Ivana Stepanovic, Modern Technology And Challenges To Protection of the Right To Privacy*, 42 BELgrade L. REV.170, 171(2014).

⁵¹ <https://www.mondaq.com/india/privacy-protection/1145790/the-data-protection-bill-2021>. (last visited on January 24, 2022).

Summation

It can be aptly concluded that privacy as a human right exists in our social structure since the commencement of human civilization. It had its inception in “Rig Veda”, the oldest and one of the most sacred text of Indians. It was originated with the dawn of Indian culture in “Vedic period” travelled all the way through medieval to modern period and finally acquired the shape of Fundamental Right. Though it existed already since ancient period, Judiciary has indisputably played a key role in recognizing and granting it the status of fundamental Right. The recent Pegasus controversy has once again stirred up the debate regarding right to privacy in India. The matter is pending in the Apex Court; therefore, it would not be feasible to comment upon it. In this digital era, this right to privacy has acquired a new virtual dimension. With the technological advancements, the right to privacy of Indian citizens is more susceptible to violation, therefore, it is the duty of State to adapt appropriate measures for safeguarding it otherwise it will become a right without remedy. The much awaited data protection bill should be enacted on priority basis to secure the data privacy of citizens. To resolve the clashes amid privacy and security, there is a need to find an optimal solution ensuring security as well as minimizing violation of privacy. Unnecessary surveillance should be avoided by the state as gaining public confidence is as much essential to maintain a strong nation. Digital literacy is the need of the time and it should be introduced as a subject in educational curriculum. Apart from it, digital awareness programmes should be organized timely by various public and private institutions and NGOs to make people aware about how they can protect their privacy.

JUSTICE K.S. PUTTASWAMY V. UNION OF INDIA: A CASE EXPOSITION

“They who can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety.” - Benjamin Franklin

*Dr. R.S. Solanki**

Abstract

Privacy, a buzz word of twenty first century is not a new thing for India. “Sarvas Swe Swe Grihe Raja” meaning thereby everyman is a king in his own house, itself speaks in volumes about importance of privacy in our society. Whether or not privacy is an intrinsic fundamental right of a person and is there any invasion in this right? The answers to such questions can be found in J Puttuswamy case, a landmark one in the matter of privacy. The apex court citing Article 21 observed that privacy is the back bone of right to life and personal liberty. The judgement will definitely open new horizons of privacy in the matters relating to state surveillance, religious expression and data protection and at the same time is also likely to open a Pandora box of some more constitutional challenges in coming future. The foundation is already set by way of challenge to the provisions relating to “restitution of conjugal rights” provision in the Hindu Marriage Act and Special Marriage Act as they are found violative of privacy rights. To quote John Perry Barlow “Relying on the government to protect your privacy is like asking a peeping Tom to install your window blinds” and so as a citizen more so a netizen, when we claim our rights, it is also our duty to ensure privacy to the extent we can protect.

Privacy, a buzz word of twenty first century is not a new thing for India. “Sarvas Swe Swe Grihe Raja” meaning thereby everyman is a king in his own house, itself speaks in volumes about importance of privacy in our society¹. Privacy was always an intrinsic part of a person's life, whether it was Veda, Upinishad, epic like Ramanayna or Mahabharata or for that matter Manu Smiriti. Going through these ancient texts, it is clearly found that even at that time privacy was regarded as an important right of an individual governed by some rules.

Ancient Indian texts like '*Hitopadesha*' do find the mention of this concept when it says, “certain matters in relation to worship, family, and sex should be protected from

* Dr. R.S. Solanki, Associate Professor & HOD, School of Law, Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan)

¹ Deshta, K., 2011. *Right to Privacy under Indian Law. deep and deep.*

disclosure².” It was a duty of the king to promote dharma and protect privacy. Kautilya's Arthashastra too prescribes a detailed procedure to ensure right to privacy. These ancient Indian texts not only talks about privacy of a man but they have given importance to privacy of women as well. . Yajñawalkya Samhita states, "If many persons know a woman against her will, each of them should be made to pay a fine of twenty four panas³". Kautilya's Arthashastra has gone further talking about the privacy of commercial sex workers when it says that she has the right, not to be held against her will. Moreover no sexual intercourse could be done forcefully and without her wish⁴. Privacy was enjoyed by women socially as well as matrimonially. Privacy of a women can best be understood by the fact that even husband was not allowed to take a glimpse of her wife while she was relaxing⁵.

Great Greek philosopher Aristotle has also talked about private domain 'the polis' and has distinguished it with public domain 'the oikos'. According to him every person's life comprises of public as well as private sphere⁶. 'On Liberty' an essay by Mill has also found the distinction between public and private domain in reference of governmental authority⁷.

Locke too has made the distinction between public and private domain while discussing property in his 'Second Treatise on Government.'⁸ Then, there are cultures protecting privacy by way of concealing the things, secluding the things or else by way of prohibition to secret ceremonies. Surprisingly, some studies on animals also suggest that privacy is not restricted to human beings but there is desire for privacy even among animals.

But when Edward Snowden observes “A child born today will grow up with no conception of privacy at all”⁹ it creates suspicion in the minds of people. Whether or not privacy is an intrinsic fundamental right of a person and is there any invasion in this right? And so, J Puttuswamy case¹⁰ has become a landmark case in the matter of privacy. It was year 2009 when Government of India introduced *Aadhar* scheme to lay foundation for the world's largest as well as unique identification system. Very soon, in 2012 a 91-year old retired High Court Judge K.S. Puttaswamy filed a petition to raise the voice against the 'constitutionality

² Law Times Journal. 2022. *Privacy as a fundamental right - Law Times Journal*. [online] Available at: <<https://lawtimesjournal.in/privacy-as-a-fundamental-right/>> [Accessed 12 March 2022]

³ Cis-india.org. 2022. *Locating Constructs of Privacy within Classical Hindu Law The Centre for Internet and Society*. [online] Available at: <<https://cis-india.org/internet-governance/blog/loading-constructs-of-privacy-within-classical-hindu-law>> [Accessed 12 March 2022]

⁴ Bisht, M., n.d. Kautilya's Arthashastra

⁵ *Ibid*

⁶ Natali, C. and Hutchinson, D., 2013. *Aristotle. Princeton and Oxford*: Princeton University Press.

⁷ Mill, John Stuart (1860). *On Liberty* (2 ed.). London: John W. Parker & Son.

⁸ Encyclopedia Britannica. 2022. John Locke - *Two Treatises of Government*. [online] Available at: <<https://www.britannica.com/biography/John-Locke/Two-Treatises-of-Government>> [Accessed 12 March 2022].

⁹ zeitgeist, D., 2022. Digital dilemmas shape the zeitgeist. [online] euronews. Available at: <<https://www.euronews.com/2013/12/20/digital-dilemmas-shape-the-zeitgeist->> [Accessed 12 March 2022].

¹⁰ *Justice K.S. Puttaswamy v. Union of India* (2017) 10 SCC 1

of *Aadhaar*'. The contention was violation of the right of privacy by filing a petition before the apex court. The petition opposed the move of the government making it compulsory to have a uniform biometric card to access government schemes and services. The apex court citing Article 21 ("No person shall be deprived of his life or personal liberty except according to procedure established by law") observed that privacy is the back bone of "Right to life and personal liberty". The historic judgement is likely to open a Pandora box of some more "constitutional challenges" in coming future¹¹.

What was the core issue?

Can privacy be regarded as a "fundamental right" by virtue of Article 21 of the Indian Constitution? Are earlier judgements in *Kharak Singh*¹² & *M. P. Sharma* case¹³, a true reflection of the Constitutional spirit?

What did Petitioner argued?

Article 21 of the Indian constitution which talks about Right to life and personal liberty is incomplete without right to privacy which is an intrinsic part of it. And so, it is our duty to protect it under our constitution. Moreover, there is a need to relook verdict in *Kharak Singh*¹⁴ & *M.P. Sharma* case¹⁵ as they violate the Right to Privacy under Article 21 of the constitution.

What did Respondent reply?

That the constitution does not ensure "Right to privacy" and thus it does not specifically protect the "Right to privacy" and so Article 21 of the Indian Constitution (the Right to life and personal liberty) does not apply in the cases of both *M.P. Sharma*¹⁶ and *Kharak Singh*¹⁷.

Decision Overview

The verdict of the Apex Court on "Right to privacy" seems to be very clear. The way our Supreme Court took liberal view in past and did interpretation in earlier cases to various facets of Right to life like "rights to education; livelihood; food, water, and shelter; against custodial violence; reproductive rights under the common umbrella of Right to life", now the interpretation is to include privacy as a right as well. The judgement, although seems to be unanimous is having six separate but concurring decisions. One Judge who authored the

¹¹ *Ibid*

¹² AIR 1963 SC 1295

¹³ AIR 1954 SC 300

¹⁴ AIR 1963 SC 1295

¹⁵ AIR 1954 SC 300

¹⁶ AIR 1954 SC 300

¹⁷ AIR 1963SC 1295

decision speaks for himself and three other judges. The rest are concurring judgments authored by five different judges. These concurring opinions of the judges have recognized the Right of privacy and have given new dimensions to “Right to life and personal liberty”.

The Judge who authored the decision speaking for himself and three other judges opined that “privacy was not surrendered entirely when an individual is in the public sphere.” Furthermore, they also observed that the Right to privacy also includes the “negative right” against the interference of State and a “positive right” to have protection by the State. And thus, they felt the need for a “data protection regime” in India. According to other concurring judgements, “Right to refuse medical treatment, a right against forced feeding, the right to consume beef and the right to display symbols of religion in one's personal appearance etc.” are deemed Right to privacy. Over the issue of consent, it was observed that consent is a key requirement for sharing personal data like health records. As far as facets of privacy are concerned, it is classified as “non-interference with the individual body, protection of personal information and autonomy over personal choices”. It is also observed that besides Right of privacy's existence as an independent right, it includes a person's right to freedom which is a precondition to fulfill the aim of liberty and fraternity as enshrined in our constitution so as to ensure dignity of the individual. The right to privacy was also discussed in context of protecting personal reputation. A need for a law on data protection with proper safeguards was also felt.

Is every majority opinion binding?

There seems to be a consensus that each and every part of the judgment is not a binding law, no matter it is a majority judgement. In the present case, the Honorable court ultimately made four holdings three holdings are based on the correctness of the earlier case law and the other confirmed that the Right to Privacy is protected as an integral part of the “Fundamental Rights”.

By seeing the pattern, one can say that the holdings should be binding to the extent it is arrived on the basis of reasoning. No doubt, it was a welcome move to overrule the infamous ADM Jabalpur case¹⁸ which went against Fundamental Rights, but when we see the things from eyes of law, can we say that it was an ultimate decision? The reason to overrule might be to overcome any cacophony with the interpretation of the Fundamental Rights. But the fact is that the ADM Jabalpur judgement was already superseded by way of an amendment in the constitution and implicitly overruled by the Supreme Court.

Of course, the law fraternity will always have a mixed opinion. Although other parts of the decision are also necessary to reach the conclusion that the Fundamental Rights at its

¹⁸ (1976) 2 SCC 521

core have Right to Privacy. But at the same time ,when we go into the details of the judgement we conclude that there is something more in the judgment which is not needed for the final holding. And thus, one can say that such parts of the judgment are only “persuasive by nature but not binding”.

When this type of judgements comes, where four judges are on one side and five judges on other side and that too with five individual judgments, the immediate question which comes to mind is about binding nature of whole judgement. It is pertinent to mention here that to make a judgement binding, the majority of judges should opine for the same. Similar voices were raised in triple talaq case where Justice Nariman ruled on arbitrariness. And how can one forget Kesavananda Bharati case¹⁹, a landmark constitutional case where 13 judges gave 6 different views on Parliament's power to amend the constitution. Thankfully in the present case of J Puttuswamy, the Supreme Court, by its judgement signed by all the nine judges has tried to remove all the ambiguities and has clarified all the related issues.

But still exists, the divergence of opinion. Justice Chandrachud's opinion for four judges seems to adopt the test of “reasonable expectation of privacy” in India but Justice Nariman seems to reject it .What will be the “nature of privacy” and what will be the “permissible limitations” are also paramount questions here. To know the binding nature of judgement, the possible way out is creation of “comprehensive matrix of issues” and marking the views of the six judgments on each of them. If a minimum of five judges have a consensus, it will be a binding then. Although it seems simple and quite obvious also, the thing is that judiciary has unwittingly relied on minority opinions in the past .To rely on “Justice Chandrachud's four-judge opinion (or to call it a majority opinion) without checking to see if at least one other judge agrees” would be an error. It is worth mentioning here that the Supreme Court has already settled down the dust by holding that the views that in a leading opinion (J Chandrachud's opinion), even if not the majority opinion, would be binding to the extent, there is no disagreement on concurring opinions.

Applicability of Right to Privacy

Can court enforce the Right to Privacy against private players? Might not but may be. The discussions are already there regarding individual rights of privacy against internet companies. It is pertinent to mention here that some of the judges have already touched the matter of internet and Right of Privacy and have also highlighted the issue of Right of Privacy and Publishers. Undoubtedly, fundamental rights are enforceable against a state action, but at the same time if state agrees to uphold those rights against private players, even

¹⁹ AIR 1973 SC 1461

private players can be brought under the umbrella of right of privacy. Vishaka case²⁰ of 1997 on sexual harassment at workplace can be taken as precedent where the judiciary found a Parliamentary vacuity over the matter. Same thing has happened in the pending WhatsApp case²¹ also where state is asked to protect the fundamental right to privacy of citizens by way of legislating over data protection.

In the present case of J Puttaswamy, it looks that the court is working on this reasoning. J Chandrachud and J Kaul's discussion on right to privacy against internet companies seems to be a recommendation of a data protection law so as to protect the privacy rights of internet users. One may also regard it as a suggestion from judiciary to have a “Fundamental Right to a data protection regime” the way it was done in Vishaka case. As far as publisher's right of privacy are concerned, J Kaul's has his own view. Although an individual's right “to exercise control over his own life and image as portrayed to the world and to control commercial use of his identity” seems tricky at the moment and is not binding right now but it may start a new debate on a new dimension of privacy rights in future. At present, it can be viewed as a matter of common law which covers private players.

Is Consent Outdated?

One criticism, the Supreme Court often faces is in context of a consent-based privacy framework. How appropriate it is in modern times of disruptive uses of data, always remain a fundamental question. Again when we see right of privacy in context of present case, except a part of “J Kaul's individual judgment”, the judiciary no way seem to be in mood of going ahead with consent-based framework. On the contrary, J Chandrachud has rather cited Y. McDermott's comment that “a solely consent-based model does not entirely ensure the protection of one's data, especially when data collected for one purpose can be repurposed for another” and says “it would be appropriate to leave the matter (of data protection) for expert determination”²².

It is worth mentioning here that any recommendation for a particular form of data protection framework is beyond the “terms of the reference” for the court. And so, the court is seen recommending only “adoption of a data protection framework”. As far as the mode of data protection framework is concerned, it is left to the government. Thus suggestions on the “mode of the data protection framework” are not binding.

²⁰ (1997) 6 SCC 241

²¹ The Indian Express. 2022. WhatsApp vs Govt: in two cases in HC, each side contradicts itself. [online] Available at: <<https://indianexpress.com/article/india/whatsapp-vs-govt-delhi-high-court-privacy-policy-update-7347103/>> [Accessed 12 March 2022].

²² Ibid

Judicial overreach?

Is judgement in J Puttuswamy case is a case of judicial overreach? One may find the observations of the court which seems like creating too much room for judicial discretion. When we go in depth of the judgement we find that “Justices Chelameswar and Nariman” both firmly believe that the judiciary should go an extra mile beyond the words of the constitution – “the necessity of probing seriously and respectfully into the invisible portion of the constitution cannot be ignored”.

The comments of “former Attorney general Mukul Rohatgi,” who argued “part of the case”, are also worth mentioning here. According to him, the Constitution of India after all the ponderings nowhere includes a “right to privacy”. And so, the judiciary should do away with writing it into the document. The power to do so rest with the Parliament²³.

The matter needs thorough examination. Whenever the court goes for wider interpretation of fundamental rights, the issue pops up. Over the years, the Supreme Court, seems as a matter of tradition has read what was not written as a right into the specified “fundamental rights”. Now it is very well settled that “the constitution is an evolving document and that the fundamental rights can always be interpreted broadly”. It seems that the court has therefore only observed “these principles and interpreted existing rights like the right to life and liberty, and to free speech and expression so as to include particular interest i.e. privacy”.

Justice Chandrachud has himself tried to settle down the dust by observing that the judgment was not "an exercise in constitutional amendment brought about by judicial decision. So, unless the principle of evolving fundamental rights is questioned, the verdict does not appear to be a judicial overreach. All of the judges eventually, trace the right to privacy to the fundamental rights specified in the constitution and the preamble. In that sense, the exercise is one of judicial interpretation, not legislation”.

Conclusion

The highest court of the land has once again proved to be the sole custodian of the constitution and champion of privacy rights in India. The much needed liberal, broader and wider interpretation done by the Apex court has opened new doors for a wide range of claims. The judgment covers all the issues and established that privacy is a “fundamental inalienable right, intrinsic to human dignity and liberty under Article 21 of the constitution of India”.

The uniqueness of the judgement is found in the fact that it comprises of six separate but concurring opinions²⁴. The end result is opening of plethora of boxes for the issues pertaining to Article 21 which relates to “fundamental right of life and personal liberty”.

²³ *Ibid*

²⁴ *Justice K.S. Puttaswamy v. Union of India* (2017) 10 SCC 1

At the time when right of privacy is making its mark as a fundamental right globally, India cannot remain untouched. The judgment in the present case seems to be a fair one and more so in the wake of technological advancements which rightly demands privacy rights to be recognized as fundamental right. It is crystal clear judgment which has rightly linked privacy and human dignity. Privacy is a modern era child and due to ever fast changing technology all around, “data protection” has now become a new responsibility or rather duty of the government.

Needless to mention, the judgement is likely to have greater and wider significance as champions of privacy may initiate a new constitutional debate over privacy at global level and its position in India. The judgement has also resulted in giving new dimensions to the “right of freedom and expression by advocating privacy as a natural right”. Any move against it now can be seen as violation of fundamental right itself which is having constitutional backing.

The judgement will definitely open new horizons of privacy in the matters relating to state surveillance, religious expression and data protection. Although the limitations of the right is going to continue in future also depending upon the nature of case as there is no defined hierarchy among the rights given under the constitution, but it seems that privacy will have upper hand against other interests. Will right to be forgotten on internet prevail over open information needs of an individual, can dignity of women be comprised with law on marital rape are few of many such questions which need answer in future. The foundation is already set by way of challenge to the provisions relating to “restitution of conjugal rights provision in the Hindu Marriage Act and Special Marriage Act” as they are found violative of privacy rights²⁵.

To wind up, the landmark judgement delivered by nine judges of the Apex court will be having a binding precedent, unless it is overruled in future. The real test of privacy will lie in “how subsequent courts apply the Puttaswamy decision to determine these varied questions”. Last but not the least, to quote John Perry Barlow “Relying on the government to protect your privacy is like asking a peeping Tom to install your window blinds” and so as a citizen more so a netizen, when we claim our rights, it is our duty also to ensure privacy to the extent we can protect²⁶.

²⁵ Editor, R., Page, O., 2022, B., Quotes, S., Sports, O., gardens, H. and rights, S., 2022. SC terms 'important' pleas seeking striking down of provisions on conjugal rights. [online] Thehindu.com. Available at: <<https://www.thehindu.com/news/national/sc-terms-important-pleas-seeking-striking-down-of-provisions-on-conjugal-rights/article35210962.ece>> [Accessed 12 March 2022].

²⁶ Mindzip.net. 2022. Relying on the government to protect your privacy is like asking a peeping tom to install your window blinds. by John Perry Barlow. MindZip. [online] Available at: <<https://mindzip.net/fl/@JohnPerryBarlow/quotes/relying-on-the-government-to-protect-your-privacy-is-like-asking-a-peeping-tom-to-install-your-window-blinds-614c3cef-4def-4898-b140-fdf939ded7e1>> [Accessed 12 March 2022].

RIGHT TO PRIVACY WITH REFERENCE OF SOCIAL MEDIA LAWS IN NEPAL

*Dr. Balram Prasad Raut**

Abstract

In Nepal, right to privacy is the fundamental rights guaranteed by the Constitution of Nepal which cannot be violated at any cost. Right to freedom of expression is also the fundamental rights guaranteed by the Constitution of Nepal which also cannot be violated at any cost. At the same time, the Supreme Court of Nepal has also established these two rights as fundamental rights in its several decisions. These rights have become universal rights in Nepal. Social media is one of the means of freedom of expression. Social media works through cyber. Here, the issue is how a person uses such means for freedom of expression. In the name of freedom of expression, the right to privacy is violated using the social media. However, one cannot peep in the personal life of another in the name of freedom. When any means is used properly, then it becomes blessings for a person and when the same is used with criminality, then it becomes curse for the human beings. Social media is not always used as a means of freedom of expression, but also for stealing the personal information or peeing in the personal life of an individual. This is a big and challenging issue in Nepal. Therefore, in this paper, the author has analysed the constitutional and legal provisions related to freedom of expression and social media. At the same, time, the paper also includes analysis of the cyber laws and the loopholes existing in the cyber laws. Further, the paper also analyses the decisions of the Supreme Court of Nepal related to right to privacy. At last, some practical suggestions have been given for the concerned authority that whether the State can control the freedom of expression through technology law or not. Or if it can control, then, up to what extent?

1. Introduction

Currently, privacy is a sweeping concept, encompassing (among other things) freedom of thought, control over one's body, solitude in one's home, control over information about oneself, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations.¹

* Associate Professor of Law, Tribhuvan University, Nepal

¹ Daniel J. Solove, 'Conceptualizing Privacy', 90 Cal. L. Rev. 1087 (2002) 1088.

Anyone who studies the law of privacy today may well feel a sense of uneasiness. On one hand, there are popular demands for increased protection of privacy, discussions of new threats to privacy, and an intensified interest in the relationship between privacy and other values, such as liberty, autonomy, and mental health.²

On other hand, media has entered in almost every sphere of our lives, connecting us to both the local and global community. Most popular these days are social media platforms. These have become the most preferred pedestals of sharing information, most importantly on glaring social issues. They have become a vital source of information, especially for the younger generation. Hence, they create a glaring impact on young minds³. Social media is basically a form of communication via the internet. Its main goal, when it came into being, was to create a virtual kinship network throughout the world. However, the social media did not bring the good things with it, but also some byproducts, for example, it has become the means of peeping in the privacy of others, it is used as a means to defaming the repote of the innocent persons and violates the several rights of individuals.

The major social networking sites are Instagram, Facebook, WhatsApp, etc. The users of these social networking sites were untroubled until the coming of the 1990s. This was when cybercrime was born. Therefore, when we talk about social media, the cybercrimes come together. Cybercrime is a new challenge for right to privacy.

Social media is related to freedom of expression. Constitutionally it is fundamental rights. However, when we talk about freedom of expression through social media, it instantaneously comes the right to privacy.

Right to privacy takes social media as a threat. One cannot interfere another right to privacy in the name of freedom of expression. Therefore, right to privacy and social media are not absolute rights. These are relative rights.⁴

It is also said that, believe it or not, it is us who give away our personal information online. Intentionally or unintentionally, we give away a lot of our personal information. This can be by signing up for Amazon prime, Facebook, Instagram etc. Out of the internet users, one third admit to knowing nothing about their personal information which is available online. Tons of cyber information available online has opened the gates for new legal challenges for which adequate laws are yet to be framed.⁵

² A. Westin, *Privacy and Freedom* (1967).

³ Tarannum Vashisht, 'Media and the right to privacy, the incursion of social media'. Available at <<https://blog.ipleaders.in/media-right-privacy-incursion-social-media>> Accessed on 4/16/2022. Dipankar Banerjee, 'Right To Privacy: Concerns Vis-À-Vis Social Media'. Available at <<https://www.legalserviceindia.com/legal/article-5917-right-to-privacy-concerns-vis-vis-social-media.html>> Accessed on 4/16/2022.

⁴ Vashisht (n.3). Banerjee (n.3).

⁵ Vashisht (n.3). Banerjee (n.3).

Right to privacy talks about no interference in an individual matters. Social media talks about no interference in the expression of thoughts. Right to privacy and freedom of expression are fundamental rights and human rights. In between, cybercrime, has posed a threat for the right to privacy in the name of freedom of expression and has created a challenge for right to privacy and social media as well.

Therefore, in this paper, I have tried to deal all these challenging aspects of right to privacy and social media for further discussion. In the first part of this paper, I have introduced the basic concept of right to privacy and social media. It is an introductory part of this paper. The second part of this paper discusses on the definition of the right to privacy and theoretical aspects of the right to privacy where I have described about the views expressed by the scholars available in various literature. In the third part of this paper, the social media and cybercrime have been defined as well as described. The fourth part of this paper covers the analysis of international human rights related to right to privacy. It also describes laws and cases laws of some specific jurisdictions, for example, United States of America, United Kingdom and India. The fifth part of this paper critically analyses the laws related to right to privacy, social media and cybercrime in Nepal. The sixth part includes the analysis of the judicial trends related to right to privacy. There are several cases related to right to privacy, however, few of them have been only described. The seventh part of this paper, which is the last part, is the concluding part which has summed up the whole article including the recommendations.

2. Privacy

2.1. Meaning of Privacy

The term “Privacy” is derived from Latin word “Privatus” which means separated from the rest. Though it is a variable concept and varies with cultural or social context, but actually it means, the right to be left alone. The need for privacy is to create a balance between individual and social interest, which is equally applicable to past, present and future society. The growth and expansion of privacy varied according to the variation in different stages of civilization.

"Privacy" is a term interpreted with several meanings. For present purposes, two types of questions about privacy are important. The first is related to the status of the term: is privacy a situation, a right, a claim, a form of control, a value? The second is related to the characteristics of privacy: is it related to information, to autonomy, to personal identity, to physical access? Support for all of these possible answers, in almost any combination, can be found in the literature.⁶ However, these questions have not been answered in this paper.

⁶ Ruth Gavison, *'The Privacy and Limits of Law'*, The Yale Law Journal, Vol. 89, No. 3 (Jan., 1980) 421-471.

The right to privacy is one of those many concepts of law whose abstract nature makes implementation of the same a complex task. The common saying “your liberty ends where my nose begins” is reflective of the layman's interpretation of their right to privacy. Although simplistic and devoid of any reasonable restrictions, for the layman, it is a reasonable presumption.⁷ A more comprehensive definition of privacy may be found in the Black's Law Dictionary, which calls privacy the “right to be let alone; the right of a person to be free from unwarranted publicity; and the right to live without unwarranted interference by the public in matters with which the public is not necessarily concerned.”

Before establishing what the definition of privacy should be, it is worth considering what makes such a definition acceptable. Parker identifies the following criteria:

First, it should fit the data. Data . . . means our shared intuitions of when privacy is or is not gained or lost. . . . A second criterion . . . is that of simplicity. . . . The standard of simplicity dictates that if some characteristic common to all or some of these evils (i.e. intuitive examples of when privacy is lost) could be found ... so much the better.... The point of the criterion of simplicity is theoretical elegance.⁸

The concept of privacy identifies losses of privacy. As such, it should be neutral and descriptive only, so as not to preempt questions we might want to ask about such losses. Is the loser aware of the loss? Has he consented to it? Is the loss desirable? Should the law do something to prevent or punish such losses?⁹ A reader can get the answer of these questions from the illustration of the theoretical definitions of the subsequent section.

2.2. Theoretical Definitions of Privacy

2.2.1. *The Right to Be Let Alone*

The "right to be let alone" occupies a hallowed place in privacy discourse. Although the phrase was coined by Judge Cooley,¹⁰ who used it not to justify a right to privacy, but rather to explain why tort law regards trespass to the person as wrongful. It is now generally attributed to Warren and Brandeis, who invoked it throughout their seminal article.¹¹

2.2.2. *Control of Personal Information*

This theory of privacy is prevalent in the legal and philosophical literature.¹² West in, an influential early commentator, wrote that privacy is "the claim of individuals . . . to

⁶ Ruth Gavison, 'The Privacy and Limits of Law', The Yale Law Journal, Vol. 89, No. 3 (Jan., 1980) 421-471.

⁷ Suprateek Neogi, 'Right to Privacy and Social Media', RGNUL Student Research Review (RSRR). Available at <rsrr.in/2018/10/27/right-to-privacy-and-social-media/> Accessed on 4/15/22.

⁸ Richard Parker, "A Definition of Privacy" (1974) 27:2 Rutgers L Rev 279.

⁹ Gavison, *The Privacy* (n 6).

¹⁰ Thomas M Cooley, *A Treatise on the Law of Torts*, 2d ed (Chicago: Callaghan, 1888) 29.

¹¹ Irwin R Kramer, "The Birth of Privacy Law: A Century Since Warren and Brandeis" (1990) 39:3 Cath U L Rev 703.

¹² Daniel J Solove, "Conceptualizing Privacy" (2002) 90:4 Cal L Rev 1087.

determine for themselves when, how and to what extent information about them is communicated to others".¹³

2.2.3. *Inaccessibility*

This theory sees privacy as "limited access to the self".¹⁴ Its most influential proponent is probably Gavison, although she was preceded by Van Den Haag¹⁵ and O'Brien¹⁶ and was followed in large measure by Moreham.¹⁷ Moreham attempts to overcome the deficiencies of Gavison's approach by developing a sensorial access theory that emphasizes the importance of the individual's *subjective desires*. According to Moreham, privacy is best defined as follows:

[T] he state of "desired 'in access'" or as "freedom from unwanted access". In other words, a person will be in a state of privacy if he or she is only seen, heard, touched or found out about if, and to the extent that, he or she wants to be seen, heard, touched or found out about.

Something is therefore "private" if a person has a desire for privacy in relation to it: a place, event or activity will be "private" if a person wishes to be free from outside access when attending or undertaking it and information will be "private" if the person to whom it relates does not want people to know about it.¹⁸

It's unequivocally argued that every right has certain restrictions and exceptions. In Roman law, consent is considered as a ground of justification against privacy, meaning thereby, there is no harm done to someone who voluntarily consents to injury or to the risk of injury. This concept is expressed under the celebrated doctrine of *volenti non fit injuria*. For instance, a doctor would not be held responsible for the infringement of the right to privacy if his patients consent to the disclosure of information relating to his health.

2.3. **Why Privacy is Important?**

Having identified what privacy is, I now turn to discuss why it is important. In *Campbell v. MGN*, Lord Hoffmann identified the "underlying value [s]" of the reworked breach of confidence action (which provides a civil remedy for the unjustified disclosure of private

¹³ Alan F Westin, *Privacy and Freedom* (New York: Atheneum, 1967) 7.

¹⁴ Daniel J Solove, "Conceptualizing Privacy" (2002) 90:4 Cal L Rev 1087.

¹⁵ Ernest Van Den Haag, "On Privacy" in J Roland Pennock & John W Chapman, eds, *Nomos XIII Privacy* (New York: Atherton Press, 1971) 149 ("privacy is violated if it is abridged beyond the degree which might be reasonably expected ... by one's activity. If one's image ... is displayed to a wider public ... than could reasonably be expected to perceive it, one's privacy is violated" 157-58).

¹⁶ David M O'Brien, *Privacy Law and Public Policy* (New York: Praeger, 1979) ("[p]rivacy may be understood as fundamentally denoting an existential condition of limited access to an individual's life experiences and engagements" 16).

¹⁷ Gavison, *The Privacy* (n 6).

¹⁸ Gavison, *The Privacy* (n 6).

information) as focusing on the "protection of human autonomy and dignity-the right to control the dissemination of information about one's private life and the right to the esteem and respect of other people".¹⁹ Lord Nicholls observed that "[a] proper degree of privacy is essential for the [well-being] and development of an individual".²⁰

In *Von Hannover v. Germany*,²¹ the European Court of Human Rights discussed the minimum content of Article 8 of the European Convention on Human Rights, which states that everyone has a right to respect for his private life and which now guides the development of there worked English confidence action.

The Court held that the scope of protection under Article 8 "includes a person's physical and psychological integrity . . . [and] is primarily intended to ensure the development, without outside interference, of the personality of each individual in his relations with other human beings".

The different emphasis placed on the values of privacy by the House of Lords and the European Court of Human Rights reflects a basic division in the academic literature-the division between what may be called deontological and consequentialist approaches.²² In essence, deontologists offer rights-based arguments; they concentrate on the inherent worth of privacy (typically as an aspect of dignity, autonomy and personhood) and they assert that respect for it, as a fundamental value, is an obligation imposed on others as a moral duty.²³ On this account, privacy is a value inherent to an individual's existence as a "human person".²⁴ Consequentialists, in contrast, offer utility-based arguments; for them, the importance of privacy lies primarily in the promotion of various goods (both for the individual and for society) that flow from its protection or are undermined by its violation.

3. Social Media

In Nepal, most of the cybercrimes are related with social media.²⁵ Social media is a type of internet-based communication. There are different types of social media, such as blogs, microblogs, wikis, social networking sites, widgets, and virtual worlds. However, social networking services such as Facebook, twitter, WhatsApp, Orkut and Myspace have grown

¹⁹ *Campbell v. MGN Ltd*, [2004] UKHL 22, [2004] 2 AC 457 [Campbell]. Since Campbell, there have been a number of important decisions which have fleshed out the elements of the cause of action.

²⁰ *Campbell v. MGN Ltd*.

²¹ (no. 2) [GC] - 40660/08 and 60641/08, Judgment 7.2.2012 [GC].

²² David Lindsay, "An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law" (2005) 29:1 Melbourne UL Rev 144.

²³ Hilary Delany & Eoin Carolan, *The Right to Privacy: A Doctrinal and Comparative Analysis* (Dublin: Thompson Round Hall, 2008) 94.

²⁴ David Lindsay, *An Exploration of the Conceptual Basis of Privacy* (n. 22) 144.

²⁵ Chuda Bahadur Roka, 'Cybercrime and Security in Nepal: The Need for Two Factor Authentication in Social Media', *Crossing the Border: International Journal of Interdisciplinary Studies* Volume 5; Number 2; 15 July 2017. Available at <file:///C:/Users/dell/Downloads/15016.pdf> Accessed on 4/18/2022.

in popularity in recent years. The primary goal of these social networking services is to create kinship in the virtual world. However, the users were unaware that this windfall was also accompanied by criminality.²⁶

The concept of cyber crime originated in the 1990s and has climbed the success ladder to whole new level. But it is us who made the bargain with the devil, and our privacy is now jeopardized. Ip address, key terms used in searchers, seemingly innocuous websites visited, information share on social media, online transactions, cookies collecting user browser history, mobile registration- each use internet generates personal information about an individual. Like amazon, the site instantaneously records our personal information. If they do this because the more personal information they supply, the more appealing they are to prospective advertisers.

As a result, incidences of identity theft, sexual predators, inadvertent stardom, cyber staking, and defamation have begun to garner attention. Scams have also been detected, such as koob face, who took personal information from Facebook users and gave it to the incorrect individuals. According to reports, html coder version 5 will provide advertising corporations access to users' online activities such as texts, images, emails, and many more.

Typically, children are the most vulnerable. They no longer hesitate to reveal their personal information with someone they do not even know. This is due to a lack of mental development and the ability to distinguish between right and wrong. As a result, these sexual predators and identity thieves are easily traced.

3.1. Cybercrime

Cybercrime can be regarded as the computer mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic network. The Encyclopedia Britannica defines cybercrime as 'any use of a computer as an instrument further illegal ends, such as committing fraud, trafficking, child pornography and intellectual property, stealing identities or violating privacy.

The United Nation Office of Drugs and Crime has defined cybercrime as an act²⁷ against the confidentiality, integrity and availability of computer data or systems, computer-related acts for personal or financial gain or harm, including forms of identity-related crime, and computer content-related acts.

Cybercrime can be regarded as “computer-mediated activities which are illegal or considered illicit by certain parties and which can be conducted through global electronic networks”. In general, cybercrime can be defined as a crime committed in a cyber

²⁶ Banerjee (n.3).

²⁷ 'Comprehensive Study on Cybercrime', United Nations Office on Drugs and Crime, (February 2013) 11.

environment, including the Internet, computer networks, and wireless communication systems. In other words, cybercrime involves crime committed through use of the computer.²⁸

This brings us to the issue of defining computer crime. Computer crime is broadly defined by the US Department of Justice as “any violations of criminal law that involve knowledge of computer technology for their perpetration, investigation, or prosecution”.²⁹

3.2. Cyber Criminal

Cyber Criminal is a person who commits an illegal act with a guilty intention or commits a crime in context to cybercrime. Cybercriminal can be motivated criminals, organized hackers, discontented employees, cyber terrorists.³⁰

4. International Instruments

Right to privacy is globally considered a sacrosanct fundamental right and it's a part of the right to life with dignity. Article 17 of the International Covenant on Civil and Political Rights (ICCPR), 1966 provides for the right to privacy in regards to family or correspondence and this provision does not go counter to Article 28 of Nepal's constitution. Article 12 of the Universal Declaration on Human Rights (UDHR), 1948 is almost in similar terms. Article 1, which guarantees human dignity, and Article 19, which is put in place for the protection and promotion of freedom of speech and expression, of UDHR, 1948 supplement and supplant right to privacy. United Nations Guidelines for the Regulation of Computerized Personal Data Files also provides for different principles that, in one or some another way relates to the boundary of privacy. It includes the principle of accuracy of data; the principle of the purpose of specification; the principle of security over the accidental loss, unauthorized use of files or misuse of data; and principle of trans-border data flows.

In the United States of America, right to privacy is protected under the Bill of Rights.³¹ In India, the Supreme Court decriminalized consensual sex, including homosexual sex, and struck down Section 377, Indian Penal Code, 1860 in the landmark case of *Navtej Singh Johar vs Union of India*.³²

²⁸ Suleyman Ozeren, *Global Response to Cyber Terrorism and Cybercrime: A Matrix for International Cooperation and Vulnerability Assessment*, Doctor of Philosophy, University of North Texas, August 2005

²⁹ Ozeren, *Global Response to Cyber Terrorism* (n. 28).

³⁰ Dr. Ajeet Singh Poonia, 'Cybercrime: Challenges and Its Classification', International Journal of Emerging Trends & Technology in Computer Science, Volume 3, Issue 6, November-December 2014.

³¹ First Amendment (Freedom of press, speech, and expression); Third Amendment (Protection of home from the quartering of troops without the consent of the owner); Fourth Amendment (Protection against unreasonable search and seizure); Fifth Amendment (Privilege against self-incrimination) and Fourteenth Amendment (Due process, i.e., just, fair, and reasonable substantial and procedural law).

³² *Navtej Singh Johar & Ors. v. Union of India* thr. Secretary Ministry of Law and Justice, W. P. (Crl.) No. 76 of 2016.

In the United Kingdom, Article 8 of the Human Rights Act, 1998 guarantees that every person has the right to respect for his private and family life, his home, and his correspondence. It is to be noted here that bodily integrity, personal autonomy, personal information, personal identity and not being subject to surveillance falls within the ambit of private life. Article 10 of the Act, 1988 guarantees freedom with respect to speech and expression. In *Campbell vs MGN Ltd*,³³ the House of Lords found Daily Mirror newspaper guilty for infringing privacy of supermodel Naomi Campbell. The newspaper carried a story about her personal life, including that of receiving treatment for drug addiction.

5. Constitutional and Legal Provisions on Right to Privacy

5.1. Constitution of Nepal 2015

Constitutionally speaking, the right to privacy is an inviolable fundamental right under Article 28 of the Constitution of Nepal which guarantees rights to individuals to decide who may enter their residence, and protects them against unauthorized intrusions. It provides the limits, the ability of state and private persons to gain access to personal information in regard to property, documents, records, statistics, and correspondence of others and to use and disclose such information. This way, the right to privacy extends to those aspects of a person's life with regard to which he or she has a legitimate expectation of privacy. And, this legitimate expectation of an individual extends to social networking sites as well.³⁴

5.2. Right to Privacy Act, 2018

Nepal has enacted the Right to Privacy Act, 2018 to implement Article 28 of the Constitution of Nepal 2015 which guarantees every person the right to privacy in relation to the person, and his residence, property, documents, records, statistics, correspondence, or reputation. The Act, 2018 casts an obligation on the state to ensure every person's right to privacy over his/her physical or mental conditions. Section 3 explicitly and authoritatively obligates the state to provide an atmosphere under which a person could secure privacy over his body, health conditions, sexual orientation, reputation or medical conditions, biological conditions, virginity, potency, consensual affair, pregnancy, and the likes.

5.3. Muluki Penal Code, 2017

Muluki Penal Code, 2017 has a separate chapter on Provisions Relating to Offences against Privacy.³⁵ The Code criminalizes conducts such as unauthorized tapping of a voice

³³ [2004] UKHL 22; [2004] 2 AC 457; [2004] 2 WLR 1232; [2004] EMLR 247

³⁴ Jivesh Jha, 'Right to privacy law in digital age: Nepal needs to educate social media users on cyber democracy', Available at <<https://www.southasiamonitor.org/nepal/right-privacy-law-digital-age-nepal-needs-educate-social-media-users-cyber-democracy>>. Accessed on 4/16/2022.

³⁵ Part 3, Chapter 1, Sections 293-304.

conversation, breach of confidentiality, taking and editing photos of a person without consent, breach of privacy of information in electronic media, unauthorized search of body or belongings of person, and trespassing. These activities are considered to be private criminal cases and the states will not proceed the case on behalf of the victim. The victim has to file a complaint within 3 months from the date of the event at the relevant District Court. The Court can impose fine up to 30,000 Nepalese rupees or imprisonment of maximum of 3 years. Further, victim will also be entitled to compensation.

Individual's right to refuse medical treatment or terminate his life and opt for euthanasia falls within the ambit of right to privacy. Right to Privacy Act is silent on this matter.³⁶

5.4. Overlapping provisions in the Right to Privacy Act 2018 and Muluki Penal Code, 2017

Although the Right to Privacy Act embodies many provisions similar to Muluki Penal Code, however, these two laws have certain overlapping provisions. Firstly, the Muluki Penal Code sets out specific punishment for each offences unlike the Privacy Act which states that the violation of the Privacy Act will result in punishment of up to NPR 30,000 or imprisonment of maximum of 3 years or both. However, the provisions related to punishment for same kind of offence under the Code and Privacy Act is divergent.

For instance, if anyone commits offence related to unauthorized search of body or belongings of person without consent, the offender would be liable for punishment of imprisonment up to 1 year or fine up to NPR 10,000 or both under the Code whereas, the offender, if prosecuted under the Privacy Act, would be liable for imprisonment up to 3 years or fine up to NPR 30,000 or both.³⁷

Secondly, the Code states that all offences provisioned therein are to be filed as a private party case whereas the Privacy Act states the offences like body search without a warrant and taking a photograph without consent is to be prosecuted by the state. These issues will create ambiguities in filing of the case and in seeking specific remedy for violation of Act.³⁸

5.5. Failure to cover emerging issues of data protection

There are certain important aspects which the Privacy Act has failed to address. The definition of the personal data only incorporates the specific forms of data. With the existing definition, the Privacy Act doesn't leave any room for the wider interpretation of personal data. For example, while 'email' address is considered as a personal data, the IP address or even a social network or website of a person will not be considered as a personal information if interpreted in a strict sense.

³⁶ Jivesh Jha and Nil Prasad Paneru, '*Assessing Privacy Law*', Available at <<https://myrepublica.nagariknetwork.com/news/assessing-privacy-law/>> Accessed on 4/16/2022.

³⁷ Jha, '*Right to Privacy Law in Digital Age*' (n. 34), Jivesh Jha and Nil Prasad Paneru, '*Assessing Privacy Law*' (n. 36).

³⁸ Jha, '*Right to Privacy Law in Digital Age*' (n. 34), Jivesh Jha and Nil Prasad Paneru, '*Assessing Privacy Law*' (n. 36).

Importantly, the Privacy Act does not define or specify about some of the vital issues in data protection such as “controller” and “processor”. The Privacy Act does not make any differences between a controller and processor of a data. This will add difficulty to the issues of data management, data protection and liability for breach of privacy difficult in practice.³⁹

The Privacy Act provides for the power to frame necessary rules to government of Nepal to implement the Privacy Act. It is yet to be seen how far would the rules clear the ambiguities of the Privacy Act, but it can be hoped that it will give way for better implementation of protection of privacy of a person and data management.⁴⁰

5.6. National Broadcasting Rules 1995

The latest is the 11th amendment to the National Broadcasting Rules in the Nepal Gazette. Like all previous ill thought out rules, this one is vague, contradictory, and unconstitutional.

The new amendment seeks to regulate Over the Top (OTT), Video on Demand (VOD) and internet television in Nepal. OTT is the service of displaying that programs through the internet without using direct-to-home cable or satellite. It also includes media streaming services through other online platforms.⁴¹

Any new law should either try to solve a problem or to facilitate a solution. But this is not just a clumsy attempt to restrict freedom of expression, but a blunt sword that can be used to go after anyone the government does not like. For example, what is a ‘regular broadcast’? Once a month? Once a week? When is an occasional post ‘regular’? Even if it is to regulate ‘regular’ social media content, it should go through an internet specific law like the proposed Information Technology Bill. If it is about a tax on the earnings of online/social media it should be governed by corporate or taxation laws, explains Santosh Sigdel of Digital Rights Nepal.⁴²

By its very nature, the internet is an open ecosystem where people can communicate openly. Nepal’s Constitution guarantees freedom of expression, and the country is also party to the International Covenant on Civil and Political Rights (ICCPR), Article 19.⁴³

Successive governments in Nepal have tried to constrict the public sphere, the right to privacy and media freedom through various bills and regulations. Their vagueness is deliberately designed for arbitrary application against people the government does not like. Nepal today stands as a beacon of press freedom in a region where the mediascape is

³⁹ Jha, ‘*Right to Privacy Law in Digital Age*’ (n. 34), Jivesh Jha and Nil Prasad Paneru, *Assessing Privacy Law* (n. 36).

⁴⁰ Anjan Neupane and Saurav Karki, ‘*Introduction to the Privacy Act 2018*’. Available at <<https://www.neupanelegal.com/news-detail/introduction-to-the-privacy-act-2018.html>> Accessed on 4/15/2022.

⁴¹ Available at <<https://www.nepalitimes.com/editorial/dont-act-on-the-act/>> Accessed on 4/15/2022.

⁴² Anjan Neupane and Saurav Karki, ‘*Introduction To The Privacy Act 2018*’.

⁴³ Anjan Neupane and Saurav Karki, ‘*Introduction To The Privacy Act 2018*’.

increasingly constricted.⁴⁴ Our lawmakers and bureaucrats should abandon the notion that they can suppress free expression just because other countries have.⁴⁵

5.7. Electronic Transaction Act 2004

Prior to 2004, the Government of Nepal dealt with cybercrimes under the Public Offence Act. The current legal framework on cybercrime and electronic evidence in Nepal mostly addresses crimes against electronic and financial transactions through its *Electronic Transactions and Digital Signature Act, 2063 (2008)*/ETA and *Banking Offence and Punishment Act 2064 (2008)*. These two laws are the major laws to regulate the cybercrime committed in the name of social media.

Nepal's cyber world is ruled by ETA that protects users online against cybercrimes. Though the incorporation of cyber law in the ETA is the good beginning and the cybercrime would be considerably reduced in the country. This can be regarded as the preliminary act as many provision related to IT related security are missing. However, the country has entered the process of drafting new cybercrime legislation titled as Information and Technology Bill, which the government expects will be addressing the current cybercrime gaps.⁴⁶

The existing legislation is inadequate in number of ways. Some of the most common forms of the cybercrime are not covered by the law. For example, there is not the definition of the cybercrime, no punishment exist for sending offensive message. Second the cybersquatting does not come under Nepal's cyber laws. Similarly, the act of electronically obtaining information for financial or personal benefit lacks legal coverage. The law is not adequate enough for the holistic depiction of cyber related crime and is not tough to act as a deterrent for online perpetrators. The imprisonment and fine determined under the Act are not high enough.

Though the cyber law is present but due to lack of proper monitoring and updates it serves little use in protecting users online. Internet provides easy accessibility and other facilities but at the same technology also threatens the nation in lack of proper mechanism and policies which needs to be researched and worked on. There have been many cases of cyberattack to people as the cyber stalking and hacking have been reported. Many of them are either put in other criminal proceeding and till now very few cases have been registered under this Act. It has not given definition about stalking, hacking, child pornography etc. So it is difficult to give decision by the court in this type of cases.

There is tribunal of three people headed by judge to look at cybercrime on the act. It has not been established but cases are heard in district court and appellate court. Sec 60, 61 of

⁴⁴ Anjan Neupane and Saurav Karki, Introduction To The Privacy Act 2018.

⁴⁵ Anjan Neupane and Saurav Karki, Introduction To The Privacy Act 2018.

⁴⁶ Available at <https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher.> Accessed on 4/15/2022.

the ETA, has mention about the formation of the district level and appellate level tribunal and in the tribunal of three people were the crime related to cyber can be filed , investigated but yet the cases are filed to the Metropolitan Police Crime division and the district court adjudicate it. It also has not mentioned how many tribunals to be made in the district. The law has not precisely covered all part of the cybercrime. The law covers only cyber fraud, computer related crime but it has not covered the other types of cybercrime like child pornography, phishing, spamming and so on.

There are many cases filed in the Metropolitan Police Crime Division but most of the cases filed were about the misuse and crisis related on the facebook and porn sites.

This current cyber law has failed to address many problems. The biggest hindrance to cybercrime prosecution is weak law enforcement. Although the present Act does touch on a few important issues the enforcement part is minimal. First both the police and judiciary have not develop sophisticated tools to investigate cybercrime. At present there are only two units to deal with the cybercrime- the cyber investigation cell at Hanuman Dhoka and the Central Investigation Bureau. But even when cybercrime cell discovers a fake account it can only block the account because Neplai law does not allow access to user's IP address. The law enforcement officials cannot effectively pursue cybercriminals unless they have the legal tools necessary to do so. These legal tools include an arsenal of well-defined cybercrime offenses for use in prosecuting cybercriminals and procedural rules governing evidence-gathering and investigation. Because cybercrime is often transnational in character, offenders can take advantage of gaps in existing law to avoid apprehension and/or prosecution. It is, therefore, important that every legal system take measures to ensure that its penal and procedural law is adequate to meet the challenges posed by cybercrimes and protect the right to privacy.

So with the growing popularity of networking sites the problem is likely to aggravate day by day. Besides enhancing our probe mechanism, we need to also focus on the increasing public awareness of the matter. They should be rigorous in evaluating the legal system's existing ability to deal with cybercrime, but they should be conservative in taking steps to improve that ability.

6. Judicial Trends on Right to Privacy

This section includes the analysis of the decisions of the Supreme Court of Nepal on right to privacy. The Supreme Court of Nepal has decided several cases on right to privacy and has established the principle that right to privacy is the fundamental right. Few of them have been analysed here. However, so far I have in my knowledge, no case has been decided by the Supreme Court of Nepal related to social media. Therefore, no cases related to social media has been analysed here.

*Annapurna Rana v. Gorak Shamsher JB Rana*⁴⁷

The first case on right to privacy decided by the Supreme Court of Nepal after the promulgation of the Constitution of Nepal 1990 is *Annapurna Rana's* case. The precedent setting ruling of the Supreme Court came in the context of a petition filed with the apex court by Annapurna Rana the granddaughter of late Keshar Sumshere Rana, in which she claimed that a Kathmandu District Court ruling directing a virginity test on her was unconstitutional and against her right to privacy enshrined as a fundamental right under Article 22 of the *Constitution of the Kingdom of Nepal, 1990*. The apex court overturned the order for the virginity test passed by the district court.

The Supreme Court of Nepal said, in an elaborate ruling, that a woman living with a man and maintaining a physical relationship with him need not necessarily be his wife. Making a detailed ruling on an aspect of right to privacy of a woman in a case involving a bitter property feud between a mother and a daughter of a prominent Keshar Sumshere family, the apex court ruled that living together and even bearing a child are not sufficient conditions in themselves to declare the two men (sic) and wife.

*Baburam Aryal v. GON*⁴⁸

The Supreme Court laid down that the right to privacy guaranteed by the Constitution is a fundamental right that may not be violated by the State or third parties. The Supreme Court further ruled that under the right to privacy, matters relating to a person's body, residence, property, documentation, data, communications, and character are inviolable, except as permitted by the law. An organisation or department that collects information and has undertaken the responsibility of such information must not use such information at its discretion. Instead, such an organisation or department must protect such a 'data bank' of information at any cost. The Supreme Court further laid down that such an organisation or department must not allow unauthorised access to such a data bank, even as an exception in the absence of a clear legal basis.

*Sapana Pradhan Malla v. Office of the Prime Minister and Council of Ministers et. al.*⁴⁹

The Supreme Court held that the right to privacy guaranteed by the Constitution must be protected. An exception to this general principle is that information relating to a person may be shared with third parties only in cases where prior consent from the concerned person has been obtained.

⁴⁷ NKP 2055 (1998) 476.

⁴⁸ NKP 2074 (2017), 25.

⁴⁹ NKP 2064 (2008), 1208.

*Sunil Babu Pant v. Nepal Government*⁵⁰

In this case, the Supreme Court of Nepal extended several fundamental rights, including the right to privacy to lesbian, gay, bisexual, transsexual/transgender and intersexual (LGBTI) persons/communities.

The petitioners, representing the LGBTI community in Nepal, filed a writ petition before the Court alleging discrimination and non-recognition of the preferred genders in the LGBTI community. They sought a direction from the Court requiring the State to put in place a legal framework for the protection of their rights and issue legal documents including birth certificates, citizenship certificates, passports, voter identity cards, etc. that recognized their preferred genders.

The Court held that the LGBTI community in Nepal was entitled to equal protection and rights under the various provisions of the Constitution as well as the international conventions that Nepal had entered into. Specifically, it held that the gender identity and sexual orientation of an individual fell within the ambit of their right to privacy and thus could not be interfered with. It condemned the societal perception that cohabitation between homosexuals and the third gender was unnatural. It noted that choosing a partner was an exercise of the right to self-determination, and this right was equally granted to LGBTI individuals as was granted to heterosexuals.

The Court held that right to privacy is a fundamental rights of an individual. The issue of sexual activity falls under the definition of privacy. No one has the right to question how two adults perform sexual intercourse and whether this intercourse is natural or unnatural. The Court directed the setting up of a Committee to undertake a study on securing the rights of these minorities and directed the State to enact appropriate legal provisions on receiving the Committee's recommendations.

7. Conclusion

It can be concluded that much needs to be done in the arena of the interface of social media and the right to privacy. There is an urgent need for the development of a unique and comprehensive statute encompassing this arena in Nepal. Also, the present statutes, that is, the *Privacy Act 2018* and *ETA 2008* have to be widened, explaining in greater detail, issues related to privacy and social media. Most importantly a wider definition of privacy is also to be adopted in this Act. There is also a need for proper implementation of guidelines issued by the Supreme Court of Nepal in various cases related to privacy and social media. The jurisprudence of right to privacy is rich. It was developed by the Supreme Court of Nepal. However, their proper monitoring mechanism is lacking due to the lack of proper implementation of social media laws.

⁵⁰ Writ No. 914 of the year 2064 BS (2007 AD).

Similarly, right to privacy includes right to refuse food or even medication. An individual's right to refuse medical treatment or terminate his life and opt for euthanasia falls within the ambit of right to privacy. Privacy Act is silent on these matters.

The companies might sell the data of subscribers to the third parties. This is the reason why most of us receive emails or text messages or phones advertising a variety of products which are, at times, so foreign to our consumption patterns. Arguably, right to privacy includes right to receive or reject something. The unwarranted message from unknown companies is infringement on privacy. Nepali laws do not address these issues.

The extensive use of cyberspace but with poor internet literacy and lack of knowledge about digital hygiene is itself a challenge for us. Facebook and other social media know about our whereabouts, for example, the places we roam, the decisions we make or friends we make.

There are many cases related to cybercrime but the success rate of the solving of the problem is very minimal. It is therefore very important for every individual to be aware of these crimes and remain alert to avoid any loss. To ensure justice to the victims and punish the criminals, the judiciary has come up with some laws known as cyber laws. Hence, it is advisable to each and every individual to know these laws. Besides, the cybercrime cannot be simply called as a technological problem. Instead, it is an approach based problem because it is not the computers that are harming and attacking the organizations instead it is the humans who are exploiting the technology to cause the damage. Therefore, it is we who need to be alert to figure out the different approaches that such criminals can take. There is a need to have intellectual mindset to sense such situation that may lead to such damages.

The solution to such crimes cannot be simply based on the technology. The technologies can just be one such weapon to track and put a break to such activities to some extent.

Legislators face the need to balance the competing interests between individual rights, such as privacy and free speech, and the need to protect the integrity of the world's public and private networks.

It's a well-known saying that "Prevention is always better than cure", therefore, it is always better to take certain precaution beforehand rather than regretting afterwards. Educating the people about the dangers of cybercrime and giving it more publicity will best determine addressing the problem. Immediately engaging expert assistance to check loopholes in systems regularly, particularly for large organisations and the government, will protect the security of systems. The government with the industry and individuals will improve their understanding of the law for a comprehensive approach to security management. This will assist in identifying gaps in the law.

The branch office of the social networking sites such as facebook, twitter, yahoo needs to be established in every country so that the victim can get the information about the perpetrator. The government must create special interest groups to address various information security aspects. These groups can function as 'watchdogs'. Also, they can be used to train others to 'enhance response capabilities'.

Nepal deserves to sanctify domestic life by cherishing right to privacy and considering it as an inherent part of right to life and liberty clause embedded in the constitution. It must not be curtailed by fresh law on Information and Technology. Every state action should be based upon a legislative mandate which serves legitimate state purpose and the law so designed to restrict privacy must be proportionate.

DATA PROTECTION RIGHTS IN INDIA: TIME TO ADD HABEAS DATA WRIT IN INDIAN CONSTITUTION

Dr. Vishal Guleria & Dr. Harish Verma***

Abstract

Data protection has become a serious concern worldwide, including India. The personal data in the hands of the data processors is always at risk of being misused, breached and leaked. Numerous countries and jurisdictions of the world have already enacted laws, rules, directives and regulations to protect personal data rights. However, in India till date, there is no precise law on the protection of the personal data of individuals. In the absence of a precise statutory mechanism on data protection, it is a correct time to add the Habeas data writ as a Constitutional right within Indian Constitution. The inclusion of the Habeas data action will offer prompt and summary procedures to redress the cases of violations of personal data rights in India.

In this backdrop, the present study has been undertaken to analyse the existing Constitutional and legal protections available to defend right to privacy and data protection in India. Also, Indian PDP Bill, 2018 will be compared with the EU's GDPR to see to what extent the best data protection practices of the GDPR have been incorporated in the PDP Bill. Further, the study will examine the concept and efficaciousness of the writ of habeas data available in the Constitution of some of the countries and jurisdictions of the world to protect privacy right and personal data of people. The paper will also study the need and benefits of the inclusion of the writ of habeas data in Indian Constitution and its adequacy to safeguard data security issues. What should be the sketch of the writ, if included, in the Constitution has also been drawn and presented by the researchers in this study. The study is purely theoretical in nature, therefore, secondary data has been consulted to complete the study and to draw the inferences and conclusions.

Keywords: *Personal data, Protection, Privacy, Laws, Writ, Habeas data, Rights.*

* Assistant Professor, School of Law, HNB Garhwal (Central) University, Uttarakhand.
** Principal, Jagran School of Law, Selaqui, Dehradun (Uttarakhand).

I. Introduction

Data protection is a matter of serious concern worldwide, including India. It has become evident from several studies¹ conducted in the past in the area of data protection that when personal data gets converted from physical form to digital form, risks of data security triggers. The problem of data security and violations of personal data rights has become common in all countries. India is also not far behind in matters of personal data rights violation incidents. Data security violations are on rise in India raising a question mark relating to the tall claims made by the government of India to enact strong personal data protection laws and rules. In the era of technology, it is responsibility of the government to guarantee the right to privacy and maintain confidentiality of the information stored with data users and service providers. There have been judicial decisions² in which courts have dealt with the right to privacy and issues associated with it. In addition to judicial creativity declaring right to privacy as a part of Art. 21 of the Indian Constitution, there have been indirect general laws³ in context of right to privacy and data protection in India. The International standards⁴, guidelines⁵ and privacy codes⁶ are also recognising right to the privacy⁷. However, the Government of India has been slow in responding to enact a specific law to protect personal data of individuals.

¹ Subashree Anantaraman and R. Krishnaraj, "Insiders Triggered Dangers to Data Protection-An Empirical Study," 16 *Indian Journal of Economics and Business* 341-54 (2017); Also see, Vivek Kumar Tygi, "Legal Off shoring Industry and Data Privacy: Global Perspectives(With Special Reference to India)," LXXIV *The Indian Journal of Political Science* 517-32(2013).

² *M.P. Sharma and Ors. v. Satish Chandra, District Magistrate, Delhi*, 1954 SCR 1077; *Kharak Singh v. U.P.*, AIR 1963 SC 1295, (1964)1 SCR 334; *Govind v. State of M.P.* (1975)2 SCC 148; *R. Rajagopal and Anr. v. State of Tamil Nadu* (1994)6 SCC 632; *People's Union for Civil Liberties v. Union of India*, (1997)1 SCC 301; *Selvi v. State of Karnataka*, AIR 2010 SC 1974; *K.S Puttaswamy v. Union of India* (2015)8 SCC 735.

³ See, *The Contract Act, 1872, Indian Penal Code, 1860, The Indian Copyright Act, 1957, The Information Technology Act, 2000, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 and The Credit Information Companies Regulation Act, 2015.*

⁴ See, *Universal Declaration of Human Rights, 1948, International Covenant on Civil and Political Rights, 1966, Convention on the Rights of the Child, 1989, International Convention on the Protection of the Rights of all Migrant Workers and Members of their Families, 1990, European Convention for the Protection of Human Rights and Fundamental Freedoms, 1950, American Convention on the Human Rights, 1978, African Charters on the Rights and Welfare of the Child, 1990 and U.N Special Rapporteur on the Right to Privacy, 2021.* Also see, Marcin Rojszczak, "Does Global Scope Guarantee Effectiveness? Searching for a New Legal Standard for Privacy Protection in Cyberspace" 29 *Information and Communications Technology Law* 22-24(2020); also see, Kristian P. Humble, "International Law, Surveillance and the Protection of Privacy", *The International Journal of Human Rights: Available at* <https://doi.org/10.1080/13642987.2020.1763315>.

⁵ OECD Guidelines on the *Protection of Privacy and Trans Border Flows of Personal Data* 1980; For details see also, Kamlesh Bajaj, "Promoting Data Protection Standards through Contract: The Case of the Data Security Council of India", 29 *Review of Policy Research* (2012).

⁶ See, *Canadian Model Code for the Protection of Personal Information, 1995*; Cloud Security Alliance Model Code.

⁷ Kristian P. Humble, "International law, Surveillance and the Protection of Privacy," *The International Journal of Human Rights* (2020) available at: <https://doi.org/10.1080/13642987.2020.1763315>.

The enactment of an omnibus piece of law on data protection seems a distant dream in a country which has been a strong supporter and signatory of plethora of International human rights instruments. In absence of the explicit personal data protection law, an inclusion of the Habeas data writ in Indian Constitution seems to be a viable solution in area of data security issues.

The present paper has VII parts. Part II of the paper covers constitutional protections and statutory framework that is indirectly useful in context of defending right to privacy and rights of the data subjects. Part III analyses the provisions of European Union (EU) Directives and EU's General Data Protection Regulation, 2018 (GDPR). Next Part of the article is devoted to Personal Data Protection Bill, 2018 (PDP, Bill) drafted by Government of India that provides protection against misuse of data. In this part, provisions of the PDP Bill have been discussed with special emphasis on personal data rights of the individuals. This part also presents a comparative analysis of Indian PDP, Bill, 2018 and EU's GDPR, 2018 to find what rights are available to individuals and what not under both the laws. Part V discusses the framework of writ of the habeas data in context of constitutions of some of the countries and jurisdictions worldwide to gain clear understanding of the habeas data action. Subsequent, Part VI being the main edifice of the present study aims to analyses the need, benefits and efficacy of the inclusion of the writ of habeas data in Indian Constitution. The researchers have drawn the sketch of the writ of habeas data in this part to see how in absence of specific law on personal data protection, the habeas data action can be a viable solution to address the data security issues and rights in India. Last part is dedicated to conclusions and recommendations.

A) Rationale of the Study

In India, the existing *Information Technology Act*, 2000 (IT, Act) and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011 (IT Rules) have some of the provisions that afford protection to informational rights of the individuals. However, the IT Act and IT Rules are neither adequate nor implemented in effective way in India, compelling the govt. of India to draft Personal Data Protection Bill, (PDP Bill) 2018. The said Bill aimed to secure personal data of the individuals in more effective manner. It was revised in 2019 and certain changes have again been proposed in it. The Bill of 2019 is pending before Joint Parliamentary Committee (JPC) and awaiting its final approval from there. Thus, till date a comprehensive specific law on personal data is missing from Indian statute book. Under such a scenario, the habeas data writ to protect personal data can be a workable solution in India to address the data protection rights of the individuals. As such, the present study has been undertaken to know the need, benefits and efficacy of the inclusion of the writ of habeas data in Indian Constitution.

B) Research Problem

Ubi Jus Ibi Remedium means that rights must have remedies⁸. But in context of the data protection rights, there is no explicit mechanism in Indian Constitution to provide the constitutional remedy. Habeas data writ has not yet been recognised as a Constitutional remedy in India. Also, a definite legislation till date has not been enacted relating to protection of personal data.

C) Research Questions

The present study aims to address the following research questions.

1. Whether existing constitutional protection on right to privacy and statutory mechanism on protection of personal data of individuals are adequate in India?
2. Whether Indian PDP Bill, 2018 is analogous to the EU's GDPR, 2018 with respect to protection of personal data rights of the individuals?
3. Whether in absence of all-inclusive personal data protection law in India, the inclusion of the writ of the habeas data in Indian constitution would be a viable solution?

Keeping in view of the above cited research questions, the present study has been worded as: "Data Protection Rights in India: Time to add Habeas Data Writ in Indian Constitution".

D) Objectives

1. To study and examine Constitutional protections, existing laws, rules and proposed DP Bill, 2018 on data protection rights in India.
2. To compare available personal data rights of individuals given in PDP Bill, 2018 with EU's GDPR model, 2018.
3. To study the meaning, concept and provisions relating to the habeas data writ or action available in some of the countries and jurisdictions of the World to gain complete understanding about the writ.
4. To study the need and benefits of the inclusion of the habeas data writ in Indian Constitution and its adequacy to protect personal data rights of the individuals.

E) Research Methodology

The present study is purely doctrinal in nature, hence secondary sources like books, law journals, periodicals, government reports, law magazines and websites will be relied upon to complete the study.

⁸ Tracy A. Thomas, "Ubi Jus Ibi Remedium: The Fundamental Right to a Remedy under Due Process," 41 San Diego Law Review 1633-45(2004).

II. Regulatory Framework on Protection of Data Rights in India

There have been several Constitutional protections and indirect laws in place to guard right to privacy in India. Some of them are as follows:

(A) Constitutional Protection

Indian Constitution does not contain any direct provision relating to protection of personal data rights of individuals. However, Art. 21 and Art. 19 have been relevant in area of defending right to privacy. The Apex Court and High Court judgements in India elaborated right to life to include personal and family privacy. For example, in *Kharak Singh v. State of UP*⁹, the minority opinion was in favour of right to privacy. According to minority opinion of judges in this case, the surveillance by domiciliary visits at night against an accused was treated against right to life guaranteed under Indian Constitution. Again in, *R. Rajagopal and Anr. v. State of Tamil Nadu*¹⁰, the right to privacy was considered implicit into the right to life and liberty guaranteed to the citizens by Article 21. Also in, *People's Union for Civil Liberties v. Union of India*¹¹, the Apex Court expressed no hesitancy in holding that right to privacy was a part of the right to life and personal liberty given under Article 21.

In recent judgement of the Apex Court delivered in *K.S. Puttaswamy v. Union of India*¹², informational privacy was considered a significant right. In this case, the Supreme Court got an opportunity to deal with an issue of personal data of individuals.

The Court was deciding the issue of the constitutionality of the *Adhaar Card Act, 2016*. The Court in this case extensively dealt with the issue of collection and compilation of the demographic and biometric data of the inhabitants of the country under the scheme. No doubt, the Court justified collecting and compiling of the data of the beneficiaries under this scheme but at the same time also stressed on the need of preservation of personal data of the individuals and favoured to impose a bar on the data sharing with the private entities. Thus, as per the Court's judgement in this case, the State can use the biometric data of individuals for the purposes to avail social services proposed to be provided by public sector. The Supreme Court clearly struck down the accessibility of private entities to *Aadhar* data.

Thus, the above judgements indicate that the constitutional right to privacy and protection of personal data has been strongly enforced by the Supreme Court and the High Courts. The Indian Judiciary irrespective of the profile of the individual accorded primacy to the right to privacy of all. The accused as well as common men have been treated equal in matter of availing privacy and informational right.

⁹ (1964)1SCR 334.

¹⁰ (1994)6 SCC 632.

¹¹ (1997)1 SCC 301.

¹² (2015) 8 SCC 735.

(B) A Protection under General Laws

The Information Technology (IT) Act and Information Technology Rules have been the main legal mechanism to deal with protection of data in India¹³. Under these laws 'personal information' and 'sensitive personal data or information'¹⁴ is protected. Both of the laws, however protected limited categories of information. Section 43(a), (b) and (i)¹⁵, 43A¹⁶ and 66 C¹⁷ of the IT Act are some of the key provisions dealing with personal data protection and punishment and fine for their breach.

However, this Act has several loopholes also. For example, under the Act the term 'sensitive personal data or information' does not include that information which is easily available in public sphere¹⁸. The Act only deals with the collection and dissemination of information by a body corporate. Even, under the amended *IT Act, 2008* cybercrime is a bailable offence. The quantum of punishment has also been reduced and fine increased in 2008 amendments in IT law. But steps to reduce punishment and increase fine have eliminated the deterrents from the IT Act¹⁹. Also, a lot of service providers are companies situated outside the territorial boundaries of India and therefore, are not required to follow the mandate of the IT Act.

Prior to IT Act and Rules, there have been several other laws²⁰ indirectly relevant to

¹³ For details on the IT Act, 2000 and IT Rules, 2011 see, Dhiraj R. Duraiswami, "Privacy and Data Protection in India," *6 Journal of Law and Cyber Warfare* 170-79 (2017).

¹⁴ Under the IT Act and IT Rules "Personal information and 'Sensitive personal data or information' means information related to (i) password (ii) Financial information such as bank account or credit card or debit card or other payment instrument details (iii) Physical, physiological and mental health condition (iv) Sexual orientation (v) Medical records and History and (vi) Biometric information".

¹⁵ It provides that "any person, who without the permission of the owner or, any other person who may be in charge of a computer, computer system or computer network-(a) accesses or secures access to such computer, computer system or computer network (b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network which includes information or data held or stored in any removal storage medium (c) steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage shall be liable to pay damages by way of compensation not exceeding the sum of INR rupees one crore to the person affected".

¹⁶ Section 43-A of the IT Act provides "Where a body corporate possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing the maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, which shall not exceed a sum of INR 5, 00, 00,000 (Rs.5 crore)".

¹⁷ Section 66C provides "Whoever, fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification features or any other person shall be punished with imprisonment for the term which may extend up to 3 years and shall also be liable to pay a fine of up to INR 1,00,000 (Rs. In lakh)".

¹⁸ See, "Data Protection and Privacy Issues in India" *Economic Laws Practice* 11 (2017).

¹⁹ *India's IT Act 2000 a Toothless Tiger?* Available at: www.csoonline.com (visited on 20 Feb. 2022).

²⁰ *IPC, 1860, Indian Contract Act, 1872, Indian Telegraph Act, 1885, The Indian Copyright Act, 1957, The Special Relief Act, 1963, The Public Financial Institutions Act, 1983, The Consumer Protection Act, 1986 and Credit Information Companies Regulation Act, 2005*. For details on these laws see, Sheshadri Chatterjee, "Is Data Privacy a Fundamental Right in India? An Analysis and Recommendations from Policy and Legal Perspective," *International Journal of Law and Management* (2018). Available at: <https://doi.org/10.1108/IJLMA-01-2018-0013>.

address the privacy and data security issues. Having general laws in place to protect personal data and privacy do not expect from the law implementing authorities to use them in deterrent manner, hence permanent direct law on data protection is vital in India.

III. Regulatory Framework of European Union (EU) Countries on Protection of Data Rights

Data protection has been vital in EU countries since nineties. Several initiatives have been undertaken in EU countries to afford protection to personal data but GDPR, 2018 has been one of most significant personal data protection regulation there. This EU's model on data protection has been adopted subsequently by number of countries across the World. Normally, the evolution of data protection framework in EU countries begins with enactment of EU's directives of 1995.

A) Protection under EU's Directives, 1995

The Data Protection Directive is a European Union Directive²¹. The EU's Directives were written to the member states and put obligations on them to bring laws in their respective countries in line with these directives²². EU's Directive of 1995 controls the processing of personal data within the EU. Under the EU's Directive, several data rights had given namely, notice to individuals to collect their data, purpose for which the data of the individual have been collected, consent of individual before sharing their data, security to collected data, information to data subjects regarding disclosure of their data, right of individuals to access their data and correction of personal data etc²³.

B) Protection under EU's GDPR, 2018

European Data Directive was found inadequate to address all personal data security issues hence, replaced with EU's GDPR, 2018. The GDPR has several noteworthy provisions for the data protection. At the outset, the GDPR defines several prominent terms

²¹ The Data Protection Directive has been adopted in 1995 by the European Union. Officially, it is known as Directive 95/46/EC. This Directive is made by European Parliament and Council on 24 Oct. 1995. They came into force on 13 December 1995 and implemented on 24 Oct. 1998.

²² Andres Guadamuz, "*Habeas Data v. the European Data Protection Directive*," 3 JILT (2001) available at: <http://elj.warwick.ac.uk/jilt/01-3/guadamuz.html>.

²³ For details on rights mentioned in EU Directive see, "What is the Data Protection Directive? The Predecessor to the GDPR" Available at: <https://digitalguardian.com> (visited on 20 Feb., 2022).

like 'personal data'²⁴, 'processing'²⁵, 'controller'²⁶, 'processor'²⁷, 'personal data breach'²⁸, 'genetic data'²⁹ and 'data regarding health'³⁰ etc.

If one goes through the definition of the term 'personal data' one can see that the public and non-sensitive information relating to data subjects falls within the ambit of 'personal data'³¹. It indicates the scope of the GDPR is broad. Also, collecting, storing, disclosing and erasing data of data subjects comes within the purview of the term processing under the GDPR.

Further, the term 'processor' under the GDPR includes natural and artificial entities like data centre or cloud provider³². These entities can be held accountable for violation of privacy laws, standards, and guidelines relating to data rights of individuals. Again, the word 'controller' includes natural (data subjects) or legal person like companies. The GDPR places the burden of responsibility on 'controller' to decide the purposes and the means of dispensation of personal data. Thus, the definitional or opening part of the GDPR indicates the toughness of the EU's model on data protection as all terms are significant from the point of view of the data security.

Further, the GDPR has a provision to exercise control over personal data if it moves outside the EU's jurisdictions. It shows that GDPR is stern to address the problems that often come when personal data crosses borders. Certain exceptions have also been mentioned under GDPR where data relating to personal or household activities, national security issues and prevention and prosecution of criminal offences cannot be disclosed.

The GDPR specifies following principles for the legitimate handling of personal data³³.

²⁴ Article 4(1) of the GDPR, 2018 says "Personal data' means 'any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic cultural or social identity of that natural person".

²⁵ Article 4(2) of the GDPR, 2018 says "Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alternation, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".

²⁶ The GDPR, 2018, art. 4(7).

²⁷ Id., art.4(8).

²⁸ Id., art. 4(12).

²⁹ Id., art. 4(13).

³⁰ Id., art. 4(15).

³¹ Chris Jay Hoofnagie, Bar van Der Sloot and Frederik Zuiderveen Borgesius, "The European Union General Data Protection Regulation: What it is and What it means," *Information and Communications Technology Law* 8 (2019) available at <https://doi.org/10.1080/13600834.2019.1573501>.

³² A cloud service is any system that provides on demand availability of computer system resources e.g. data storage and computing power, without direct active management by the user.

³³ Available at: <https://www.uhi.ac.uk> (visited on 21 Feb., 2022).

1. Lawful, Fairness and Transparency³⁴ - Personal data shall be handled in legal, fair and transparent manner.
2. Purpose Limitation³⁵ -Personal data shall be collected for legitimate purposes and after use; the data processed should be deleted. However, processing for archiving in the public interest, scientific or historical and statistical researches shall be allowed.
3. Data Minimisation³⁶ - Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. Accuracy³⁷ - Personal data shall be accurate. It should be kept up to date. Inaccurate data shall be erased or rectified without delay.
5. Storage Limitation³⁸ - Personal data shall be kept stored for a limited period. The storage of personal data for a longer period is allowed only for archiving purposes in the public interest or for research purposes. After use, the personal data should be erased.
6. Integrity and Confidentiality³⁹ -Personal data shall be kept fully secured and confidential. Collected data should not come into the public domain. It must be protected against loss, destruction, damage and unlawful processing. In order to ensure protection to data, the data users or controllers shall be under obligations to check unauthorised use of data.
7. Accountability⁴⁰ -The Controller, data fiduciaries and data users shall be responsible for protection of personal data. Data Controllers are answerable for observing these principles.

The above principles of the GDPR points out that these are fundamental to ensure good data protection regime in EU's countries. Principles are specific, clear and subject to limited exceptions. They inform everything that is required to be done to protect personal data of the individuals. Besides principles, individuals are entitled to enjoy following rights under the GDPR⁴¹.

³⁴ The GDPR, 2018, art. 5(1)(a).

³⁵ Id., art. 5(1)(b).

³⁶ Id., art. 5(1)(c).

³⁷ Id., art. 5(1)(d).

³⁸ Id., art. 5(1)(e).

³⁹ Id., art. 5(1)(f).

⁴⁰ Id., art. 5(2).

⁴¹ The GDPR, 2018 defines data subject rights in arts. 15-22. For details on data subject rights see "Data subject rights and Personal Information: Data Subject Rights under the GDPR". Available at: <https://www.i-scoop.eu> (visited on 22 Feb., 2022).

1. Right to Request Access to Personal data⁴² - This is significant data related right of an individual. It means that the data subjects shall have the right to know about the processing of their data. The data subject can access his or her personal data.
2. Right to Rectification⁴³ -Right to rectify or correct personal data is another right recognised under GDPR. This right is available, if personal data has been entered wrongly by the data users in registers. The Controller has responsibility to correct the inaccurate data.
3. Right to Erasure or Right to be Forgotten⁴⁴ - As per this provision, data subject can ask for erasure of his or her previously mentioned/used data. Data subjects shall have a right to ask to delete personal data which data subjects no longer want to be processed. The companies or data users, then, shall have no legitimate reason to retain personal data.
4. Right to Restriction of Processing⁴⁵ -It means that citizens shall have a right to restrict processing of their personal data.
5. The Right to be Informed⁴⁶ -According to this right, the Controllers or Data processors shall have obligations to provide clear and correct information to the data subject about his or her personal data with them. If one person wants to receive personal data of another person, then the controller must inform the recipient of data (in this case the former person) who got personal data of any individual, where feasible. Also, the data subject has a right to ask or make inquiries about the recipients who are interested in procuring data of the data subject.
6. The Right to Data Portability⁴⁷ - Under this right, the data controller will provide and transmit personal data to data subject in structured form or machine readable form. The provided personal data by the data controller in a format makes it easier for the data subject to reuse the information in another context.
7. Right to Object⁴⁹ -It means that the data subjects can say that they do not want the personal data processing to be done. Thus, giving importance to right of say to the individual is significant under GDPR.

⁴² The GDPR, 2018, art. 15.

⁴³ Id., art. 16.

⁴⁴ Id., art. 17.

⁴⁵ Id., art. 18.

⁴⁶ Id., art. 19.

⁴⁷ Id., art. 20.

⁴⁸ Data is structured and machine-readable if it can be easily processed by a computer.

⁴⁹ The GDPR, 2018, art. 21.

8. Right of Automated decision making⁵⁰-It means that one should not base a decision solely on automated means, including profiling, which produces legal or similar effects.

These above mentioned rights of the data subjects are fundamental and core provisions of the GDPR. It is therefore, expected from any government to follow GDPR while drafting new data protection law.

VI. New Proposed Legislation on Data Protection in India

A) Evolution of New Data Protection Law

To prevent possible violation of personal data rights of individuals, the PDP Bill had been brought into existence in 2018. It remained pending in Parliament for a long time and certain changes had also been suggested in it in 2019⁵¹. The PDP Bill now is pending before JPC which has accorded approval to it in Dec. 2021. The approval from JPC is a noteworthy step towards changing India into an active and strong data economy⁵².

B) Some Provisions of the PDP, Bill

There are several features of the PDP, Bill. The Bill provides a strong basis for maintaining the privacy of the data of individuals. The 'data fiduciary' has been given responsibility to handle private data of the individuals under the Bill⁵³. The Bill is applicable to govern the processing of personal data by government, companies, and foreign companies⁵⁴. The Bill in its section 3 defines several key terms like 'Biometric data' 'Personal data' 'Personal data breach' 'Data Principal' 'Data Fiduciary' 'Data processor' and 'Profiling'. The meanings of these terms are almost same as stated in EU's GDPR earlier under this study. Like EU's GDPR, the PDP Bill also sets out certain principles⁵⁵ like prohibition on processing of personal data, limitation on purpose of processing and collection of personal data and requirement of notice for collection or processing of personal data. However, the bill also specifies certain grounds for processing of personal data without consent of data principal⁵⁶.

Also, some rights have been guaranteed to individuals under the PDP, Bill. Those rights are also given under GDPR and hence their meanings have already been covered in details previously under present paper. Consequently, it would not be useful to repeat them in details here.

⁵⁰ Id., art. 22.

⁵¹ The DP, Bill 2019 was brought into Lok Sabha on 11th of Dec. 2019. From there, the Bill was referred to a Joint Parliamentary Committee for detailed examination.

⁵² S.D. Pradhan, "JPC Approves Personal Data Protection Bill, 2019: Crosses an Important Landmark," available at <https://timesofindia.indiatimes.com> (visited on 21 Feb., 2022).

⁵³ See, objectives of the Personal Data Protection Bill, 2019.

⁵⁴ The PDP Bill, 2019, sec. 2

⁵⁵ Id., sections 4-11.

⁵⁶ Id., secs. 12-15

C) Comparison of Individuals Rights between Indian PDP Bill and EU's GDPR

It is worthy to mention here that the GDPR is considered as one of the best models on personal data protection worldwide. The PDP Bill also matches with GDPR to some extent. The PDP Bill varies from the EU's GDPR with respect to the existence of the provisions connected to social media intermediaries and non-personal data. A clause for non-personal data is missing in EU's GDPR which is a major flaw in it. Similarly, the meaning of the term 'sensitive personal data' does not include financial data in the GDPR. But PDP Bill includes financial data also.

Further, in matters of availability of rights to data subjects within both laws, it seems that India still lags far behind in providing rights to individuals as compared with GDPR. The comparison of availability and non-availability of data rights to individuals in both laws is presented in **Table-1** below.

Table-1
Data Protection Rights in Indian PDP Bill and EU's GDPR ; A Comparison

Sr. No.	Name of Personal Data Rights	India's DP Bill	EU's GDPR
1	Right to Rectification of data errors	Available	Available
2	Right to Access to data	Available	Available
3	Right to withdraw consent	Not Available	Available
4	Right to be Forgotten	Available	Available
5	Right to be informed	Not Available	Not Available
6	Right to Data Portability	Available	Available
7	Right to Restriction of processing	Not Available	Available
8	Right to Object to processing	Not Available	Available
9	Right to Complain to relevant data protection authority	Not Available	Not Available
10	Right to Object to marketing	Not Available	Available

Source: Compiled by Researchers

Table-1 depicts that as compared to GDPR, less rights are available to data subjects under PDP Bill in India. Out of 10 rights specified in the table above, only 4 rights are available to data subjects under PDP Bill and in GDPR out of 10, 8 rights are available to EU's citizens. The rights missing in India under PDP Bill are right to withdraw consent, right to be informed, right to restriction of processing, right to object to processing, right to complain to relevant data protection authority and right to object to marketing. So far as the GDPR is concerned only two rights are not available under it namely, right to be informed and right to complain to relevant data protection authority. Such a scenario indicates that government of India has failed to adopt best personal data protection practices as mentioned in the EU's GDPR. At this juncture, inclusion of the habeas data writ in Indian Constitution has left out the only solution with govt. of India to address violation of data related rights.

V. Writ Framework on Protection of Personal Data Rights

A) Meaning and Concept of Habeas Data

The term 'habeas data writ means 'you should have the data'. Habeas data right is a constitutional remedy which is prescribed in some of the countries and jurisdictions across the World. This writ aims to protect personal law suit filed in court, to protect the image, privacy, honour, information self-determination and freedom of information of a person⁵⁷. Some of the studies have described writ as 'a procedure designed to safeguard individual's freedom from abuse in the information age'⁵⁸. This writ is available to citizens as a mechanism to assure control over sensible personal data.

The history and origin of the habeas data writ can be traced to certain European legal mechanism that protected privacy of the individual⁵⁹. The Council of Europe 108th Convention on Data Protection, 1981 is the predecessor of the habeas data right⁶⁰.

Thus, in general, the Habeas data writ can be filed by any citizen against any register⁶¹ to find out what information is held about his or her person. Aggrieved person whose data has been processed can request the correction, updating or even for the destruction of the personal data held by data users.

⁵⁷ See, <https://en.m.wikipedia.org> (visited on 24 Feb., 2022).

⁵⁸ Falcon, Enrique, "Habeas Data: Conceptoy Procedimiento(1996) Editorial Abeledo Perrot, Buenos Aires p.28.

⁵⁹ Andres Guadamuz, *supra* note 22.

⁶⁰ For details see, A. Charles "Recent Development in Latin America and Asia are Driven by Local Interests and Technology". Privacy and American Business (1998). Available online at: <http://Hudson.idt.net/pad/global.html>.

⁶¹ In general, register means "a register in which details are entered and kept by data users or companies why they are processing personal data. It includes information about the data subjects and personal data, as well as the categories of recipients (where applicable)".

B) World's Constitutions and Status of the Habeas Data

At international level, the habeas data writ or right has been adequately recognised in Constitutions⁶². In the following countries, the said writ is being used to protect personal data.

Brazil

Brazil has been the first country in which the Habeas data writ was used and recognised as a major safeguard to protect personal data rights of the individual. It was the first Latin American country to adopt the writ of habeas data in 1988.

The Constitution of the Federative Republic of Brazil, 1988⁶³ has specified the Habeas data action to cure the right to correction and access to the personal data of the data subjects. The Brazilian Constitution however does not offer any remedy, in case, the data users fail to update or destruct the data of the data subjects after use. In Brazil, the habeas data action can be presented before several authorities⁶⁴. For example, the Supreme Federal court is empowered to initiate legal proceeding, in case of habeas data writ against the acts of the President of the Republic, Directing Boards of the Chamber of Deputies and the Federal Senate, Federal Audit Court, Attorney General of the Republic and the Supreme Federal court itself. It shows that the power of the highest court of the Brazil to entertain writ is extensive and it covers multiple of authorities against whom writ can be initiated there.

Paraguay

The Constitution of the Paraguay, 1992, has a provision for the habeas data writ⁶⁵. The citizens in Paraguay have a right to access to information like Brazilian citizens. But as compared with the Brazilian Constitution, the scope of the writ is wider under Paraguay Constitution. Under the Constitution of Paraguay, the competent authority or court can secure updating, rectification or destruction of entries made in official or private registries of a public nature, if they are wrong or if they are illegitimately affecting rights of the data

⁶² For detailed discussion on Constitutional Rights to Habeas Data, see, Marc-Tizoc Gonzalez, "Habeas Data: Comparative Constitutional Interventions from Latin America against Neoliberal States of Insecurity and Surveillance" 90 Chicago-Kent Law Review 641-68(2015).

⁶³ Article 5. section LXXI provides that "Habeas data shall be granted (a) to ensure the knowledge of information related to the person of the petitioner, contained in records or data banks of government agencies or of agencies of a public character. (b) for the correction of data, when the petitioner, does not prefer to do so through a confidential process, either judicial or administrative". Details available online at: <https://www.globalhealthrights.org> (visited on 23 Feb., 2022).

⁶⁴ See, Title IV, Chapter III, sections II-IV of Brazilian Constitution, 1988.

⁶⁵ Art. 135 provides "All persons may access the information and the data that about themselves, or about their assets, (that) is (obren) in official or private registries of a public character, as well as to know the use made of the same and of their end. All persons may request before the competent magistrate the updating, the rectification or the destruction of these, if they were wrong or illegitimately affected their rights". Available online at: <https://www.constituteproject.org> (visited on 23 Feb., 2022).

subjects. However, under the Brazilian Constitution, there is no provision for updating and destruction or removal of data after use. Thus, Paraguay Constitution has offered more protection to citizens against violation of their data rights.

Argentina

The Argentine Republic Constitution, 1853 amended in 1994 has a provision for the writ of *amparo*.

The word 'Habeas data' is not specifically mentioned under the constitution because the Argentinean government had merged several individual constitutional complaints under the name of *amparo*⁶⁶. However, irrespective going into the controversy of nomenclature of the writ under Argentine Republic Constitution, it is crystal clear from the reading of section 43 of the Argentina Constitution⁶⁷ that personal data protection can be secured through prompt and summary proceeding, provided there is no other legal remedy. Under section 43 most of the rights of the data subjects like right to obtain information about personal data, their purpose, right to rectification and the right to suppression of false data are covered. The violations of these rights can be redressed by the competent courts. However, beside the rights protected under Paraguay and Brazilian Constitutions, the Argentinean Constitution also protects right of confidentiality of data and imposes prohibition to broadcast or transmit incorrect or false information by press. Thus, Argentinean Constitution is more liberal and wider in scope in matters of protecting data rights of individual as compared with Paraguay and Brazilian Constitutions.

Colombia

There is no explicit provision as such on habeas data in Colombian Constitution. But Colombian courts through various judgements have implanted the habeas data writ as a fundamental part of the Constitutional system there. The Colombian Constitution, 1991 has provisions relating to privacy and data of the individuals within it. The highest Colombian law has defended the individuals' right to know, right to access, right to update and rectify

⁶⁶ *Amparo* means shelter or protection. In Philippines, this writ is generally used to support the inadequacy of the writ of habeas corpus.

⁶⁷ The relevant portion extracted from the language of section 43 states that “Any person shall file this action to obtain information on the data about himself and their purpose, registered in public records or data bases, or in private ones intended to supply information; and in case of false data or discrimination, this action may be filed to request the suppression, rectification, confidentiality or updating of said data. The secret nature of the sources of the journalistic information shall not be impaired”.

⁶⁸ Article 15 states that “All individuals have the right to personal and family privacy and to their good reputation, and the State has to respect them and to make others respect them. Similarly, individuals have the right to know, update, and rectify information collected about them in data banks and in the records of public and private entities.” Article further states that “Freedom and the other guarantee approved in the Constitution shall be respected in the collection, processing and circulation of data. Correspondence and other forms of private communication may not be violated. They may only intercepted or recorded on the basis of a court order in cases and following the formalities established by Statute”.

personal data⁶⁸. According to the Colombian Constitution, the data banks of the public nature and private entities are under obligations to process personal data in an impartial manner.

Peru

New Peruvian Constitution, 1993 amended in 2021 has provided the habeas data action within its framework⁶⁹. Under the Constitution, the writ of habeas data operates in case of an act or omission. The writ lies against any authority, official or non-official that violates or threatens the rights of individuals. Under the Constitution, individuals have a right to request information⁷⁰ and right not to provide information affecting personal and family privacy⁷¹. Thus, the writ is a significant constitutional protection created under the Peruvian constitution.

In addition to the above countries and jurisdictions, the idea of the habeas data action is also debated and found reflection within the legal system and Constitutions of the Costa Rica and Philippines.

VI. Sketch of the Proposed Writ of Habeas Data in India

The violation of fundamental and statutory rights should not go unaddressed. But data rights of individuals are frequently violated and in absence of effective legal enforcement mechanism violation remain unnoticed most of the time. So, the habeas data writ can be incorporated in Indian Constitution. The researchers seem the inclusion of the writ of the habeas data in Indian Constitution as effective tool to address violation of data rights. But when one thinks to add the habeas data writ into Indian constitution, certain questions are likely to arise into mind such as: What would be the nature and scope of the writ? Against whom the writ would be maintainable? On what grounds it would be granted? And what would be the benefits of its inclusion in Indian Constitution? To answer these questions and to demonstrate how the habeas data writ might be useful to protect individuals' data rights, the researchers have drawn the sketch of the habeas data writ herein below.

A) Nature, Scope and Maintainability

In India, issuing of 'prerogative writs' is right of the Supreme Court and the High Courts. Part III of Indian Constitution deals with enforcement of fundamental rights. Article 32 empowers the Apex Court of India and Art. 226 permits High court of each State to entertain writs. Thus, both the above-mentioned courts would also be competent courts to issue the writ of the habeas data.

⁶⁹ Art. 200 sec. 3.

⁷⁰ Sec. 2 sub para 5 states that "Every person has a right to request, without statement of a cause, information he requires, and to receive it from public entity within the legal term, at its respective cost".

⁷¹ Sec.2 sub-para 6 states that "Every person has the right to the assurance that information service, whether computerised or not, whether public or private, will not provide information affecting personal and family privacy".

Further, the writ of habeas data like other writs⁷² in the Constitution would be maintainable against the 'State'. The term 'State' as defined in Art. 12 includes Central and State governments, local authorities, government departments and other instrumentalities. The term 'other instrumentality' has also been interpreted liberally to include several statutory and non-statutory corporations within the ambit of the 'State' under Art. 12.

If we look at the definition of the term 'State' under Art. 12 and interpretation of the term 'instrumentality or other authority' as done by courts, it becomes clear that government, companies, data principal and data fiduciaries in India would be held liable for violation of individuals' data rights as 'State' under Art. 12. Foreign companies located outside India, if are working in India through their branches or units, shall be accountable if they are dealing with processing of data. So, the writ would be maintainable against foreign companies as they would also come within the purview of 'State' under Art. 12.

Thus, the outline of the writ of the habeas data drawn above clearly indicates that various data users irrespective of their profile, working domain, nature and location can be treated 'State' under Art. 12 and hence the writ is maintainable and enforceable in case of violation of data rights in India.

B) Need and Benefits of Inclusion

After discussing the outline of the habeas data action, it becomes crystal clear that it would be an effective constitutional remedy to deal with data rights violations. The researchers point out the following justifications to include the writ as constitutional remedy in Indian Constitution.

Prompt and Summary Proceedings

The technique to file the habeas data writ is simple. In order to file it, no formality relating to producing of facts and proof are required. The procedure under Art. 32 and Art. 226 will be summary and prompt. Even letters, e-mails and postcards had been treated as writ petitions in the past. For example, in a case⁷³, a telegram was treated by Indian court as writ petition. It exhibits that even in violation of informational right to privacy, letter, postcard and e-mail can be treated as writ petition and the courts would not insist on the observance of procedural technicalities. The writ of the habeas data like other constitutional writs would be

⁷² Presently five writs are given in Indian Constitution which protects individuals' against different types of violation of fundamental rights. These writs are; Habeas Corpus, Mandamus, Certiorari, Prohibition and Quo warranto. For details on writs see, M.P. Jain, *The Law of Constitution in India* (Lexis Nexis Publication Pvt. Ltd. 11th edn., 2011).

⁷³ In case titled "*Chintakrindi Venkateswarlu v. Head Constable 6th Town Police, 1997 CriLJ 3319*, a telegram was sent by a father to the Chief Justice of the High Court alleging that his son was kidnapped and his whereabouts were not known and that he is apprehending danger to his son's life. This telegram was taken up as Writ petition under art. 226 of the Constitution of India and notices were issued to the concern.

entertained in the form of simple letters written and affidavits submitted. In event of other petitions, lower court can appoint commissions to confirm the genuineness of facts produced in any case which comes before it, follow whole procedural technicalities and record the evidence. But these all formalities are usually not used in matters of filing writ petitions.

Suo Motu Cognizance

Indian higher judiciary takes suo motu cognizance to enforce fundamental rights. The Apex Court or High courts can also take suo motu cognizance of the cases of violation of data rights of the individuals. So, if data rights are violated by data users, the Apex Court and High Court need not wait for a writ petition to be filed. Exercise of suo motu jurisdiction by courts is useful especially in case of flagrant abuse of law, disturbing the public. The courts while exercising suo motu jurisdiction will issue notices etc. to the respondents at their own level without help of other law enforcement agencies.

Enforcement of Rights by the Highest Court of the Country

On incorporation of the habeas data writ in Indian Constitution, there would be no need to introduce a separate judicial scheme and any separate government agency to enforce rights of the data subjects. The Supreme Court under Art. 32 and High Courts under Art. 226 would become automatically eligible to entertain the habeas data action. So, we have already separate judicial structures in place that can provide faster remedy to data subjects if their rights are violated. Individual studies⁷⁴ have already favoured the highest level of protection possible, and faster procedures and availability of better courts to enforce data rights of individuals. If specific data protection law came into being even then the habeas data action should be kept retained in Indian Constitution as its retaining would strengthen the enforcement of data rights.

No Time Limit to File Writ

Stale claims are not maintainable in courts. They are imperfect rights which cannot be enforced. But limitation period to file a writ is not mentioned hence inordinate delay in filing writ petition may be excused specially where any significant issue and question of fundamental right is found involved in a case. The Supreme Court has done it in the past. For example, in the case of *Narmada Bacho Andolan v. Union of India*⁷⁵ the Apex Court entertained delayed writ petition on the grounds that the issue of the violation of fundamental rights were involved. The court in this case refused to deal with other claims asserted by the petitioners on the ground of laches but partially allowed writ petition due to the reason of involving fundamental rights.

⁷⁴ *Habeas Data v. European Data Protection Directive* 3 JILT (2001).

⁷⁵ AIR 2000 SC 3751.

VII. Conclusions and Recommendations

A) Conclusions

The foregoing discussion makes it amply clear that the existing regulatory framework on privacy right and data protection is ineffective and flawed. The judicial efforts in evolving fundamental right to privacy and protection of personal data seem effective but it is not a permanent solution. The reason is clear that judiciary does not make laws unless a case comes before it for adjudication. Except in writ matter, the courts cannot exercise *suo motu* jurisdiction. The GDPR, 2018 applicable and followed in European member countries are the best regulations on personal data protection from which several other Latin American countries have taken lesson. The GDPR, 2018 afford protection to rights of data subjects. Several rights like right to access to data, right to correction, right to erasure, right to withdraw consent and right to be informed have been basic rights provided to data subjects under the GDPR. The PDP Bill has several notable provisions which are in line with best data protection practices followed globally but the problem is that this Bill is still pending before the JPC for approval. Even, if this Bill gets approved, even then the data protection will remain a significant issue as most of the laws in India remain in moribund like situation in absence of their proper implementation after enactment. There is likelihood that the PDP Bill, 2018 on becoming a law might not be implemented effectively and properly, especially in case where governments and influential companies are the data users. Moreover, the complicity and procedural technicalities usually seen in the Indian courts in enforcing ordinary rights is a major hurdle in hundred percent implementation of the PDP law. Under such circumstances, the researchers have proposed to add the writ of the habeas data in Indian Constitution so that procedural and other legal technicalities, normally experienced, in enforcing rights of the individuals can be subsided and rights of data subjects can be addressed via habeas data action filed in the highest court of the country.

The habeas data writ would be useful to promptly address the rights of the data subjects because all writ petitions are based on summary procedure and judges can also exercise *Suo moto* jurisdictions under Art.32 and Art. 226 of the Indian Constitution. There would be no time limit pressure to entertain the writ petitions and courts in the past have allowed writ petitions that have been filed after inordinate delay.

It is true that no legal system is free from defects so the habeas data action may be hampered if judges would not be techno savvy and burdened to dispose of backlog of cases. Few recommendations given below may be useful to strengthen the statutory mechanism on personal data protection in India. Also, recommendations have been given below how writ of the habeas data can be made effective if incorporated in Indian Constitution.

B) Recommendations

In fast emerging era of technology, all data rights of individuals are required to be protected. Government of India has to ponder over how to protect data rights of the data subjects. This part of the paper offers some recommendations for the law and policy enforcement agencies in India.

- The PDP Bill is pending before JPC. To provide statutory protection to rights of individuals, it is recommended to convert this bill into law at the earliest.
- Clause 9 of the PDP Bill imposes obligation on the data fiduciary to delete the data after use, but the procedure to delete data is not clearly specified. It is not notified clearly under the Bill how data principal would delete the data after its use. It is thus recommended that a proper procedure is required to be notified to data Principal how and when personal data can be deleted.
- Under the draft Bill neither the data fiduciary nor the Data Protection Authority (DPA) shall have any duty to inform the data subject about the breach of his or her personal data. However, the DPA can publish information about the data breaches on its website. The notification of data breaches on website may go unnoticed therefore, it is recommended to fix clear responsibility of the data fiduciary to inform data principal about breach of personal data. Also, publication of data breach on website may further expose the data principal to huge number of escapes of his or her personal data and its abuse. Hence this practice should be discontinued.
- A voluminous personal and sensitive data crosses Indian borders for the purpose of processing, storage and use. The Data Bill does not provide a strong enforcement mechanism to prevent it. Therefore, it is suggested that DPA need to appoint a team of separate data handling experts who can filter what data may or may not be allowed to be transferred cross border.
- Under the Draft Bill, governments' can access information of individuals in national interest. The term 'national interest' is not clearly defined in the PDP Bill. In absence of it, this term may be subject to different interpretation by governments. In the name of national interest governments' can reach to all sort of personal and sensitive information of individual. The unlimited reach to information by the governments can lead to exploitation of the personal data of the data principal. Therefore, it is recommended to clearly define the terms like national interest, national security and sensitive data within the Bill.
- The GDPR has the best data protection practices. But some of the rights stipulated within GDPR are not available in the PDP Bill. Therefore, it is

recommended to bring the Indian PDP Bill in line with the GDPR, 2018 to provide wider protection to individuals.

- It is recommended to amend Indian Constitution so that the writ of habeas data can be included in Indian Constitution under Art. 32 and Art. 226.
- It is also recommended to appoint more judges in the Indian higher judiciary so that the writ of habeas data may be decided promptly. Further, the backlog of variety of other cases before the higher judiciary may hamper disposal of the writ of habeas data so, appointing more judges will also be useful.
- Judges in India may not be well acquainted with data processing technicalities and associated problems. This can also hinder effective use of the writ to address data rights in India. In this context, it is recommended that special techno savvy staff can be appointed in Supreme Court and High Courts who can assist court in understanding the data security related issues. Further, judges should also be trained and made aware time to time about the changing data processing system.

DATA PROTECTION IN INDIA: HUMAN RIGHTS PERSPECTIVE

*Shobhna Jeet**

Abstract

Privacy which is probably the most essential element for the survival of mankind on this planet, is heard to be threatened these days in the name of “Procedure Established by Law” or “Public Duty” by the public servants. If we just wander for a second, that what will the situation of any person, if he/she doesn't have any privacy rights, which covers all the private rights including of family, workplace, relationships, etc. Privacy in simple sense, is as important as oxygen to a human body, it is the medium which actually ensures a peaceful life with dignity and liberty, which is the essence of Article 21 of our Indian Constitution. Gradually as our Country is moving towards Digitalization, it is not wrong to call it is a “Cyber Era”, with the increase in use of social media and Internet in various spheres, the Data Security and Data Protection, which constitutes a vital element in terms of privacy as your digital footprint, is a National Issue as well as National Obligation to ensure for. Data Protection and Privacy are fundamentally interlinked, and constitute a very crucial and most sensitive space in the legal world at present times. The Research Paper is prepared on analogical method of research, as due to spread of pandemic Covid-19, and its implied restrictions, the secondary sources are used in the paper for gathering the information and further converting the same into a precise piece of information.

Keywords: *Privacy, Rights, Data, Digital Foot prints, Cyber Era*

1. Introduction

In the cyber age, Information and Communication Technology (ICT) is benefitting billions across the world by bridging certain gaps and multiplying human potential in every walk of life. Digital services provision that is being developed for our society has enormous positive potential. The Internet has revolutionized the way businesses approach and conduct work. For consumers, the idea of purchasing online is appealing for several reasons. A well designed and implemented e-commerce system can lower transaction costs, reduce inefficiencies, promote better information flow, and encourage better co-operation between buyers and sellers. With little more than a click of a mouse, business can communicate,

* Associate Professor at IILM University, Gurgaon. I acknowledge my guide Prof. Satish C. Shastri for guiding and blessing me throughout my research work.

engage in commerce, and expand their business opportunities. At the same time, there are certain social, political, and economic implications being observed globally either in the form of 'spying websites' like 'wikileaks'¹ hacking activities or illegal decryption of data. The global character of digital space, internationally spread services, and the global development of social network sites go hand in hand with the emerging international crime networks raising serious challenges to the existing social, economic and political set up. There emerges a clash between personal development and economic prosperity, and sustained security of humans. The sustained security of human includes the protection of data. The citizens have trust in society and government to protect their peace, safety, security and prosperity. The advancement of information technology has raised various challenges before us to deal with such issues. As observed, the business, data and knowledge process outsourcing industries at global level have grown significantly in the last few years. But it also raised the concerns of data theft and misuse of private and personal information. To cope-up these problems, *The Data Protection act* has been enacted at international level like in United Kingdom (UK) the Data Protection Act 1998, Sectoral Legislation in USA, etc. However, India is lacking behind in formulation of separate legislation for protection of data². Data Protection means preventing the malicious or illegal disclosure of personal information. A person has right to know that for what purpose his data is compiled, and where it is transferred or transmitted. In all cases, the individual, government, or entity has to take the consent from respective person for using his or her data. In recent past, a growing number of cases have emerged related to the breach of privacy of human being in India. The present study is an attempt to have a brief glance of the data protection laws in the UK and USA. It also highlights the laws related to privacy of data in Indian statutes and draws policy lessons based on the experiences of UK and USA for further strengthening the data privacy. No-doubt, the economic, political and social conditions of the countries are different from each other, but the problems occurred from internet revolution such as infringement of privacy, lapses in the data protection, malicious disclosure of personal information and illegal decryption of the data, can be considered more or less same across the World.

2. Data Protection in UK

United Kingdom introduced the *Data Protection Act (DPA) 1984*, which came into force in 1987 and, among other things, provided individuals certain rights with respect to their personal data. In 1998 DPA revised and replaced the provisions of the 1984, and the Act was commenced in 2000. This Act has been aimed to provide protection to individuals and,

¹ Wiki leaks is a website that publishes anonymous submissions and leaks of sensitive governmental, cooperate, organizational, or religious documents, while attempting to preserve the anonymity and untraceability of its contributors.

² Madhavi Divan, 'The Right to Privacy in the Age of Information and Communication' (2002) 4 SCC (Journal) 12.

ensure that the data is not processed without their consent or knowledge. This Act also defines a category of sensitive personal data which is subject to follow more stringent conditions on their processing rather than other personal data. The collection, storage, release and lapses in personal data is amount to interfere with an individual's right (Right to Privacy). In democratic society, this right is not absolute one, but confined to reasonable restrictions. In the *Data Protection Act, 1998* certain principles have been laid down to guide the collection, processing and use of personal information by both public and private sector organizations. Data Protection is derived from the European Data Protection Directive which originated from European Convention on Human Rights, 1950. So there is mutual interplay between Human Rights and Data Protection. Data Protection Act provides guidance to public bodies on how to meet their obligations under the Human Rights Act to respect personal data.

The objectives of the Act as follows:

- To protect the rights and freedoms of individuals regarding the processing of personal data.
- To harmonize data protection standards throughout Europe and
- To limit movement of data to those countries outside of Europe that does not have adequate levels of protection³.

The Act covers personal data and defines a category of sensitive personal data, such as racial or ethnic origin, political opinions, religious or other beliefs, whether a member of a trade union, physical or mental health, sexual life, and court record, or allegations of such. There are eight principles governing the processing of personal data i.e. “Data Protection Principles” which must be kept in mind by the private individuals, private organizations, government or its agencies while receiving the data:

- (a) The data should be processed fairly and lawfully,
- (b) The data should be obtained for specific and lawful purpose,
- (c) The data should be adequate, relevant and not excessive,
- (d) The data should not be kept for longer than necessary,
- (e) The data should be processed in accordance with the rights of data subjects, and
- (f) Measures should be taken against unauthorized or unlawful processing.

³ Refer to the EU Directive on Data Protection available at, <http://www.doc.gov/ecommerce/eudir.htm>

⁴ A person who alone, jointly or in common with others determines the purposes for which and the manner in which any personal data are processed and responsible for ensuring that the provisions of the Data Protection Act are complied with (*Data Protection Act 1998*)

For the implementation of the above principles, Data Controllers⁴ are responsible for decisions in regard to the processing of personal data, over viewing the complaints relating to processing and disclosing of personal data and claim for compensation. The Act requires that processing should be carried out according to eight Data Protection Principles (discussed above) and data controller is committed to uphold these principles. Data Controller will ensure that data are obtained, used and kept fairly, after taking his/her explicit consent. The processing of data is necessary for the performance of a contract related to the concerned data between the parties. In light of these principles, the performance of the Data Protection Act has remained satisfactory in U.K. According to the annual report (2010-11) of Information Commissioner, U.K., the casework received under data protection act in 2010-2011 has declined by 21 per cent. In absolute number, the figure has declined to 26227 complaints in the year 2010-2011 as compared with 33234 complaints in 2009-2010. It can be argued that the stringent implementation of the Act has forced the entities to protect the sanctity of personal information.

It is also stated that UK has made considerable progress in shrinking the age profile of the data protection caseload, reducing the number of cases over nine months old by 96 percent, and cases over six months old by 85 percent⁵.

Information regarding to one's personal matter is the matter of their private and family life. But if that barrier of personal matter is intervened, it also indicates the violation of one's Human Rights. According to article 8 of European Convention on Human Rights, 1950, *Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others*⁶.

The above article safeguards the right to respect for private life as well as respect for the personal information. The disclosure and processing of one's personal information without taking the consent also contravenes the Human Rights. The DPA has enlightened the importance of protecting the personal information and has harnessed the unauthorized disclosure of particular information. Thus DPA is one of the Acts that protects the basic Human Right.

3. Data Protection in USA

⁵ Information Commissioner (Christopher Graham)'s Annual Report and Financial Statements 2010/11. available at www.ico.gov.uk/about_us/~/media/~/reports/annual_report_2011. I acknowledge sincere efforts of Mr. Ashwani (Department of Economics, Central University of Haryana) for interpreting the data given in the above report.

⁶ <http://www.hri.org/docs/ECHR50.html#C.Art8>

The rapid expansion in technology has forced the developed nations to raise the concern over the issues related to privacy. U.S. has a different approach to deal with the privacy in contrast to the European Union. U.S. has adopted the sectoral approach that relies on the mix of legislations, regulations and self regulation⁷. A patchwork of federal laws covers some specific categories of personal information⁸. These include financial records⁹, credit reports¹⁰, video rentals¹¹, cable television¹², children's (under age 13) online activities¹³, educational records¹⁴, motor vehicle registration¹⁵ and telephone records¹⁶. Further, the important step for protection of privacy was taken up by the enactment of Children's Online Privacy Protection Act (COPPA)¹⁷ and was passed by the US Congress in October 1998. Under the Act, commercial websites and online services directed to children under 13 or that knowingly collect information from them must inform parents of their information practices and obtain verifiable parental consent before collecting, using, or disclosing personal information from children. Like U.K., USA has also considered the importance of the protection of privacy in the era of information technology and enacted various laws to meet with the problem of malicious disclosure of data. The enormous efforts put by the USA Government in this direction have led to improvement in the privacy of personal information. Between April 1, 2010 and March 31, 2011, the PCO (Privy Council Office) received 10 requests for personal information under the Privacy Act, compared to 4 received in the previous year. In 2010-2011, the PCO completed 10 requests for personal information under the Privacy Act. This is comparable to the 9 requests, including requests carried over from previous fiscal years completed in 2009-2010¹⁸. The decreasing numbers in complaints can be used as an indication of the efficiency and strictness of the laws to deal with the problems of infringement of privacy in the country.

4. Data Protection Laws in India

In the era of globalization, it is considered that information technology is rendering incredible role in the economic growth of our country. In today's rapidly changing world of e-

⁷ <http://jurisonline.in/2011/04/data-protection-law-in-india-2/>

⁸ Marc Rotenberg, The Privacy Law Sourcebook, EPIC 1999: <http://www.epic.org/bookstore/pls>

⁹ Right to Financial Privacy Act.

¹⁰ Fair Credit Reporting Act, PL 91-508, amended by PL 104-208 (Sept.30, 1996). <http://www.ftc.gov/os/statutes/fcra.htm>.

¹¹ Video Privacy Protection Act, 1988

¹² Cable Privacy Protection Act, 1984: http://www.epic.org/privacy/cable_tv/ctpa.html

¹³ See Center for Media Education, A Parent's Guide to Online Privacy: <http://www.kidsprivacy.org/>

¹⁴ Family Educational Rights and Privacy Act, 1974: <http://www.epic.org/privacy/education/ferpa.html>

¹⁵ Drivers Privacy Protection Act, PL 103-322, 1994: http://www.epic.org/privacy/laws/drivers_privacy_bill.html

¹⁶ Telephone Consumer Protection Act, 1991.

¹⁷ <http://www.cdt.org/legislation/105th/speech/copa.ht>

¹⁸ Annual Report to Parliament on the Privacy Act 2010-2011. available at <http://www.pco.bcp.gc.ca/docs/information/publications/parl/privacy-personnel/docs/privacy-personnel-eng.pdf>

commerce, almost anything can be bought over the internet and delivered right to one's front door. The internet services have facilitated in easing the transactions worldwide. By transcending international boundaries, the internet and the World Wide Web enable a company to market and deliver goods and services to customers who are located in target countries often thousands of miles away, more efficiently and cost-effectively. But at the same time the information technology has created few intricate problems particularly in malicious uses of the personal information. Any private and government organization is not allowed to use, disclose and release the data of the persons without taking their explicit consent. Recently, in Nov, 29 2010¹⁹ Tata group chairman Rattan Tata moved the Supreme Court seeking action against persons responsible for the disclosure and “unauthorized” publication of tapes of his conversation with professional corporate lobbyist Nira Radia, alleging that it was absolute violation of his right to privacy. Now it will be meaningful to see how the court interprets to Tata's plea for privacy. If one looks at the breach of privacy as the data was improperly protected, thus leading to the lapses in protection of data, the Tax Department may be found to have violated the information privacy of Tata. If one looks at the breach of privacy as the fact that personal contents of conversations were made public with the intent to expose the 2G scam, the claim is really one that his personal privacy has been invaded. Because India does not have a specific legislation on privacy, there is no clear definition of what privacy is, and whether or not Tata has had his privacy invaded²⁰. The decision by the courts will help to clarify how Indian society defines privacy, and where the line between public and private sphere lies. The court's decision will also help to define the context where the right of privacy applies, and the context in which other needs supersede the right of privacy. In the absence of a specific law, data protection in India is handled through the enforcement of privacy and private rights. Privacy rights are enforced under the Indian Constitution and the *Information Technology Act, 2000*, the *Indian Contract Act, 1872*, the *Copyright Act, 1957*, and the *Indian Penal Code, 1860*²¹.

4.1. Data Protection and Privacy Rights

The Constitution of India does not provide a right to privacy (Part III) explicitly. In order to deal with the cases related to privacy, judicial activism brought the Right to Privacy within the realm of fundamental rights. The Supreme Court deduced the right from the Right to Life and Personal Liberty enshrined in Article 21 of the Constitution through an extensive interpretation of the phrase²². But constitutional rights can normally be claimed only against the state or state-owned enterprises and not against private individuals or establishments.

¹⁹ <http://www.indianexpress.com/news/2g-tapes-my-privacy-violated-tata-tells-sc/717442/>.

²⁰ <http://privacyindia.org/2010/12/07/should-ratan-tata-be-granted-the-right-to-privacy/>

²¹ Majmudar & Co., International Lawyers, India.

²² *R.Rajagopal v. State of T.N. (1994) 6 SCC 632*; also see *Gobind v. State of M.P. (1975) 2 SCCC 148*.

The problems arisen with the illegal decryption of data is outside the ambit of said article.

4.2. Data Protection and the Information Technology Act 2000

The Information Technology (IT) Act, 2000 penalizes “cyber contraventions” (section 43(a) to (h) and “cyber offences” (section 65-74). Section 43, in particular deals with the unauthorized access, downloading, virus attacks or any contaminant, causing damage, disruption, denial of access or interference with the service availed by a person. This section provides for a fine up to one crore rupees by way of remedy. Section 65 deals with tampering of computer source documents and provides for imprisonment up to three years or with fine, which may extend up to two lakh rupees or with both. Further section 67 deals with publication and transmission of obscene material in electronic form, and provides punishment which may extend to five years and also with fine which may extend to ten lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to ten lakh rupees.

Under the IT Act, a network service provider or an intermediary is liable for any known misuse of third party information or data or for not exercising due diligence to prevent the offence. An “intermediary” is defined as anybody who receives stores or transmits a particular electronic message on behalf of another person, or who provides any service with respect to that message. Therefore, an Indian Business Process Outsourcing (BPO) Company may be liable as a “network service provider” because it acts as a service provider and receives transmits information or data. The IT Act covers offences and contravention inside and outside India, irrespective of the offender's nationality, as long as the computer system is located in India. Although IT act provides specific section for the protection of data of individuals and provides penalties on the contravention of it. But the violation of these sections (mentioned above) still continued. Such problems demanded a separate Personal Data Protection Act in India. The Personal Data Protection Bill, 2006 has been drafted to provide the protection of personal data and information of an individual collected for a particular purpose by one organization, and to prevent its usage by other organization for commercial or other purpose and entitle the individual to claim compensation or damages due to lapses in disclosure of personal data or information of any individual without his/her explicit consent. It defines personal data as information or data which relate to a living individual who can be identified from that information or data whether collected by any government or any private organization or agency for the prevention of detection of crime; the prosecution of offenders; and the assessment or collection of any tax or duty.

The bill imposes sanctions if the personal data of any collected and is disclosed to any other organization for the purposes of direct marketing or for any commercial gain and states

that any person whose personal data or details have been processed or disclosed for direct marketing or for any commercial gain without consent shall be entitled to compensation for damages in such manner as may be prescribed. However the personal data of any person may be disclosed to charity and voluntary organizations after obtaining prior consent of the person. The demand for separate act to protect the data has not been accepted but in due to the amendment in IT Act in 2008, The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 or privacy rules were issued to implement India's 2008 IT Security Act amendment. The Privacy Rules oblige organizations to notify individuals when their personal information is collected via letter, fax, or email²³. They require covered organizations to make a privacy policy available, to take steps to secure personal information, and to offer a dispute resolution process related to the collection and use of personal information.

4.3. Data Protection and the Indian Contract, 1872

The Indian Contract Act offers an alternative solution to protect the data. The Indian companies acting 'data importers' may enter into contracts with 'data exporters' to adhere to a high standard of data protection. These contracts are binding and may fulfill the requirements of overseas customer's national legislations. Hence, Indian IT enabled companies/BPO (Business Process Outsourcing) sector presently have to follow a very stringent policy to ensure the protection of their client's information, and all the employees are contractually bound to protect the confidential information which is used by the company. The employment contracts clearly specify the terms and conditions over the period of time for maintaining the information more secret and confidential.

4.4. Data Protection and the Copyright Act, 1957

The *Copyright Act, 1957* protects Intellectual Property Rights (IPR) in literary, dramatic, musical, artistic and cinematographic works. The term “literary work” includes the computer databases²⁴. In this case, copying computer database amounts to the infringement of copyright for which civil and criminal remedies can be initiated.

4.5. Data Protection and the Indian Penal Code (IPC), 1860

The offences of theft and misappropriation under the IPC only apply to movable property; it has been defined to include corporeal property of “every description” except land and things permanently attached to the earth. In this process, computer databases can be protected under the IPC, as they are movable by their very nature. In brief, the India has taken various initiatives to deal with the issue of data protection. Further, the protection of data has

²³ By Thomas Claburn InformationWeek, May 05, 2011, available on <http://www.informationweek.com/news/government/policy/229402835>.

²⁴ According to Section 2(o) of the *Copyright Act, 1957*.

been associated with the human rights to strengthen the existing data privacy initiatives.

5. Data Protection and Human Rights

The basic right to protect an individual's privacy has been enshrined in the *Universal Declaration of Human Rights, 1948 (UDHR)* as follows:

“Article 12: no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, or to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”

This Human Right has also been articulated in the *International Covenant on Civil and Political Rights (ICCPR), 1976*. The obligations imposed under the ICCPR require the state to adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right²⁵. The UDHR and the ICCPR are directly binding upon India, being a signatory to both these international conventions. To live in secured atmosphere and enjoy complete privacy in family, home and correspondence is the basic right that has been protected under Human Rights Act. It can be stated that the protection of privacy is a Human Right as well as a fundamental right.

6. Conclusion and Suggestions

The revolution in Information and Communication Technology (ICT) has benefited the globalized world in various dimensions. But also produces numerous challenges before us related to the threat of protection of data and privacy. The present study explores the various laws that are used to deal with these problems in UK, USA and India. UK and US are having the *Data Protection Act, 1998* and sectoral legislation respectively to cope up such problems of violation of the privacy. It is found that US has received handful requests related to the privacy and these numbers has declined recently.

These figures may be used as an indication of the efficiency and strictness of the laws to deal with the problems of infringement of privacy in US. Similarly in U.K., the casework received under data protection act in 2010-2011 has declined by 21 per cent. It is also stated that UK has made considerable progress in shrinking the age profile of the data protection caseload, reducing the number of cases over nine months old by 96 percent, and cases over six months old by 85 percent. It can be argued that the stringent implementation of the Act has forced the entities to protect the sanctity of personal information.

Unlike UK, India is protecting the illegal intervention in personal privacy, malicious disclosure or lapses of data under various laws i.e., Constitutional Law of India, *Information Technology Act, 2000, Indian Contract, 1872, Copyright Act, 1957, Indian Penal Code, 1860*. The basic right to protect an individual's privacy has been enshrined in the *Universal*

²⁵ [http://www.unhchr.ch/tbs/doc.nsf/\(symbol\)/CCPR+General+comment+16.En](http://www.unhchr.ch/tbs/doc.nsf/(symbol)/CCPR+General+comment+16.En)

Declaration of Human Rights, 1948. It can be stated that the protection of privacy is a Human Right as well as a fundamental right. In this direction, the sincere efforts of India have led it to handle the problems originated from the illegal disclosure of personal information. The above information signifies that India has not a specific law to deal with the problems of breach of privacy, and even defining 'privacy' has been a debatable issue in India as mentioned in the case filed by Tata Group. In this skepticism, clearly stating the definition of 'privacy', and enacting a separate or specific regulation may be the right initiation in complement to the existing standards of personal information to protect the basic Human Right and fundamental right.

VIOLATION OF PRIVACY THROUGH SURVEILLANCE IN THE DIGITAL AGE: A BIRD'S-EYE VIEW

Shiv Kumar* & Professor (Dr.) Preeti Misra**

Abstract

The United Nations General Assembly in 2013 adopted a resolution wherein it has clearly acknowledged the concern over increasing issues of eroding privacy protection in the digital age. UN further stated that the rapid pace of technological development enables individuals all over the world to use sophisticated information and communication technologies; at the same time enhances the capacity of governments, companies and individuals to undertake surveillance, interception and data collection, which may violate or abuse human rights, in particular the right to privacy, as set out in article 12 of the UDHR and article 17 of the ICCPR, and is therefore an issue of increasing concern. In June 2013, Edward Snowden revealed with the help of the Guardian the involvement of US government in surveillance of citizen's communication using modern technology. In 2021, The Hon'ble Supreme Court of India in Pegasus case is called upon to examine an allegation of the use of a modern technology, its utility, need and alleged abuse. The surveillance potential of powerful government IT systems as well as social media operators prompted demands for specific rules governing the collection and handling of personal information. This paper focuses light on the violation of privacy through surveillance by the states and private actors of social media, its impact on human rights and anticipated possible remedies.

Keywords: Privacy, Surveillance, Social Media, Human Rights

INTRODUCTION

Privacy is a sweeping concept, encompassing inter alia freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations¹. Prof. Alan Westin provides most influential definition of privacy in sense of control over personal information "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others²." In modern society, privacy is inherently linked to surveillance. One of the main ways in which privacy can be threatened is by the act of placing an individual under surveillance.

Privacy is at least in some ways about control over how much is known about us by whom. In the online world, where decisions are made on the basis of information of data that

* Research Scholar, Department of Human Rights, School of Legal Studies, Babasaheb Bhimrao Ambedkar (Central) University, Lucknow (Uttar Pradesh), India
e-mail: shivkumarrawat@gmail.com

** Dean, School of Legal Studies & Head, Human Rights, Babasaheb Bhimrao Ambedkar (Central) University, Lucknow (Uttar Pradesh), India

¹ Daniel J. Solove, *Understanding Privacy I* (Harvard University Press 2008).

² Alan Westin, *Privacy and Freedom I* (IG Publishing 1967).

aspect of privacy becomes particularly significant. To protect our autonomy, to have influence over what happens to us online, over what we see online, over what decisions are made about us and for us, we need to have protection over how data is gathered about us, how that data is used, who can hold that data and so forth³.

Privacy is linked to both positive and negative freedoms. In terms of positive freedom, privacy expresses the set of rights for a person's ability to control four broad areas of legal concern: freedom of personal autonomy; the right to control personal information; the right to control property; and the right to control and protect physical space. As a negative freedom, privacy is understood as the absence of invasion of privacy by the government, business, or other actors into the space considered personal⁴.

PRIVACY CONCERN IN THE DIGITAL AGE

Privacy as a basic human right touch upon fundamental needs and values associated with man's gregarious nature. In Puttaswamy⁵ Case it was held that "Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the state but from non-state actors as well".

The United Nations General Assembly in 2013 adopted a Resolution 68/167 relating to the right to privacy in the digital age wherein it has clearly acknowledged the concern over increasing issues of eroding privacy protection in this technologically advanced world.

The relevant portion of the preamble reads as "*Noting that the rapid pace of technological development enables individuals all over the world to use new information and communication technologies and at the same time enhances the capacity of governments, companies and individuals to undertake surveillance, interception and data collection, which may violate or abuse human rights, in particular the right to privacy, as set out in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights, and is therefore an issue of increasing concern*"⁶. Considering the potential threats in the form of communication surveillance, its interception, data theft, unauthorized personal data access, trans-border flow of data etc. the UN has affirmed that the same rights that people have offline must also be protected online, including the right to privacy⁷.

³ Paul Bernal, *Internet Privacy Rights* 15 (Cambridge University Press 2014).

⁴ Monroe E. Price ET. AL., *Routledge Handbook of Media Law* 470 (Routledge 2013).

⁵ *Justice (Retd.) K.S. Puttaswamy v. Union of India* (2017) 10 SCC 1.

⁶ Dr. Lisa P Lukose ET. AL., *Human right and Social media*, https://www.researchgate.net/publication/331715928_Human_Right_and_Social_Media (last visited on Feb 22, 2022).

⁷ The right to privacy in the digital age : report of the Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age : (un.org) (last visited on Feb. 22, 2022).

DEFINITION AND FORMS OF SURVEILLANCE

Based on Foucault's notion of surveillance as disciplinary power, one can define surveillance as a specific kind of information gathering, storage, processing, assessment and use that involves potential or actual harm, coercion, violence, asymmetric power relations, control, manipulation⁸, domination or disciplinary power. Surveillance is instrumental and a means for trying to derive and accumulate benefits for certain groups or individuals at the expense of other groups or individuals.

Prof. Alan Westin in his seminal work, 'Information Technology in a Democracy' identified three forms of surveillance that might be conducted by public authorities⁹.

- Physical
- Psychological
- Data

Physical surveillance, as the name suggests, involves the act of watching or listening to the actions of an individual. Physical surveillance is as old-established as society. Psychological surveillance includes include forms of interrogation or the use of personality tests, as favoured by some employers. Data surveillance involves a different, more passive approach. Every action by an individual reveals something about the person. Very few actions do not involve individuals in giving out a measure of information about themselves. This may occur directly, for example, in filling out a form, or indirectly, as when goods or services are purchased. The essence of data surveillance lies in the collection and retention of these items of information.

PRIVACY VIOLATION THROUGH EMERGING NEW TECHNOLOGIES

Technological innovations and applications such as the internet, social media, mobile applications and cloud computing have created great economic and societal values, and enhance the productivity and competitiveness of enterprises in ways beyond our imagination. At the same time, they also pose immense risks to privacy and raise serious concerns about the protection of personal data.

One of the great innovations of the 1990s and beyond is the sudden and rapid growth of social media, or social networking sites, which permit people to communicate quickly and easily through the Internet¹⁰. Privacy is rapidly becoming inextricably linked to the world of digital communications and social media. Social media and social networking sites (SNS) have risen sharply in popularity and widespread use, allowing new forms of socialization,

⁸ Christian Fuchs, *Social Media A Critical Introduction* 188 (Sage Publications India Pvt Ltd 2017).

⁹ Ian J. Llyod, *Privacy, Technology, a Surveillance* 19 (Oxford University Press 2017).

¹⁰ Stephen Currie, *How is the Internet eroding the privacy rights* 25 (Reference Point Press 2014).

sharing and communication between people. This new state of communication raises new privacy questions.

Social Networking sites like Facebook, Google and many others are violating privacy of users through economic surveillance. Economic surveillance on corporate social media is surveillance of prosumers, who keeps on creating and sharing user-generated content, browse profiles and data, interact with others, join, create and build communities and co-create information. The corporate web platform operators and their third-party advertising clients continuously monitor and record personal data and online activities. They store, merge and analyse collected data. This allows them to create detailed user profiles and to know a lot about the users' personal interests and online behaviours. Social media that are based on targeted advertising sell prosumers as a commodity to advertising clients. There is an exchange of money for the access to user data that allows economic user surveillance¹¹.

Google also engages as Facebook in user surveillance for the end of capital accumulation. Google surveillance is primarily a form of economic surveillance. Google uses a powerful search algorithm. The details of the PageRank algorithm are secret. Basically small, automated programmes (web spiders) search the WWW, the algorithm analyzes all found pages, counts the number of links to each page, identifies keywords for each page, and ranks its importance. The PageRank algorithm is a form of surveillance that searches, assesses and indexes the WWW.

Big Data is an even newer concept, trend, development than social media. Big data “refers to the movement to analyse the increasingly vast amounts of information stored in multiple locations, but mainly online and primarily in the cloud”. According to UN report, it is a massive volume of both structured and unstructured data that is so large that it's difficult to process with traditional database and software techniques. The characteristics which broadly distinguish big data are sometimes called the '3 V's': more volume, more variety and higher rates of velocity. The report further provides examples of such data, including data from sensors used to gather climate information, posts to social media sites, digital pictures and videos posted online, transaction records of online purchases, and from cell phone GPS signals¹². Big Data has advanced a culture of control, surveillance, fear-mongering, scapegoating and suspicion in which law and order politics and surveillance are seen as fixes to the complex societal problem of terrorism¹³.

REVELATION OF SURVEILLANCE BY EDWARD SNOWDEN

¹¹ Supra note 8, at 108.

¹² United Nations Development Group, *Data Privacy, Ethics And Protection Guidance Note On Big Data For Achievement Of The 2030 Agenda*, https://unsdg.un.org/sites/default/files/UNDG_BigData_final_web.pdf (last visited on Feb. 22, 2022).

¹³ Supra note 8, at 53.

In June 2013, Edward Snowden revealed with the help of the Guardian the existence of large-scale Internet and communications surveillance systems such as Prism, XKeyscore and Tempora. According to the leaked documents, the National Security Agency (NSA), a US secret service, in the PRISM programme obtained direct access to user data from seven online/ICT companies: AOL, Apple, Facebook, Google, Microsoft, Paltalk, Skype and Yahoo. The Powerpoint Slides that Edward Snowden leaked refer to data collection “directly from the servers of these U.S. Service Providers”. Snowden also revealed the existence of a surveillance system called XKeyScore that the NSA can use for reading emails, tracking web browsing and users' browsing histories, monitoring social media activities, online searches, online chat, phone calls and online contact networks, and following the screens of individual computers. According to the leaked documents, XKeyScore can search both meta-data and content data¹⁴.

RIGHT TO PRIVACY IN HUMAN RIGHTS LAWS

Various International instruments contain the provisions of right to privacy. A few of them are as follows:

Article 8 of ECHR (European Commission of Human Rights) *“Everyone has the right to respect for his private and family life, his home and his correspondence”*.

Article 12 of UDHR *“No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence. Everyone has the right to the protection of the law against such interference”*.

Article 17.1 of ICCPR - *“No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence.*

Article 17.2 of ICCPR - *“Everyone has the right to the protection of the law against such interference or attacks”*.

PROTECT, RESPECT, AND REMEDY FRAMEWORK

In 2011, Ruggie's work culminated with an endorsement of the United Nations' Guiding Principles on Business and Human Rights (UNGP)¹⁵. The UNGP provides a set of principles that states and businesses should apply to prevent, mitigate, and redress corporate-related human rights abuses. The UNGP elaborates the distinction that exists between the state duty to protect human rights, and the corporate responsibility to respect human rights based on three pillars, often called the “Protect, Respect, and Remedy” framework. The first

¹⁴ Supra note 8, at 202.

¹⁵ Report of the Special Representative John Ruggie, Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework, U.N. Doc. A/HRC/17/31 Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, John Ruggie : (un.org) (March 21, 2011) (last visited on Feb. 22, 2022).

pillar (Protect) focuses on the role of the state in protecting individuals' human rights against abuses committed by non-state actors; the second pillar (Respect) address the corporate responsibility to respect human rights; and the third pillar (Remedy) explores the roles of state and non-state actors in securing access to remedy¹⁶.

DATA PROTECTION REGIME IN THE WORLD

Data privacy laws systematically regulate the use of information about people. They are also known as 'data protection' or 'fair information practices' laws and the individuals affected are sometimes called 'data subjects.' Data privacy laws essentially comprise a set of enforceable data privacy principles based on the 'life cycle' of personal data (collection, accuracy, security, use, disclosure, access, retention, etc.) coupled with an enforcement structure backed by legal measures requiring compliance.

Enforcement usually involves a data privacy authority, often called a 'Data Protection Authority' (DPA) or 'Privacy Commissioner', but often involves other enforcement authorities as well¹⁷.

In 1972, the UK Government set up the Younger Committee, which was tasked a broad remit to consider whether legislation was needed to protect individuals and organizations from intrusions into their personal privacy¹⁸. The Organization for Economic Co-operation and Development (OECD) Privacy Guidelines (1980) were an early influence on the development of data privacy laws¹⁹. The OECD Guidelines on the Protection of Privacy and Transborder Flow of Personal Data were one of the first formulations of a comprehensive set of information privacy principles. In 1984, The Data Protection Act of UK established new rights for individuals to know if an organization was processing personal data about them and the right to have a copy of the information. The European Union, which had tended to leave human rights issues to the Council of Europe, became involved in data privacy in the early 1990s, and by 1995 adopted the general data protection directive 95/46/EC.

All organizations which collect and process personal data must comply with the obligations of the UK data protection regime. This is set out in the UK Data Protection Act 1998. In 2012, the European Commission revised the existing privacy protections in the European Union, and declared to bring uniform law on the data protection i.e. 'General Data Protection Regulation' (GDPR). On May 25th, 2018, the European Data Protection

¹⁶ Molly K. Land ET.AL., *New Technologies for Human Rights Law and Practice* 255 (Cambridge University Press 2018).

¹⁷ Graham Greenleaf, *Asian Data Privacy Laws* 6 (Oxford University Press 2014).

¹⁸ Laura Scaife, *Handbook of Social Media and the Law* 242 (Informa Law from Routledge 2015).

¹⁹ Supra note 17, at 10.

Regulation came into effect in order to harmonize data privacy laws across Europe²⁰. This regulation replaced the Data Protection Directive of 1995. European Union General Data Protection Regulation aims to²¹: lay down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data; protect fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

RIGHT TO PRIVACY IN INDIAN LEGAL SYSTEM

The right to privacy, before Puttaswamy case²² derived its ambiguous basis from the right to life and personal liberty, as enshrined in Article 21. In the language of the over-arching Article of the Constitution of India, Article 21 reads as follows:

21. Protection of life and Personal Liberty. *No person shall be deprived of his life and liberty except according to procedure established by law.*

*The Supreme Court in M.P. Sharma v. Satish Chandra*²³ and *Kharak Singh v. State of U.P.*²⁴ has held that there is no fundamental right to privacy.

The Supreme Court undertook a comprehensive examination of the question of the right to privacy in *Kharak Singh*. In the instant case, the question for consideration before the seven-judge Bench was whether surveillance under Chapter XX of the Uttar Pradesh Police Regulations infringed fundamental rights guaranteed by Part III of the Constitution. Regulation 236(6) which allowed surveillance by “domiciliary visits at night” was held to contravene Article 21. The court elaborately analysed the connotations of the words “life” and “personal liberty” in Article 21.

However, in *Gobind v. State of M.P.*²⁵ Mathew J., following the minority opinion in *Kharak Singh*, asserted that the “right to privacy” was a fundamental right. However, it was not recognised in an absolute sense and was subject to restrictions on the basis of compelling public interest.

In *R. Rajagopal v. State of T.N.*²⁶, it was held that the “right to privacy” is implicit in right to life and liberty guaranteed to the citizens of this country by way of Article 21. Furthermore, in *People's Union for Civil Liberties (PUCL) v. Union of India*²⁷, it was held

²⁰ General Data Protection Regulation GDPR, <https://gdpr-info.eu/> (last visited on Feb. 22, 2022).

²¹ General Data Protection Regulation GDPR, art. 1, <https://gdpr-info.eu/art-1-gdpr/> (last visited on Feb. 22, 2022).

²² Justice (Retd.) K.S. Puttaswamy v. Union of India (2017) 10 SCC 1.

²³ M.P. Sharma v. Satish Chandra AIR 1954 SC 300.

²⁴ Kharak Singh v. State of U.P. AIR 1963 SC 1295.

²⁵ Gobind v. State of M.P. (1975) 2 SCC 148.

²⁶ R. Rajagopal v. State of T.N. (1994) 6 SCC 632.

²⁷ Union for Civil Liberties (PUCL) v. Union of India (1997) 1 SCC 301.

that “right to privacy” insofar as it pertains to speech is part of fundamental rights under *Articles 19(1) (a) and 21 of the Constitution*. In *Puttaswamy*²⁸ Case it was held that

“Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the state but from non-state actors as well. We commend to the Union Government the need to examine and put into place a robust regime for data protection. The creation of such a regime requires a careful and sensitive balance between individual interests and legitimate concerns of the state.”

Hon'ble Supreme Court of India in this case further held that Indians have a constitutionally protected fundamental right to privacy that is an intrinsic part of life and liberty under Article 21 and further held that privacy is a natural right that inheres in all natural persons, and that the right may be restricted only by state action that passes each of the following three tests:

- First, such state action must have a legislative mandate;
- Second, it must be pursuing a legitimate state purpose; and
- Third, it must be proportionate i.e., such state action both in its nature and extent, must be necessary in a democratic society and the action ought to be the least intrusive of the available alternatives to accomplish the ends.

India does not have any specific law for data protection. Statutory protection of privacy can be found in India is scattered across a number of statutes. The *Information Technology Act 2000* (IT Act), as amended by the *Information Technology (Amendment) Act 2008* (ITAA), has the broadest scope.

As a result of *Puttaswamy* case, a committee headed by Justice B. N. Krishna presented a draft of Personal Data Protection Bill. The Bill was further amended and still pending in form of The Personal Data Protection Bill, 2019 to come into force.

THE INFORMATION TECHNOLOGY RULES, 2021

In February, 2021 the Ministry of Electronics and Information Technology, Government of India has notified new rules under the *Information Technology Act, 2000* (“IT Act”) for monitoring social media digital media platforms. The new rules, viz. *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021* (“*Intermediary Guidelines*”)²⁹ inter alia aims to serve a dual-purpose: (1) increasing the accountability of the social media platforms (such as Facebook, Instagram, Twitter etc.) to prevent their misuse and abuse; and (2) empowering the users of social media by

²⁸ Justice (Retd.) K.S. Puttaswamy v. Union of India (2017) 10 SCC 1.

²⁹ https://www.meity.gov.in/writereaddata/files/Intermediary_Guidelines_and_Digital_Media_Ethics_Code_Rules_2021.pdf (last visited on Feb. 22, 2022).

establishing a three-tier redressal mechanism for efficient grievance resolution. The Intermediary Guidelines have been framed in exercise of powers under section 87 (2) of the IT Act and supersede the previous Information Technology (Intermediary Guidelines) Rules, 2011.

PEGASUS CASE: SURVEILLANCE THROUGH TECHNOLOGY

In *matter of Manohar Lal Sharma V. Union of India and Others (2021)*³⁰ (Popularly known as Pegasus Case) the Hon'ble Supreme Court is called upon to examine an allegation of the use of such a modern technology, its utility, need and alleged abuse. The factual position of the present case is as follows:

“In September 2018, Citizen Lab, based out of the University of Toronto, Canada, released a report detailing the software capabilities of a Pegasus spyware developed by an Israeli Technology firm, viz., the NSO Group. The report indicated that individuals from nearly 45 countries were suspected to have been affected. Once the software installed on an individual's device, it has the capacity to access the entire stored data on the device, and has real time access to emails, texts, phone calls, as well as the camera and sound recording capabilities of the device. On 18 July 2021, a consortium of nearly 17 journalistic organizations from around the world, including one Indian organization, released the results of a long investigative effort indicating the alleged use of the Pegasus software on several private individuals. This investigative effort included a list of some 50,000 leaked numbers (out of which 300 numbers belonged to Indians) under surveillance by clients of the NSO Group through the Pegasus software. The above reports resulted in largescale action across the globe. Some of the Writ Petitioners before Hon'ble Supreme Court of India allege to be direct victims of the Pegasus attack, while others are Public Interest Litigants.

Hon'ble Supreme Court while dealing with these petitions made following observations: the entire citizenry is affected by such allegations due to the potential chilling effect; no clear stand taken by the Respondent-Union of India regarding actions taken by it; possibility that some foreign authority, agency or private entity is involved in placing citizens of this country under surveillance.

The Hon'ble Supreme Court constituted a technical committee under the supervision of Justice R.V. Raveendran, former Judge, Supreme Court of India to enquire, investigate and determine:

i. Whether the Pegasus suite of spyware was used on phones or other devices of the citizens of India to access stored data, eavesdrop on conversations, intercept information and/or for any other purposes not explicitly stated herein?

³⁰ *Manohar Lal Sharma Vs Union of India and Others* 2021 SCC Online SC 985.

- ii. The details of the victims and/or persons affected by such a spyware attack.
- iii. What steps/actions have been taken by the Respondent-Union of India after reports were published in the year 2019 about hacking of WhatsApp accounts of Indian citizens, using the Pegasus suite of spyware.
- iv. Whether any Pegasus suite of spyware was acquired by the Respondent-Union of India, or any State Government, or any central or state agency for use against the citizens of India?
- v. If any governmental agency has used the Pegasus suite of spyware on the citizens of this country, under what law, rule, guideline, protocol or lawful procedure was such deployment made?

The Hon'ble Supreme Court of India has directed this committee to make recommendations regarding enactment or amendment to existing law and procedures surrounding surveillance and for securing improved right to privacy; regarding enhancing and improving the cyber security of the nation and its assets; to ensure prevention of invasion of citizens' right to privacy, otherwise than in accordance with law, by State and/or non-State entities through such spywares; regarding the establishment of a mechanism for citizens to raise grievances on suspicion of illegal surveillance of their devices; regarding the setting up of a well-equipped independent premier agency to investigate cyber security vulnerabilities, for threat assessment relating to cyberattacks and to investigate instances of cyberattacks in the country.

CONCLUSION

Today, all democratic societies have come to realize that privacy is at the heart of all human rights. Privacy is inherently linked to surveillance. With the ability to digitise any form of information, boundaries between the various forms of surveillance are disappearing with the application of information technology linking surveillance techniques into a near seamless web of surveillance. The reach of systems of physical surveillance has been increased enormously by the involvement of the computer to digitise and process the information received. Facebook and Google are huge advertising, capital accumulation, and user-exploitation machines. Data surveillance is the means for Facebook's and Google's economic ends. Although various nations around the globe have granted their citizens the right to privacy, they have not been able to formulate effective legislations for the protection of online privacy.

Even with the adoption of legal and other protections, violations of privacy remain a concern. The danger today is that data flows are invisible and when society becomes aware of the potential for misuse, it may be too late to put this technological genie back in the bottle. It is therefore suggested that to protect our privacy in digital age we need to know the value of

our personal information that we share online and other aspects like who is gathering data about us, how that data is used by whom, who can hold that data, how can we delete our personal data and so forth; Effective remedy against the violation of privacy can be a reality only when the law considers the context of the time. A flexible yet robust privacy protection regime in India is the need of today; there is need to explore the roles of state and non-state actors in securing access to remedy in case of violation of privacy; there are large gaps in our knowledge, research and understanding of developing issues in social media platform, big data and other technologies. More research is needed to appraise ourselves of all potential solutions and policy decisions as well as assisting websites to fully engage their own (corporate, moral and legal) responsibilities and functional capabilities.

PRIVACY: AN ESSENTIAL PRE-REQUISITE IN PROFESSIONAL RELATIONSHIPS

Dr. Money Veena. V.R*

Abstract

The Concept of right to privacy is recognized by almost all nations of the world. In some countries it is given statutory recognition while in some others it is mentioned in the Constitution itself. In India, it is not expressly guaranteed as a fundamental right. But the Honourable Supreme Court had in many cases held that for constituting fundamental right, it is not necessary that a right should be there specifically in the Constitution. The Apex Court had in many times held that right to privacy is implied in the Article 21 of the Constitution which guarantees right to life and personal liberty. Right to privacy is protected in all spheres of life. In certain relations the communications made between the parties are protected from disclosure. The Indian Evidence Act 1872 protects certain communications known as privileged communications made between the parties in certain fiduciary relations. To value privacy of certain relations, such a protection is offered by law and these communications are not admissible as evidence. The communications between an advocate and his client is protected under sections 126-129 of the Evidence Act. The Indian Medical Council (Professional Conduct, Etiquettes and Ethics) Regulations 2002 also prevents a medical professional from disclosing information about his patients. This paper is an attempt to analyse the concept of right to privacy in professional relationships and also to examine the exemptions in various legislations.

Keywords: Privacy, Personal liberty, Privileged Communications, Fiduciary Relations etc.

Introduction

All democratic nations in the world believe in the dignity of the individual and treats him with respect as a worthy human being. As far as India is concerned, right to privacy is protected in various personal laws and it has been treated as a constituent part of right to life and personal liberty under Article 21¹. The term privacy has been defined in different terms by various authors and jurists. It has been defined as the state of being free from intrusion or disturbance in one's private life affairs². Privacy means one's private life or the right to be left alone³. Privacy is also defined as the condition or state of being free from public attention to intrusion or interference or interference with one's acts or decisions⁴.

The right or quest for privacy is a basic instinct of human beings for establishing individual boundaries and restricting others. This paper is an attempt to analyse various facets of right to privacy and the need to ensure privacy in professional relationships with special reference to

* Assistant Professor of Law, Government Law College, Vanchiyoar, P.O, Trivandrum, Kerala.

¹ Article 21 of the Constitution of India guarantees to all persons the right to life and personal liberty and it cannot be deprived of except according to the procedure established by law. Narendra Kumar, *Constitutional Law of India* 345 (Allahabad Law Agency 2018)

² Wharton, *Concise Law Dictionary* 514 (Universal Law Publishing Co, New Delhi 2012)

³ R.P. Remesan, *Law Dictionary* 514 (Swamy Law Series 2016)

⁴ Bryan.A.Garner(ed), *Black's Law Dictionary* 1233 (West Publishing 2004)

Legal, Medical and Chartered Accountancy professions.

Privacy in the international sphere

Universal Declaration of Human Rights 1948 proclaims various human rights and for the first time this document expressly declared right to privacy as an independent right⁵. American Declaration of Rights and Duties of Man 1948⁶ in article 1 ensures right to life, liberty and security of individuals. *International Covenant on Civil and Political Rights*, 1966⁷ in article 17 (1) ensures various protections against arbitrary or unlawful interference with privacy, family, home or correspondence. It also includes protection against unlawful attacks on his honour and reputation. Article 17 (2) offers legal protection if there is interference over this right. Convention for Protection of Human Rights and Fundamental Freedoms 1950⁸ in Art 8 ensures the right to protection for family and private life. American Convention on Human Rights 1969⁹ in Article 11 provides that everyone has the right for respecting his honour and dignity. As per this Convention, no one is permitted to have arbitrary or abusive interference with other's life, family, home, correspondence, or of unlawful attacks on his honour or reputation. The article also provides that everyone is entitled to legal protection against such interference or attacks.

Privacy in UK

Historically, English law has not recognised a positive right to privacy although the courts have developed the common law in a number of areas to protect privacy¹⁰. Series of Private Member's Bills were introduced in the UK Parliament during 1960s, which dealt with privacy issues. In the parliamentary debates on the first of the Private Member's Bills on Privacy introduced in the UK during 1960, Lord Mancroft's Right to Privacy Bill, 1981 Lord Denning said that the law on privacy in the US had evolved from the English Common law and that in England, the judges may well do it¹¹. *The Protection of Human Rights Act 1998*¹² offers protection of family and personal life. Everyone has the right to be protected

⁵ Article 12 UDHR-All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood. <https://www.un.org/en/about-us/universal-declaration-of-human-rights> (February 15, 2022, 7:20 PM)

⁶ This was adopted on May 2, 1948, and it is the world's first general international human rights instrument, preceding the Universal Declaration of Human Rights.

⁷ The International Covenant on Civil and Political Rights is a multilateral treaty that commits states parties to respect the civil and political rights of individuals, including the right to life, freedom of religion, freedom of speech, freedom of assembly, electoral rights and rights to due process and a fair trial.

⁸ The European Convention on Human Rights (ECHR) protects the human rights of people in countries that belong to the Council of Europe.

⁹ The purpose of the Convention is "to consolidate in this hemisphere, within the framework of democratic institutions, a system of personal liberty and social justice based on respect for the essential rights of man

¹⁰ *Andrew Nicol Qc, Gavin Millar Qc & Andrew Sharland, Media Law And Human Rights* 9 (2nd edn Oxford University Press 2009)

¹¹ *S.k.sharma, Privacy Law-a Comparative Study* 11 (Atlantic Publishers and Distributors 1994)

¹² Article 8- This article protects the right to respect for family and private life, home and correspondence

against unlawful interference upon one's privacy. The common law allowed the individual to speak and act in his own home as he pleases and to carry on his daily business, provided that, in so doing, he does not infringe rights of others, or behave in such a way as is likely to cause a breach of the peace or to commit an offence¹³.

USA and right to privacy

In the United States of America, rights and freedoms of the citizens are set forth in the Constitution itself. Many of the fundamental rights assured contributes indirectly to privacy. *The Privacy Act 1974* excludes gathering of information about the political or religious beliefs of any person. But this can be done after getting written consent of the individual. The US Supreme Court in 1960 constitutionally denominated right to privacy as a fundamentally personal right emanating from the totality of the constitutional scheme under which the people are living¹⁴. *Later in Griswold v. Connecticut*, the US Supreme Court invalidated a Connecticut¹⁵ statute which made the use of contraceptives a criminal offence on the basis of violation of privacy. Douglas J observed that various guarantees like 1st¹⁶, 3rd¹⁷, 4th¹⁸ and 5th¹⁹ amendments of the US Constitution created zones of right to privacy²⁰. In *Jane Roe v. Henry Wade*²¹ the US Supreme Court established the Constitutional right to privacy.

Privacy in other countries

Most of the democratic countries assures right to privacy to the citizens in some form or other. *Canada Act 1982* indirectly mentions the right to be secure against unreasonable search or seizure²². The Constitution of Eire 1937 provides right to privacy of dwellings of citizens²³. The Constitution of Japan 1946 recognizes right to privacy by expressly stating that the homes, papers and effects of all persons shall be secured against entries, searches and seizures except upon warrant issued for adequate cause²⁴. The Constitution of West Germany 1949 contained provisions in relation to marriage and family²⁵. The Constitution of USSR

¹³ S.K.SHARMA, supra note 11

¹⁴ *Poe v. Ulman* (1960) 367 US 497

¹⁵ 381 US 479 (1965)

¹⁶ It was in 1791 which prevents the Government from making laws prohibiting the freedom of press, freedom of speech, freedom of assembly etc.

¹⁷ The amendment was in 1791 and which placed some restrictions upon placing soldiers in private homes.

¹⁸ This was in the year 1971 for prohibiting unreasonable searches and seizures.

¹⁹ It was in the year 1991 and it granted rights against self-incrimination, right to grand jury etc.

²⁰ *Jyothi J Mozika, Law and Protection of Right to Privacy* 15 (1st edn R.Com Bray & Co. Pvt. LTD 2013)

²¹ (1973) 35 L.Ed.2d 147.

²² Article 8 of Canada Act-Everyone has the right to be secure against unreasonable search or seizure.

²³ Article 50(5) of the Constitution of Eire-the dwellings of every citizen is inviolable and shall not be forcibly entered save in accordance with law.

²⁴ Article 35 of the Constitution of Japan.

²⁵ Article 6

1979 guaranteed that citizens may not be arrested except by court decision or on the warrant of a procurator²⁶.

The Constitution of the People's Republic of China 1982 declares that the freedom of persons or the citizens of the People's Republic of China is inviolable. No person can be arrested except as provided by law²⁷.

Privacy right in India

The Constitution of India is the basic document or the source of rights of the people. But there is no express mention in the Constitution about right to privacy. The Hon'ble Supreme Court in *Kharak Singh v. State of UP*²⁸ considered right to privacy, the case related to police surveillance and domestic visit at night. Later in *Govind v. State of MP*²⁹ the Court established that the right to privacy is a fundamental right and Article 21 protects right to privacy and promotes the dignity of the individual. The judiciary has established this as a *fundamental right in many cases*³⁰. For the happiness of a man, it becomes necessary to protect intrusion into one's secrets which is basic to a free society and more particularly in a *democratic world*³¹. According to Justice V.R Krishna Iyer, right to privacy is a part of the right to human dignity and the public law on information must frown on the violation of that intimacy of life which is the core of individual wellbeing³².

Privacy under laws in India

Privacy is respected or considered as a right directly or indirectly in different legislations in India. Indian Penal Code contains many provisions for protecting the identity or respecting the privacy of the victims. Most of the family laws have provisions for ensuring privacy during divorce or other related proceedings. The Protection of Children from Sexual Offences (POCSO) Act 2012 ensures that the identity of the child shall not be revealed³³ and this is for ensuring the privacy of the child. The Indian Evidence Act has many provisions protecting certain communications between parties, which is to respect the sanctity of certain relations and for respecting the privacy of the parties.

Privacy under the Indian Evidence Act 1872

Chapter IX of the Indian Evidence Act sections 118-134 deals with examinations of witnesses. General rule is that all persons are competent to testify unless due to reasons like

²⁶ Article 54 of the USSR Constitution

²⁷ Article 37 of the Constitution of People's Republic of China.

²⁸ AIR 1963 SC 1295

²⁹ AIR 1975 SC 1378

³⁰ *R. Rajagopal v. State of TN* AIR 1995 SC 264, *Mr. X v. Hospital Z* AIR 1999 SC 495

³¹ Justice Frankfurter in *Wolf v. Colorado* (1949) 338 US 25

³² VR Krishna Iyer, *The Right to Know is Fundamental in Salvaging Democracy* 119 (1990)

³³ Section 23 of the POSCO Act prohibits the media from disclosing the identity of the child

disease, old age, tender years or anything else, they are incapable of understanding the questions.

But competency is different from capability to give evidence³⁴. A witness though capable to give evidence, maybe privileged or protected from answering certain questions. In other words, it is a case of prohibition, that is even if the witness is willing to answer, the law prohibits³⁵.

Privileged communications

There are certain matters which a witness in India cannot either be compelled to disclose or even if the witness is willing to disclose, he will not be permitted to do so, such matters are known as privileged communications. These are of two kinds, namely those which are privileged from disclosure and those which are prohibited from being disclosure. The policy of law is that certain communications should not be disclosed. The law does not permit for the disclosure of these communications even if the party possessing that information is willing to disclose it³⁶.

Communications protected from disclosure

Some communications between parties are protected from disclosure. It includes communications during marriage³⁷. This is because destruction of confidence between husband and wife would cause much misery and affect the marital relation itself. Those living in marital relation is not allowed to betray the mutual trust and confidence which such relation implies³⁸. This privilege admits certain exceptions too which include acts apart from communication, evidence by third parties, waiver of privileges and crimes or suits between parties.

The second communication which is exempted is evidence as to affairs of state³⁹. The only exception is that they may be disclosed with the permission of the Head of the Department concerned. Third exemption is giving privileges to public officers to refuse to disclose matters which are brought to their knowledge in official confidence⁴⁰.

Evidence Act section 125 is to encourage people to give information about offences by protecting the source of information, for otherwise no one would like to give such information⁴¹.

³⁴ *M.p.Tandon, Indian Evidence Act 377* (13th edn 2020, New Era Law Publications)

³⁵ *Abhinandan Malik, Vepa P Sarathi's Law of Evidence* 386 (Eastern Book Co.2020)

³⁶ *Dr.avtar Singh, Principles of The Law of Evidence* 122 (23rd edn, Central Law Publications 2018)

³⁷ Section 122 Indian Evidence Act

³⁸ *Still v. Stillman*, 115 Mis 106,107 : 187 NYS 383, cited Richardson on Evidence (pp453-54) *Compellability And Privileges: Three Problem, cowen And Carter*) *Essays On The Law of Evidence* 219)

³⁹ Section 123 of Indian Evidence Act

⁴⁰ Section 124 Ibid

⁴¹ Section 125 Ibid

Professional communications between advocate and client

Privilege that is attached to professional communications is dealt with under Sections 126 to 129 of the Indian Evidence Act. This is mainly concerned with the communication between the legal adviser and client. The section not only protects the legal advisers from disclosing communications made to him by his clients when interrogated as a witness, but he is not permitted to do so even if he is willing to give evidence unless with the express consent of his client⁴². It is based upon the principle that if communications to a legal adviser were not privileged, a man would be deterred from fully disclosing his case, so as to obtain proper professional aid in a matter in which he is likely to be thrown into litigation⁴³. As per the section, no attorney or vakil shall at any time be permitted to disclose any communications made by his client for the purpose of employment, the privilege also extends to documents prepared in connection with the client's claim for the dominant purpose of preparing for litigations⁴⁴.

The purpose of legal professional's privilege is to allow a client to make full disclosure to a solicitor without fear that disclosure of their communications might subsequently be made against his will. In the absence of this prohibition, it would have been difficult for anybody to get the best professional advice. If such communications were not protected, no man would be willing to consult a professional adviser for his defence or for the enforcement of his rights. In such an instance, no man could safely come into a court for obtaining redress or for defending himself⁴⁵.

Conditions

There are certain conditions for availing this privileges, firstly, the communications should have been made to a barrister or attorney or pleader or vakil⁴⁶.

This includes any person who is duly licensed by the state to practice law⁴⁷. It includes all kinds of legal work and not merely appearance in court. Second condition is that the communications should have been made by a person who is related to the vakil as a client. It is not necessary for enjoying this protection that any fee should have been paid to the vakil

⁴² *Ratanlal & Dhirajlal, The Law of Evidence 1199* (20th edn, WADHWA & COMPANY)

⁴³ *Ratanlal & Dhirajlal, The Law of Evidence 707*, BM Prasad & Manish Mohan (25th edn Lexis Nexis)

⁴⁴ *Ibid*

⁴⁵ *Sudipto Sarkar & Vr Manohar, Sarkar On Evidence 1859* (14th edn 1993, Wadhwa & Co, Nagpur)

⁴⁶ The Madras High Court had cited these decisions in *D. Varasekaran v. State of TN* 1992 Cr LJ 2168 (Mad) where the advice of an advocate to his client to remain absconding was not allowed to be cited in the prosecution of the advocate under Terrorist and Disruptive Activities Prevention Act 1987 (*V Muraleedharan v. NJ Antony* 1985 Cr LJ 633, *Maneka Sanjay Gandhi v. Ram Jethmalani* AIR 1979 SC 468)

or that he should have accepted the brief. Even if vakil rejects the case, the communications made to him must remain protected. The scope of the protection is that it will apply only to such communications as have been made for the purpose of professional employment and also to the advice given by the vakil. It also extends to the contents of any document which came to his knowledge in the course of such employment

Exceptions

This privilege is subject to few exceptions. Firstly communications made in furtherance of an illegal purpose is not protected⁴⁸. Secondly if a lawyer finds in the course of his employment that any crime or fraud has been committed since the employment began, he can disclose such information⁴⁹. Thirdly such communications can be disclosed with the express consent of the client. Fourthly if the communication is overheard by third person, he may be compelled to disclose. There is no privilege to communication made before the creation of relationship of pleader and client⁵⁰.

Professional communication between Doctor and Patient

In a doctor patient relationship, the patient trust the doctor and reveals all confidential information about him to the doctor. In India, the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations 2002⁵¹ speaks about patience, delicacy and secrecy under section 2.2. This is covered under chapter 2 which deals with duties of doctors towards patients. The section states that confidences concerning individual or domestic life entrusted by patients to a physician and defects in the disposition or character of patients observed during medical attendance should never be revealed. The Code of Ethics also provides some exceptions like the need for involvement of other health professionals for better or alternative treatment, or for ensuring safety of the patient from themselves, or when asked by court of law.

It is the bounden duty of all health professionals to keep the patient's information obtained during care or treatment confidential. The code of ethics is providing some responsibilities to the doctors, but at the same time, it is not absolute in nature. It has exceptions including the need for involvement of other health professionals for improvement in treatment, disclosing information for ensuring the safety of the patient or when asked by a court of law. The Code of Ethics as per Rule 7.14 states that the physician is not supposed to disclose the secrets of a patient which he has come to know about during

⁴⁷ Avtar Singh, Supra note 36 at 533

⁴⁸ *R. V. Cox 14 QBD 153, Russel v. Jackson* 21 LJ Ch 146, *Kelly v. Jackson* 13 Eq R 129

⁴⁹ *R. V. Downer 14 Cox 486*

⁵⁰ Ratanlal and Dhirajlal, Ahmadkhan The Law of Evidence 738 (26th edn 2017, LexisNexis)

⁵¹ These Regulations are made by the Medical Council of India exercising the powers under section 20 A read with section 33 (m) of the *Indian Medical Council Act 1956*.

medical examination except in a court of law under orders of the presiding judge. Physician can disclose these information in circumstances where there is a serious and identified risk to a specific person or community or in the case of notifiable diseases. The consequences of violation is given under chapter 8.2 If there is a complaint of professional misconduct against any registered medical practitioner, and if it is brought before Medical Council, the council will hold inquiry. If the medical practitioner is found guilty of committing professional misconduct, he will be punished and the council may remove the medical practitioner for a specific period.

The council may restrict the physician from performing the procedure or practice during the pendency of complaint. Other than the Code of Ethics, there is no legislation in India for regulating doctor patient relation. The law proposed is known as Digital Information Security in Healthcare Act (DISHA). The Act is intended to provide electronic health data privacy, confidentiality, security and standardization and also the establishment of National Digital Health Authority and health Information Exchanges. There are legislations in other countries to protect personal information of patients. The US law is *Health Insurance Portability and Accountability Act 1996 (HIPAA)* which ensures legal framework for privacy and protection of health information and ensures that patients have substantial control over their personal health information.

The fair expectation of mutual trust is the base of any confidential relation. Patients share their sensitive and secret information to the doctor and the doctor can diagnose and provide proper treatment only if all the details of the patient are collected. If at any point of time, the patient feels that the information is not protected or it is being leaked, they might not reveal the information. The purpose of this professional secrecy in medical field is to protect the interest of the patient.

Professional secrecy of Chartered Accountants (CA)

A chartered accountant is having a duty to keep confidential all information he received from the client. CA deals with financial records of individuals and institutions and it is to be kept secret always. People would always like to keep their financial transactions secret and if it is disclosed by the CA, it may affect their business and future. This profession and the conduct of the professionals are governed under the Chartered Accountants Act, 1949. This Act is enacted with the view to provide regulations for the profession of Chartered Accountants. The profession is regulated by the Institute of Chartered Accountants of India (ICAI) established under the Act. The ICAI regulates the profession through the Council which lays down the standards of the profession. Ethical Standards Board is also set up by the ICAI as a standard setting body. This Board works towards the excellence of the professionals. It sets Code of Ethics for Professional Accountants according to local laws and also taking into consideration international standards. The Code recognizes the

objectives of the Accountancy profession, which include credibility, professionalism, confidence and quality of services. This Code has great value in the society and it announces to the public that the professionals would adhere to the same and would exercise their duties only in public interest.

Section 140 of the code of Ethics for Chartered Accountants deals with confidentiality. A professional accountant is refrained from disclosing information without proper authority⁵². He is not supposed to use the information to his personal advantage or the advantage of third parties⁵³. He should make it sure that the staff employed by him also takes proper care for maintaining the secrecy of the information of the client⁵⁴. The necessity to maintain confidentiality exists even after the relation between the clients is over. At the same time, as in all professional communications, there is also some exceptions when the professional accountant can reveal the information obtained during professional relation. When the disclosure is permitted by law and is authorised by a client, it can be disclosed⁵⁵.

Disclosure is permissible for producing before legal proceedings⁵⁶ or before the public authorities for infringement of law⁵⁷. Disclosure is also permissible during investigations and for protecting the interests of the profession.

Conclusion

Privacy is not given a conclusive or comprehensive definition. Even after centuries of discussion regarding the definition of privacy, there still has confusions with respect to the nature of interest which privacy is designed to protect. It is the right or freedom of individual to decide the extent to which his opinions and beliefs are to be disclosed to others. Though many international and national instruments ensure privacy of individuals, no definition is universally adopted. One thing cannot be denied that privacy in certain relations are to be respected. So many legislations in India protect and respect privacy in one or the other form in matters of marriage, divorce, certain offences etc. As seen provided in the Indian Evidence Act, it protects privileged communications from being admissible as evidence. Criminal laws and Information Technology Law also protect privacy. As far as professional relations are concerned, privacy in that relationship is most important. This provides individual with opportunity for sharing confidential informations. The individual can completely disclose information as he is aware of the punishments if it is revealed by the professional. When professionally competent persons listens to the problems and provide advice, their

⁵² Section 140.1 a., Code of Ethics

⁵³ Section 140.1.b, Ibid

⁵⁴ Section 140.5, Ibid

⁵⁵ Section 140.7.a, Ibid

⁵⁶ Section 140.7.b.(i) Ibid

⁵⁷ Section 140.7.b.(ii) Ibid

professional standards and position in the society is an assurance to the individual that these information won't be used against him later. In fact, professional secrecy is for the protection of the client and it safeguards the identity of the client. A professional whether Doctor, Advocate or Chartered Accountant is under a moral obligation to respect the confidence reposed in him and is not supposed to disclose the information revealed to him by the individual in a professional confidence.

GENERAL FACET OF RIGHT TO PRIVACY AND FREEDOM OF SPEECH

Abha Singh*

Abstract

This paper is related to right to privacy and freedom of speech which has been guaranteed by the Constitution of India. The article focuses on the general aspect on the application of the right to privacy as guaranteed under Article 21 and freedom of speech as given under Article 19(1)(a) of the Indian Constitution as the fundamental right to its citizens. Similarly, Right to Privacy and Freedom of Speech is one of the most important and necessary right of the citizens. Though privacy and freedom of speech are considered complementary to each other but there has been an argument which creates a chilling effect on individual action and prevents them from exercising their rights and liberties. There has been debate and discussions on the importance of privacy which is a shield to protect the freedom of speech. Right to Privacy is a right which an individual enjoys by birth. Thus, privacy means the right of an individual to be left alone which is recognised by common law¹. The Right to Privacy can be both negatively and positively defined. The negative Right to Privacy involves that individuals are protected from undesirable interference by both the state and private actors into their life. The positive right requires an obligation of states to remove hindrances for a self-governing shaping of individual identities.

I INTRODUCTION:

The Constitution of India has given various fundamental rights to its citizens. Similarly, Right to Privacy and Freedom of Speech is one of the most important and necessary right of the citizens. Though privacy and freedom of speech are considered complementary to each other but there has been an argument which creates a chilling effect on individual action and prevents them from exercising their rights and liberties.

There has been debate and discussions on the importance of privacy which is a shield to protect the freedom of speech. Right to privacy is a right which an individual enjoys by birth. Consequently, privacy is the right of an individual which is to be left alone and is recognised by common law².

* PhD scholar, University of Petroleum and Energy Studies, Dehradun, India

¹ Emily Howie, Protecting the human right to freedom of expression in international law, 2017, International Journal of Speech-Language Pathology, Taylor and Francis

² Kristian P. Humble, International law, surveillance and the protection of privacy, 2020, The International Journal of Human Rights, Routledge Taylor and Francis.

The Constitution of India, 1950 under its Preamble guarantees liberty of thought, expression, belief, faith and worship to all the citizens of the country. Article 21 of the Constitution of India which embraces the word “personal liberty” divulges that for an individual to lead a dignified life, liberty should be protected which in due course demand right to privacy to be given legal recognition. Article 21 is the heart and soul of the Indian Constitution, which speaks of the right to life and personal liberty. Right to life is one of the basic fundamental rights and the state also does not have the authority to violate or take away that right. Right to dignity has been recognised to be an essential part of the right to life and ensues to everyone on account of being humans. The Right to privacy can be defined in two ways that is negatively and positively. The negative right to Privacy involves the individuals are protect from undesirable interference by both the state and private actors into their life. The positive right requires an obligation of states to remove hindrances for a self-governing shaping of individual identities.

INTERNATIONAL ASPECT:

The privacy has been recognised as a value of fundamental constitutional part of India's commitment to a global human rights regime. Article 51 of the Indian Constitution, 1950 forms part of the Directive Principles of State Policy which has been adopted from Irish Constitution by the makers of the Constitution of India, requires the State to endeavour to nurture respect for global law and treaty requirements in the dealings of organised peoples with one another³. Article 12 of Universal Declaration of Human Rights, recognises the right to privacy which says that “ No one shall be subjected to uninformed meddling with his privacy, family, home or correspondence, nor to bout upon his honour and status”.

Similarly, the International Covenant on Civil and Political Rights in its Article 17 provides that “No one shall be subjected to an illogical and illicit interference with his/her privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation, and that all and sundry has right to the shield of the law against such nosy”.

In order to have a clear-cut understanding of Right to Privacy in Indian Constitution. It is necessary to have a thorough knowledge about USA privacy laws since Indian judiciary relied upon those laws for the interpretation of private matters.

In many of the nations where privacy is not overtly recognized in the Constitution, such as the United States, Ireland and India, the courts have found that right in other provisions of laws. In the early 1970s, countries began adopting extensive laws which were envisioned to protect individual privacy. All over the world, there is a general movement

³ Jennifer Holt and Steven Malcic, *The Privacy Ecosystem: Regulating Digital Identity in the United States and European Union*, 2015, *Journal of Information Policy*, Penn State University Press.

towards the acceptance of comprehensive privacy laws that set a framework for protection. Maximum of these laws are based on the models introduced by the Organization for Economic Cooperation and Development and the Council of Europe⁴.

In 1995, aware both of the shortcomings of law, and the many differences in the level of protection in each of its States, the European Union passed a Europe-wide directive which will provide citizens with a wider range of protections over exploitations of their data. The order on the "Guarding of Individuals with regard to the meting out of personal data and on the free movement of such data" sets a scale for national law. Each European Union State must pass corresponding legislation by October 1998.

The Directive also imposes an obligation on member States to warrant that the personal information relating to European citizens is covered by law when it is exported to, and processed in, countries outside Europe. This prerequisite has brought about in growing pressure outside Europe for the passage of privacy laws. More than forty countries now have data protection or information privacy laws and many others are in the process of being enacted.

III. INDIAN CONTEXT:

The right to privacy came into being after the broadening the dimensions of the vital fundamental right which is Article 21 of the Indian Constitution. The Black's Law Dictionary has precisely defined the term Privacy as “right to be let on your own; the right of a person to be free from any needless publicity; the right to live without any meddling by the public in matters with which public is not necessarily concerned”.

The Right to Privacy has not been defined anywhere in the Constitution of India nor has been enumerated as a Fundamental Right in the Constitution under Article 21 which states that “No person shall be destitute of his life or personal liberty except conferring to the procedure established by regulation”.

In the popular case of *Kharak Singh v. The State of U.P.*⁵ A minority opinion recognized the right to privacy as a fundamental right. The minority magistrates said that right to confidentiality was both the right to personal liberty and freedom of movement as well. *Govind v. State of M.P.*⁶ In this case, the Supreme Court confirmed that the right to privacy is a fundamental right. The right was said to include and protect personal intimacies of the home, marriage, family, motherhood, etc. but it also detected that it was subject to “captivating state subject”.

⁴ Vishal Rakhecha, Privacy, the shield that protects or the sword that strikes freedom of speech?, 2021, Routledge Taylor and Francis Group

⁵ 1964 SCR (1) 332

⁶ 1975 SCR (3) 946

Yet in another case of *People's Union for Civil Liberties v. Union of India*⁷ the Supreme Court extended the right to privacy to communications. The court laid down regulations in intervention provisions in the country like such orders were to be dispensed by the home secretaries only, stipulation of the information was the considered, etc. The Central Bureau of Investigation sought access to the huge database conformed by the Unique Identity Authority of India for the obstinacies of examining a criminal offence. The Apex Court, however, said that the UIDAI was not to transfer any biometrics without the consent of the person.

There are various enactments that have been adopted prior to the Constitution of India which acknowledges the right to privacy both as a right between the individuals and the government as well as between the individuals. These requirements are:

1. Section 126-129 of *The Indian Evidence Act, 1872* which deals with the protecting certain classes of communication as privileged
2. Section 4 of *The Indian Easements Act, 1882* which states defining easements as the right to choose how to use and enjoy a given piece of land
3. Section 5(2) of *The Indian Telegraph Act, 1885* specifying the permissible grounds for the government to order the interception of messages
4. Section 5 and 6 of *The Bankers Books (Evidence) Act, 1891* mandating a court order for the production and inspection of Bank records
5. Section 25 and 26 of *The Indian Post Office Act, 1898* specifying the permissible grounds for the interception of postal articles and themselves becoming agents of political power qua the state

In the case of Justice *K.S. Puttaswamy v. Union of India and others*⁸, The government of India decided to provide to all its citizens a unique identity known as Aadhar which is card containing 12-digit number. The registration of this card was made compulsory so as to permit the people to file tax returns, opening bank accounts, etc. Though, the process of registering for such card required the citizens to give their biometrics such as fingerprints, iris scans etc. Retired Justice K.S. Puttaswamy filed a petition challenging the constitutional validity of this Aadhar project challenging that there was a violation of right to privacy of the citizens since, the registration for Aadhar is made mandatory. As upshot of which all those who don't even want to register themselves, are not left with any option. Additionally, there is a lack of data protection laws in India and henceforth, there are chances that the private information of people may be seeped if proper care is not taken. This will lead to violation of Right to Privacy of individuals. It was held that Privacy is a constitutionally protected right

⁷ AIR 1997 SC 568

⁸ WRIT PETITION (CIVIL) NO. 494 OF 2012

which not only arises from the guarantee of life and personal liberty in Article 21 of the Constitution, but also ascends in fluctuating contexts from the other facets of freedom and dignity recognised and guaranteed by the Fundamental Rights contained in Part III of the Indian Constitution⁹.

In India, freedom of expression under Article 19 (1)(a) is not limitless. While the Constitution vows freedom of speech and expression, it also imposes “reasonable restrictions” on this fundamental human right. Earlier than 2015, the legislation separated online and offline expression into two types. Anybody who uploaded anything that was enormously aggressive, troublesome, injurious, threatening, or insulting in nature may be confined for up to three years under Section 66A of *India's Information Technology Act, 2000*. In a historic decision

*in Shreya Singhal v. Union of India*¹⁰, the Apex Court of India knocked down this excessively harsh and severe clause for violating the constitutionally given right to free speech and expression. In this case, the Supreme Court pardoned content hosting platforms such as search engines and social media websites from constantly monitoring their platforms for prohibited content, enhancing the prevailing safe-harbour protection or legal protection given to internet companies for content posted by their users. “Only official government authorities and the judiciary might legitimately request that internet companies remove information”, according to the Court. This was a turning point in India's online free-speech legislation, as content compering platforms are the caretakers of digital expression. The right to freedom of expression refers to the capability to express oneself without interference, and it is unaffected by any restrictions.

Written and verbal communications, the media, public protest, broadcasting, creative works, and commercial advertising are all protected under the Right to Freedom of Speech. It derives with unique obligations and may be constrained for a variety of reasons. Restrictions might be imposed on access to particular websites or the advancement of vehemence.

VI STRUGGLE BETWEEN THE RIGHT TO PRIVACY AND FREEDOM OF SPEECH AND EXPRESSION:

The Right to Privacy and Freedom of Expression are pretty often interconnected rights; however, they might come into battle in certain circumstances, such as when privacy claims are used without justification to prevent the distribution of information about individuals in order to limit reporting on matters of public interest and to avoid public analysis, or consciously delude others. At the same time, conceding that the unnecessary disclosure of private information may intrude severely on the Right to Privacy, particularly

⁹ Mariyam Kamil, Puttaswamy: Jury still out on some privacy concerns?, 2017, Indian Law Review

of individuals in vulnerable circumstances.

In order to promote a see-through framework for the protection of both freedom of expression and privacy rights wherever they battle particularly in virtual space, one must take into consideration the relevant provisions of the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), the African Charter on Human and Peoples' Rights

African Charter on Human and Peoples' Rights, and the American Convention on Human and Peoples' Rights; the European Convention on Human Rights and the EU Charter of Fundamental Rights and Freedom.

The Internet is a worldwide resource that should be managed in the community interest. Digital technologies have improved freedom of expression and access to information while also posing noteworthy challenges to the protection of individuals' right to privacy and personal data. There are various issues regarding the thoughtful risks stood to the right to privacy of an individual and their personal data when massive data is released for societal benefits.

V CONCLUSION:

The Right to Privacy and freedom of speech is a Fundamental Right. It is a right which protects the internal domain of the individual from meddling with both state and non-state actors and allows the individuals to make independent life choices. The inference can be drawn that India relied upon the US Constitution and UDHR for the interpretation of Right to Privacy and freedom of speech within Indian sphere, therefore it can be articulated that American Constitution and UDHR has crucial and significant role in moulding of Right to privacy in precise shape. It was constantly detected that Right to Privacy is derived from Right to Life and Personal Liberty. It is correctly articulated that the technology has made it possible to cross the threshold and this is equally possible both by the state and non-state actor. The privacy of the home must protect the family, marriage, procreation and sexual orientation which are all important aspects of dignity. The Right to live with dignity and the right to privacy both are now recognised as dimensions of Article 21 of the Constitution of India. Both these rights and freedom are the part of golden triangle and one must not be deprived of these rights and freedoms as guaranteed by the Constitution of India.

¹⁰ WRIT PETITION (CIVIL) NO.21 OF 2013

The Impact of Information Technology Act on the Right to Privacy

Ms. Deeksha Kumari*

Abstract

Right to Privacy in today's era has become crucial and important human right which could be traced from the judgments of Supreme Court. Right to Privacy is a right that has been one of the branches of right to life and personal liberty as encompassed under article 21 of Indian Constitution. Today a lot of debate and discussion is going on about the aspect that is making Aadhar card mandatory for availing any service valid or not. Here, the paper attempts to analyze the provisions of information technology act which effects the right to privacy. Information Technology act 2000 is a legislative provision which was enacted for the transactions that are carried out by means of electronic data interchange and other means of "electronic communication." Which involve the use of virtual platform to conduct the transactions. This might lead to data theft which can violate the right of privacy the individual using the virtual platform for transactions. Data theft is a cybercrime in which the person stealing the data available by hacking a network and using it to the adverse interest of the individual. This data theft is intrusion of the third person in the life of individual without being informed and it effects and violates the right to privacy which is the fundamental right of the citizen of India.

I. Introduction

The world has changed, and the coming of new technologies the privacy of the individuals are hampered. Internet has brought the world close as now through virtual platform anyone can connect with the other person at the ease of sitting in their own space. With this the dissemination of personal information of individual has also become easy. As now everything has shifted from physical to online all the data and information now a days are being saved on google drive or online apps. Every individual since its birth has some rights that vests in the individual and one of the rights is to have his own personal space. Right to privacy is recognized by the international law as one of the basic rights. Indian Constitution also talks about the right to privacy which is included under right to life and personal liberty as enshrined under Article 21.

* Assistant Professor, IILM University, Gurugram, Haryana

In today's era the right to privacy has become a complex right. It is very difficult to identify when exactly your right to privacy gets hampered. It has become important and crucial topic in the ever-changing times. The research paper tries to examine the impact of information technology on the right to privacy. It explores the concept of right to privacy and how it is changing with the changing times. It also examines the laws and then suggests the changes that could be helpful in protecting the privacy of individuals.

II. Concept of Privacy

It is important to understand what the word “Privacy” means. According to Black's Law Dictionary “Right to be let alone, the right of a person to be free from any unwarranted publicity the right to live without any unwarranted interference by the public in matters with which public is not necessarily concerned¹.

• Constitutional Privacy

The scope of right to privacy first came up for consideration in **Kharak Singh's Case**² which was concerned with the validity of certain regulations that permitted surveillance of suspects.

Article 19(1) (d) the right to privacy was again considered by the Supreme Court in 1975. The right to privacy is one of the fundamental rights that is explicit under Article 21 right to life and personal liberty³. By the term “Right to Life” we mean the right to have an existence that is not just the animal existence. The right to privacy is an element of various legal traditions to restrain governmental and private actions that threaten the privacy of individuals over 150 national constitutions mention the right to privacy. Information is of two kinds one personal and the other non-personal information. Personal information refers to any information that can be used to identify an individual internet.

The issues related to privacy can be traced in number of cases. The aspect can be said to relate to his basic human right which he or she can claim against the state through the disclosure of Fundamental Rights guaranteed under part III of the Constitution of India.

The issue of privacy relating to various aspects like body, cyberspace, identity etc. has existed from the beginning when technological advancement started. In 2017 judgment the issue pertaining to right to privacy got media coverage. In the judgment of *K.S. Puttuswamy v. Union of India*⁴ this case also popularly known as the Aadhar case where justice Dr. D.Y. Chandrachud addressed the challenges relating to the right of privacy which is explicit under Article 21 of the Indian Constitution. We are aware that the Aadhar Project

¹ Black's Law Dictionary, Definition of RIGHT OF PRIVACY Law Dictionary TheLaw.com

² *Kharak Singh v. The State of Uttar Pradesh and others*, AIR 1963, 1295, 18 December 1962.

³ The Constitution of India, Article 21 “Right to Life and Personal Liberty”.

⁴ *K.S. Puttuswamy v. Union of India*, 26 September 2018

was carried out by Central Government, the government gathered numbers and demographic biometric data which was sensitive data to let its subject profit offices which individuals thought could be abused effectively with most recent innovation. In this judgment a nine-judge bench held Right to Privacy as the utmost important right under part III of Constitution of India.

- **Information Privacy**

Internet privacy is one of the most crucial aspects. It involves the right or mandate of personal privacy concerning the storing, repurposing provision to third parties and displaying of information pertaining to oneself via the internet. The term Information

privacy means the privacy of personal information and usually relates to personal data that is stored on system.

There is a need to have information privacy regulation that is applicable to collected personal information such as medical records, financial data, criminal records, political records, business related information or website data. The data privacy relates to various data types which includes:

- a. Online privacy
- b. Financial privacy
- c. Medical privacy

We are living in the era where now to avail any of the services like banking service we no longer stand in long lines in front of banks. we can just from a click get our products delivered. The information technology sector has boomed. There are various apps that have been launched only in covid 19 pandemic which help person in sending or receiving products etc. sitting at their homes. It has become important that the sensitive information of the individuals is kept confidential. Data privacy refers to the authority or determination of the information holder as to what extent the data or information shall be made accessible to the third party. Most of the information is sensitive in nature. They include data of various nature, like economic, defense, medical, financial, educational, etc. Information holders, who are generally organizations, have the major responsibility of protecting the data as there are chances that if it falls into the wrong hands, they might be misused and cause harm to the owner of the information⁵.

- **Moral reasons for Protecting Personal Data**

Today data is becoming very important and the skills and expertise to retrieve different kinds of data are also evolving fast. Ignorant and careless behavior in processing

⁵ Debapriya Majumder, Data Privacy Laws in India, All You Need To Know About Data Privacy Laws In India (ipleaders.in)

personal data can cause harm to persons. The purpose of protection of data is to protect personal information as well as to protect and uphold the fundamental rights and the freedom of persons as enumerated by the Constitution of India that relates to personal data. It should be ensured that while protecting personal data the person's rights and freedoms are also protected. It should be an endeavor that the individuals comply with personal data protection regulations as non-compliance can lead to hard situations where it might be possible to extract the money from a person's bank account etc.

Regulations pertaining to information protection is necessary to ensure fair and consumer friendly services. The regulations create a situation where the confidential information can't be sold freely, and the individual has greater control.

III. The Impact of Information Technology on Privacy

The arguments on the right to privacy revolve around the coming up of new technology. Information technology involves the use of computers and the communication networks. The amount of information that can be stored or processed in any information system depends on the kind of technology used. In the past decades the capacity of the technology has increased. Now in the current scenario we can store and process data on the exabyte level⁶. This rapid change have increased the need for careful consideration of the desirability of the effects. Technology has posed a lot of questions that discusses about the scope of right to privacy⁷.

The twenty first century has brought the world closer where the advanced technology has interconnected the world economies, different cultures and populations. The data shows that India has over 400 million internet users as of 2018. India is ranked as second largest internet population country on earth.

While its prominent usage it can lead to enormous progress at the same time it leaves our computerized social orders open to new weaknesses.

Cyber crime has no boundaries. It can be done sitting anywhere on the earth with the use of technology. The NCRB's data states that the total of 44546 cases of cyber crimes was registered in 2019 which is way more than the tally of 2018 where 28,248 cyber crime cases were reported. The rate of cyber crime is increasing in India. The spike in the increased number of cases could be seen in the lockdown of Covid-19. A spike of 350% can be seen in the phishing websites with various other cyber-crimes against women⁸.

⁶ Privacy and Information Technology, Stanford Encyclopedia of Philosophy, 30 November 2014, Privacy and Information Technology (Stanford Encyclopedia of Philosophy)

⁷ Privacy and Information Technology, Stanford Encyclopedia of Philosophy, 30 November 2014, Privacy and Information Technology (Stanford Encyclopedia of Philosophy)

⁸ Yash raj Verma & Apurva Surve, Technology: A threat to Privacy, 5 November 2020, *Technology: a threat to Privacy* - iPleaders

IV. Law, Regulation, and Indirect Control Over Access

Excessive collection of data might have an adverse effect on society narrowing individual right to freedom of speech, freedom of expression because of the fear of threat. The relevant law that deals with the data protection are the information technology act. It provides for various laws and punishments to prevent misuse of data and protect the individuals from the cybercrimes which breach the confidentiality and privacy. There are directions that have been given by central government sought to prevent any misuse and abuse of personal data laying down comprehensive rules to protect data.

Section 43 A⁹ of the Information technology act specifies the compensation for failure to protect data. This section was inserted and came into enforcement on 27.10.2009 which states that where a body corporate has any information or deal with any sensitive personal data or information in a computer resource which it owns, controls or operates is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so effected. The explanation discussed the definition that pertains to “Sensitive Personal Data or information” it means the personal information as

prescribed by the central government in consultation with such professional bodies, or associates as it may deem fit¹⁰.

Further section 66E specifically talks about the punishment for violation of privacy. It says that “whoever intentionally or knowingly captures, publishes or transmits the image of a private area of any person with out his or her consent, under circumstances violating the privacy of that person shall be punished with imprisonment which may extend to three years or the fine which not exceeding 2 lakh rupees or with both¹¹.”

The explanation talks of only the privacy which relates to private body parts¹².

Here the privacy covered here is only which relates to the personal parts and this section lacks to cover the privacy that relates to personal data or information which is private to individuals.

V. Conclusion

The concept of privacy has changed a lot since the coming of Industrialization and Globalization. The world has become small with the coming up of technology. With this where we get the benefit of connecting people all over the world sitting in our rooms, we are

⁹ *Information Technology Act 2000*, Section 43A

¹⁰ *Information Technology Act 2000*, Section 43A, explanation iii

¹¹ *Information Technology Act, 2000*, Section 66E

¹² *Information Technology Act, 2000*, Section 66E, Explanation

also at risk of losing our personal information which is disseminated on various platforms by us. We do have laws for securing our personal data, but these laws are ineffective and does not cover the aspect relating to dissemination of our personal data. Hence, India needs to bring forth stringent laws which would indeed prove efficient in tackling the issue of breach of privacy which is our fundamental right given by the Supreme Law of the land. It is the duty of the State to protect and promote the rights of citizens. If India comes up with certain laws which handles the issue aptly then nothing can stop our nation from developing using the latest technology. In the era of Artificial intelligence the government can think of coming up with different program which will empower nation and fulfill the need of the hour.

A Study on Critical Analysis of Right to Privacy and Media Trial in India

Ms. Poonam Kumari*

Abstract

Even before India became Independent, it had already become party to the United Nations Declaration on Human Rights 1948 (UDHR). Press had played a very important and productive role in the independence movement, through its strong support for the popular movement of Satyagraha and abdication of foreign goods and other similar forms of freedom struggle. Such was the impact of the print media that it frightened the British, as it gave a picture of a strong India, though the reality was a disintegrated India ruled by princely kings and people in deep poverty. The framers of our Constitution knew the immense power vested in the print media, therefore they imbibed the Freedom of Speech and Expression in Article 19(1) (a) of the Indian Constitution from Article 19 of the UDHR, and also reflected similarly in Article 19 of the International Covenant on Civil and Political Rights 1966 (ICCPR). UDHR 1948 in Article 12 and ICCPR 1966 in Article 17 give protection to the concept of privacy. Though freedom of speech and expression given in Article 19 of the UDHR 1948 and ICCPR 1966 was enshrined in Article 19(1)(a) of the Indian Constitution. We do not find such constitutional recognition given to privacy in India. Here, privacy is not given any separate constitutional status. Right to life, liberty and security of person is enshrined in Article 3 of the UDHR 1948. This is recognized in Article 21 of the Indian Constitution. Privacy was not included in this Article. In Nihal Chand v. Bhagwan Dei during the colonial period, as early as in 1935, the High Court recognized the independent existence of privacy from the customs and traditions of India. But privacy got recognition in free India for the first time in Kharak Singh case. In Kharak Singh v. State of U.P., the Supreme Court struck down domiciliary visits by the police as it violates Article 21. But it was in the minority view given in this case by Justice Subha Rao, that privacy got recognition as a right included in Article 21 of the Constitution. In this case the apex court recognized privacy as part of right to life and personal liberty. Privacy was recognized as a separate right in UDHR 1948. This has failed to materialize in the same spirit as a

*

Pursing Ph.d in Constitution Law from Uttarkand University, Dehradun

fundamental right in the Indian Constitution, like the right to speech and expression and right to life. Article 3 of the UDHR 1948, protects life and personal liberty, not privacy. In India privacy is described as part of right to life and personal liberty in Article 21 of the Constitution as there is no separate provision for privacy in the Constitution. Privacy has been defined by Supreme Court in Sharada v. Dharampal as 'the state of being free from intrusion or disturbance in one's private life or affairs'. This is different and distinct from the life and liberty in Article 21 of the Constitution. India being signatory and party to the UDHR1948 is bound to protect Privacy as a fundamental right in the Constitution and also to give a higher status to it in reference to Press.

Keywords: Privacy, Article 21, Press, Indian Constitution, Liberty, Law Commission of India

Introduction

Privacy is a concept that has been dominantly accepted in the history & religion of the world. The significance of privacy has, in various ways always been referenced & perceived by numerous individual scriptures, traditional reviews, & messages. The Quran perceives the concept of privacy & the proof of it, is evident in the Saying of the prophet Mohammad. The idea of privacy can likewise be found in the Bible & in the Jewish laws as well, as the idea of "opportunity for being not viewed". The English author Sir George Orwell, anticipated 50 years ago that there will be an authoritarian state & people would be under observation using advance innovation & the "privacy" would turn into a relic of past times & "and Boss would watch us & privacy be would be censured for the sake of safety of the state"¹

The U.N declaration of human rights, the global treaty on social & political rights just as in numerous other provincial & universal arrangements it perceives privacy as the basic human right. & today it has turned into the most heated problem that is begging to be addressed of the 21st century. Today about every nation of world has accepted the privilege to privacy & have successfully enshrined this achievement completely in their particular constitutions. Indeed, even the latest composed constitution of government of South Africa & Hungary accommodates by expressly providing the right with respect to access & control of people's individual data.

Indeed, even in the states like India, The United states, Ireland where their particular

¹ Pandurang Vaman, *History of Dharma Shastra* 58, (Bhandarkar Oriental Research Institute, Poona, 5th edn., 2010).

constitutions doesn't provide for privacy as unequivocally as the others, the legal set up of their particular countries have discovered the privilege by method for either legal elucidation or construction & interpretation of their constitution. As precedent, India perceives the right to privacy as provided in Article 21 of Indian constitution. In numerous international treaties that perceive privacy rights, the law regarding the right to Privacy which has been deliberated upon by many of the international convention of the world for example as mentioned above U.N.G.A and the international convention on the political and civil rights or the EU Convention. The collaboration of the nations of the world nations has explicitly adopted the principle of the right to privacy and the model recommended by them.

RIGHT TO PRIVACY UNDER INDIAN CONSTITUTION

The father of the Indian constitution DR. BHIM RAO AMBEDKAR has not mentioned or has not specifically provided for the Right to Privacy because at the time there was no need of this particular right. But Dr. Ambedkar in the meetings of their constitution drafting committee had a reserved opinion about the right to privacy. The opinion of late Dr Ambedkar has in the recent times found its way back through the constitution of India. As under article 21 of the Indian Constitution & included within the meaning of “life & liberty” by the supreme court of India in recent times.

The constitution is the tombstone of every right that we enjoy today & therefore the incorporation of right to privacy in the constitution has made it clear that there will be a right always guaranteed & protected by the Indian Constitution.

The right to life is universal right as provided under the Art.21 of the Indian Constitution. As the right is extended to citizens and non citizen residing in the territory of India. The right to life can be said to be a foundation right to all the other Fundamental rights provided under the constitution of India. It is the most fundamental of all the other rights simply for the fact, that in order for the other rights to valid they require a pre-requisite, that is LIFE itself as the rights granted under the Part III of the Constitution of India for instance Right to Speech and Expression and alike other rights can to applicable until there exists a life or in other words a living human being in order to exert those rights. Some of the judges of the Supreme Court have also remarked about the right to life as according to Justice Iyer “it is the MAGNA CARTA of the security of Life and liberty”, further according Justice Bhagwati “the Article 21 holds utmost value in the democratic set up of the country”

Article 21 which provides for Right to Life and Liberty states that, “No person shall be deprived of his life or personal liberty except according to procedure established by law².” However the interpretation of the term life does only means mere existence or in other

² Article 21 of The Indian Constitution, 1949.

words animal like existence, but in fact the right so granted to us by the Indian Constitution life is widely interpreted by our respected Judiciary and the right covers a whole range of subsequent rights that falls within the ambit of the Right to Life and Personal Liberty for instance Right to live with dignity, right to livelihood or right to clean drinking water, etc.

The second aspect of the Article 21 of the Indian Constitution is the right to liberties. And liberties are those essential elements of the Human Life that make us distinct from the other primitive species that do not enjoy any form of liberty. Or to put it differently it the liberties due to which man is distinguishable from the animal. And under this aspect of the Article 21 of the Constitution of India which now grants us the Right to Privacy and establishes it as the fundamental Rights guaranteed under part III. The right to privacy is a recently incorporated fundamental right falling within the scope of the right to life and liberty. And was brought to existence through the Justice *K.S Puttaswamy v. Union of India*³.

In *Sunil Batra v. Delhi Administration*⁴, the S.C in the agreement to the observations made in the Kharak Singh case reinstated that right to life and liberty is inclusive of the right to maintain a healthy lifestyle and lead his life according to his cultural, personal, heritage value in accordance to his wishes.

RIGHT TO PRIVACY IN INDIAN CONSTITUTION

The Constitution of India as a rule doesn't have any express arrangement in regards to the Fundamental Right to Privacy yet at the same time by the methods for legal choices the right is supposed to be under Part III of the Constitution. Following are the arrangements which are said to have the arrangements identified with the 'right to Privacy':

- *Article 19 : Freedom of Speech and Expression-*

Part III of the Constitution of India is entitled 'Key Rights' and records a few opportunities that are viewed as essential to every single Indian individuals. Some basic rights, especially the right to life and freedom, stretch out to all people in India, regardless of whether they are not 'residents'. Article 19(1) (a) gives that "all residents will reserve the option to the right to speak freely of discourse and articulation." However, this is advocated by Article 19(2), which says that it won't impact the execution of any current law or prevent the State from making any law, to the extent that such law forces sensible limitations on the act of the right in light of a legitimate concern for India's sway and uprightness, state security, well-disposed binds with remote nations, open request, fairness or profound quality⁵. Article 13 keeps the State from making any law which damages the Part III of the constitution.

³ WRIT PETITION (CIVIL) NO 494 OF 2012

⁴ AIR 1978 SC 1675

⁵ HM Seervai, *The Constitutional Law in India : A Critical Commentary* 43 (Central Book Publication, New Delhi, 2003)

Thus, the opportunity of articulation guaranteed by Article 19(1) (a) isn't a flat out right, yet a skillful right which, under the sacred framework, is equipped for being shortened under explicit conditions.

- *Article 21 : Right to Life and Personal Liberty*

Article 21 of India's constitution gives residents and non-residents the right to protection⁶. This isn't clearly expressed in it, yet as a legal support, the Supreme Court demonstrated the equivalent. Article 21 of the Constitution states as follows: "No individual will be precluded from claiming his lives or individual flexibility aside from as gave by the methodology set up by law⁷."

Article 21 is the core of Indian individuals' opportunity. The expressions "method made by law" in this article have been the subject of discussion since the Indian constitution was sanctioned. The correct methodology that is required is that, in the circle of individual flexibility, the centrality of the activity made by law isn't unmistakable from that of the fair treatment provision of the Fifth Amendment to the American Constitution⁸.

FREEDOM OF PRESS IN INDIA

Media in the 21st Century not only includes the press but also the electronic media and the social networking sites. In India Press is considered as the fourth pillar of democracy. It acts as a watchdog on the three pillars - Legislature, Executive and Judiciary. It is included under Article 19(1) of The Constitution of India. However it has certain restrictions imposed on it as per Article 19(2).. These restrictions are imposed in the light of the sovereignty and integrity of the nation and most important with respect to the security of the state. These grounds were inserted in the Constitution through various amendments and also judicial pronouncements. *In Brij Bhushan and Another v. The State of Delhi*⁹ case Supreme Court had held that the imposition of pre-censorship on a journal is restriction on the liberty of press which is an essential part of the right to freedom of speech and expression, Press plays a very significant role for public welfare but at times it acts in a very insignificant manner. It provides information to the people from every aspect and globally. It serves as an agency of the people to gather news for them. It is because of this reason that the freedom of press has been emphasized in the democratic countries, while it was not permitted in feudal or totalitarian regimes. Apart from all these things, Media has a great responsibility to see that the information which it is imparting is true and also it is serving the public interest at large.

When Media conveys false information, it harms the reputation of the individual

⁶ Ibid.

⁷ JN Pandey, *Constitutional Law of India* 92 (Central Law Agency, New Delhi, 2007)

⁸ MP Jain, *The Constitutional Law of India*, 1175 (Lexis Nexis, New Delhi, 8th edn., 2018)

⁹ [1950] AIR 129

which is irreparable. Also, at times it is necessary to hide the identity of the individual, because the disclosure of identity causes those problems like damage to reputation, harsh opinions and comments being passed by close and far off people, and friends and colleagues. When Alex Perry a foreign Journalist published an article about Prime Minister Vajpayee's fitness, thereby questioning his ability to lead nation, the ruling party took this as the damage to the identity of Mr. Vajpayee and his invasion of privacy by doubting his abilities and skills. This Right to privacy of individuals should be rightly blended with the Right to Know. Media should gather and broadcast only that much information which is in the interest of the public at large and just not keep on prying in the private lives of Princess Diana and President Clinton, the way it did. Because news likes these are simply waste of public energy and resources. So, this is how the freedom of press exists with reasonable restrictions.

Right to Privacy as defined in Black Law dictionary is the 'the right to be let alone, the right of the person to be away from unwanted publicity. It originated under tort law. 'Right to Privacy is granted under Article 21 of the constitution of India. Supreme Court first recognized Right to privacy in *Kharak Singh v. State of Uttar Pradesh*¹⁰ in this case Article 21 was not referred to but in the subsequent case of *R. Rajagopal v. State of Tamil Nadu*¹¹ it was directly linked to Article 21. "The right to Privacy is the right to be let alone. A citizen has the right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, child bearing and education among other matters. None can Publish anything concerning the above matters without his consent whether truthful or otherwise and whether laudatory or critical. If he does so, he would be violating the right to privacy of the person concerned and would be liable in action for damages." However, this is with the exception that the publication has become a public record and publication relates to discharge of official duties of a public servant, unless the publication is proved false, malicious or is untruthful. This right has developed over a period of time and it comes with reasonable restrictions and is considered as a fundamental right. Violation of right to privacy brings action against the person violating the same. We have seen that press has violated the privacy of individuals in various ways. The Ratan Tata case that has been discussed above is the perfect example. Right to Information and Right to Privacy of Individual conflict between the press and the public at large. With the process of globalization, and development of technology, the convergence of information beyond technological barriers has become a common affair.

Supreme Court held that in a case, that the petitioners have a right to publish what they allege to be the autobiography of Auto Shankar in so far as it appears from the public records and also his consent is not required. However, if they go beyond that and publish his

¹⁰ 1964 SCR (1) 332.

¹¹ 1994 SCC (6) 632

life story, they might invade his right to privacy. Examples are many in which media has crosses its limit of fair reporting in cases. There was a case of brutal murder of a 14-year-old teenager in Noida in which media recklessly reported the incident and tarnished the reputation of the victim and her parents. The court clarified in this case that transparency is something and secrecy in investigation is another¹².

David Feldman argues that privacy of an individual is limited by three factors out of which one of them is state's responsibility for the welfare of the citizen. Another one is the need for regulation in financial services, industries and professions. Thirdly, there is the aspect of public interest. When there is conflict between the right to privacy of individual and right to know of citizens, at that point the right to know will prevail as it serves larger public interest. In *State of U.P v. Raj Narain*¹³ the right to know of the citizen is defended by the court. Privacy and defamation are two different concepts. Privacy is all about true information whereas defamation is about false information. However, a fictionalized non-defamatory story can invade the right to privacy. It is seen that Newsworthiness is an exception to the right of privacy of the individual. It is the most convenient defense for the press. Public interests, figures and records are the three basic aspects of newsworthiness.

CONCLUSION

A study of the development of privacy traces back to *Nihal Chand v. Bhagwan Dei* in 1935, where the High Court recognized the independent existence of privacy from the customs and traditions of India. India even before independence became a member of UN and was signatory to the UDHR 1948. The UDHR was almost fully incorporated into the Indian Constitution. One of the exceptions to it was the giving no recognition to the concept of privacy. UDHR gave privacy a foremost position in Article 12, while freedom of speech and expression found place only in Article 19. Article 19 was subject to conditions such as reputation, national security, and public order and of morals. In the Indian Constitution, the restrictions imposed on freedom of speech and expression in Article 19(2) was on the lines of libel, slander, defamation, contempt of court or any matter which offends against decency or morality or which undermines the security of or tends to overthrow the state. This clause was later amended by the 1st Amendment Act of 1951, and a new clause was inserted instead of the above clause. The new clause brought reasonable restrictions on the lines of security of state, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence. This took away further, the grounds of restrictions in the earlier unamended clause i.e. libel and slander.

Freedom of Press was included in this right to speech and expression by the Apex

¹² Bindu Singhal, 'Role of Media and Right to Privacy in India Legal Perspective' [2013] MLJ 130
¹³ 1975 AIR 865

Court in *Romesh Thapper v. State of Madras*. Here the Court held that this freedom includes right to propagate ideas including the right to circulate. All the above factors further gave impetus to press but at the same time the right of an individual to plead right to privacy against undue interference by press was completely denied as this right to privacy was not given an independent status as a fundamental right on the same footing as of freedom of press in the Constitution. The framers of the Constitution failed to imbibe the full spirit of UDHR 1948 by neglecting to recognize the right to privacy as a fundamental right.

It was in *Kharak Singh*, that the Apex Court had the opportunity to discuss privacy for the first time, wherein it struck down domiciliary visits on an accused under Article 21 of the Constitution. But it was only through the minority view of Justice Subha Rao, that privacy found a place in Article 21 of the Constitution. This was due to lack of an article on privacy. Article 21 of the Indian Constitution protects life and personal liberty which is on the lines of Article 3 of the UDHR. Therefore Article 21 is not the solution to the problem faced in the matter of privacy protection. Article 21 is only an interim relief till legislative weapons are put in action to bring in a parallel Article on the lines with Article 12 of the UDHR in the Indian Constitution to protect Privacy.

Due to lack of Constitutional and legislative measures to protect privacy, the victims of press abuse had to take the help of tort law. Tort law did not refer to privacy but only other offences such as libel, slander, defamation, morality and decency. These different offences form part of the term 'Privacy' but individually these offences could never fulfill the need of protection of privacy faced by individuals. Even Indian penal code allowed punishment or penalty for the above offences but not for privacy.

RIGHT TO PRIVACY: A STUDY INTO THE RAMPANT VIOLATION OF THE RIGHT

Megha Middha* & Navna Singh**

Abstract

Griswold v. Connecticut to Puttaswamy's case Judgment; from U.S. to India, everywhere the right to privacy has been the talk of the towns. In India, it has been considered to be an integral part of Article 21 of the Constitution. In various facets of life, the right plays a pivotal role. Whether it is the privacy of a woman, the privacy of a consumer, the privacy of a celebrity, everywhere the right comes into picture. What makes us ponder upon is the fact that despite the right being available, it has been seen to be grossly violated by the various sections of the society. The present article shall with the help of various case laws look into the instances of the violation of this Fundamental Right. Moreover, the article shall further try to analyse the laws in India and in the foreign territories with respect to Right to Privacy. Also, a deep study shall be delved into with the help of myriad examples as to how in various areas of day-to-day lives; the right to privacy is seen to be violated. The article shall focus its study to various aspects of online breaches that take place and the related subject matter.

Based upon the time constraint, the article shall be based upon non-empirical, descriptive and analytical research, wherein case laws, legislations, articles and various text books shall be referred for the study.

The finding of the article shall conclude if the steps being taken for the protection of right to privacy sufficient to prevent the violation or if something more and in addition is required to be done.

INTRODUCTION

Right to Privacy is one of the basic fundamental right to which every human being is entitled to. Privacy can have various forms and meanings. It can differ from person to person. And as we live in a dynamic society, the right to privacy can exist in various contexts. For example, one can talk about bodily privacy, where one has a right to choose, whether to give 'consent' or not; else it could amount to breach of privacy rights. Similarly, in the present technological era, the issues that turn up are related to social media and privacy rights. Moreover since most of the people are involved in online shopping and are using the online

* Assistant Professor, School of Law, Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan).

** Assistant Professor, School of Law, Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan).

platforms in their regular habits; that many of them, do not even know, how they share their personal information to various sources, like email ids., phone numbers, etc. In this generation of internet, anything one search on Google, the same thing or the advertisements related to them can be seen popping up on other social media platforms as well. This behavior clearly shows the data privacy breaches of the consumers by various online companies. In the contemporary world, the term 'privacy' is not just confined to a closed space but has its horizon expanded to cyber space as well. The present article aims to study the various forms in which the right to privacy is exercised by the individuals and also the different ways in which the violation of right takes place. The article shall be based upon Doctrinal Research and secondary resources are used to analyse the concept of privacy. Various articles available on the subject matter, books available, judgments related to privacy have been researched upon in order to know and comprehend the dynamics of privacy law. The research question upon which the further sections shall be dealing with are- what is the meaning of privacy and in what different ways the right can be exercised. Further, the article shall try to answer how the breach of privacy takes place? Whose rights are violated and who are the ones liable for violation? What is the effect of Puttaswamy judgment on society? What are the laws dealing with privacy violations and if they are enough? The article shall try to emphasize upon the EU General Data Protection Regulations (EU GDPR) and what is that which is missing in Indian Laws. Further, the description and analysis as to what is 'right to be forgotten' in internet age shall be discussed and various case laws shall be looked into, as to, in what circumstances, the right has been granted and in what, it is rejected. The findings of the article shall state what steps are required to be taken that the right of privacy of the citizens is not infringed.

I. Meaning and Historical significance of 'Right to Privacy'

The term privacy has not been defined anywhere in the Constitution nor has the right to privacy been explicitly mentioned in the Constitution. But, time and then, Supreme Court through various judgments has considered Right to Privacy as part of Article 21 of the Constitution. Privacy is a kind of expectation by a person that one is enjoying in one's area without the interference of any person until and unless consent is given to that person to intrude into the private place of the person. It can be related to privacy of one's own body or privacy of data. It was in *Kharak Singh v. UOI*¹, when the police conducted the visit at the appellant's home at odd hours, that the court held that right to privacy forms an intrinsic part of Article 21, i.e. protection of life and personal liberty. Justice Subba Rao in the case held that the right to privacy can be intruded but only with calculative analysis and not arbitrarily. In another case of *State v. Charulata Joshi*², the apex court held that the freedom of press as

¹ 1963 AIR 1295

² Criminal Miscellaneous (Main) Appeal No. 2675 of 1995; MANU/DE/0626/1996

enshrined under Article 19 (1) (a) of the Constitution is not an absolute right. Press has a freedom to express its views, opinions, take interviews of the people but if a person is not willing to be interviewed, then press can't force him, intruding upon his rights of privacy. In *R. Rajagopal case*³, Justice P.B. Jeevan Reddy stated that right to privacy includes the 'right to be left alone' under Article 21 of the Constitution.

It was also in *Griswold v. Connecticut*⁴, a case of U.S. where the Supreme Court in 7:2 decision, held the right to privacy to be an integral part of the person's basic rights. In this case, a law was passed by the government of Connecticut which criminalized the use of contraceptives. To this, the Supreme Court (SC) held that such law is in clear violation of the person's marital privacy⁵.

Then in 2003; in the case of *Lawrence v. Texas*⁶, it was held that the government cannot intrude into the private spaces of persons. In this case the government of Texas made it a crime for the people of same sex to engage in private and intimate acts. But the Court held the same law, as unconstitutional which is depriving a person of the right of privacy.

II. Various Facets of Violation of Privacy Rights

An individual's privacy is invaded in various ways. With the advent of technology and internet, the ways of intrusion have expanded beyond. People these days keep posting every minute detail on their facebook, instagram, whatsapp pages, twitter, etc. as to the places they visit, the activity they are engaged into, their moods and how they are feeling by posting various emoticons. It becomes very difficult to have the right to privacy being exercised when so much is shared voluntarily. When so much of the information is shared through the social media apps, it can sometimes become embarrassing as well in certain situations when certain personal family photos of the vacation are seen by colleagues in the office. People think it cool to share videos having parties and drinks with friends on social media apps⁷, and then, if the same video or photos of the activity somehow reaches their family, they complain of privacy breaches.

There are various dimensions attached to the concept of privacy which include- a.) privacy of the person; for example, submission for the biometrics, freedom from any kind of

³ *R. Rajagopal v. State of Tamil Nadu*, 1995 AIR 264; 1994 SCC (6) 632

⁴ 381 U.S. 479 (1965)

⁵ Alex Mc Bride, Expanding Civil Rights, Landmark Cases, THIRTEEN MEDIA WITH IMPACT, (Feb. 15, 2022, 7:20 PM), [https://www.thirteen.org/wnet/supremecourt/rights/landmark_griswold.html#:~:text=Connecticut%20\(1965\)-,In%20Griswold%20v.,the%20right%20to%20marital%20privacy.&text=Douglas%2C%20ruled%20that%20the%20law,be%20enforced%20against%20married%20people.](https://www.thirteen.org/wnet/supremecourt/rights/landmark_griswold.html#:~:text=Connecticut%20(1965)-,In%20Griswold%20v.,the%20right%20to%20marital%20privacy.&text=Douglas%2C%20ruled%20that%20the%20law,be%20enforced%20against%20married%20people.)

⁶ 539 US 558 (2003)

⁷ Theodore F. Claypoole, *Privacy and Social Media*, Business Law Today, AMERICAN BAR ASSOCIATION, January 2014.

torture, etc.; b.) privacy of the behavior of a person, which includes that a person can conduct himself in a private space in the manner he likes without any unreasonable surveillance. It has become very common to find hidden cameras in the changing rooms of various outlets, that is a gross violation of the bodily privacy and privacy of the way a person is conducting himself in a private space; c.) privacy of personal communications, this may include the mails, phone tapings that take place, etc.; d.) privacy of personal data, which is also called as informational privacy⁸. In the famous case of K.S. Puttaswamy⁹ (I), also informational privacy was considered to be an integral part of right to privacy. The data privacy breaches have become a common phenomenon as the information shared on a platform by a consumer or user is shared with other platforms or with third parties which the users are not even aware of, it is very easy that if a pair of shoes is searched on any online shopping app, one can find the mails, advertisements in other social media apps popping up etc.

Similarly, consumers also share their phone numbers and other details asked on online platforms. What becomes important is that these online platforms need to take the charge and responsibility for looking into the privacy concerns of the individuals. The online platforms record our activity and then tend to share the information to the third parties, thereby, intruding the privacy of the persons. Moreover, a study by National Academy of Sciences has shown that simply by identifying the 'likes' a person does on any social media app, the attitude of a person/ consumer can be known, to what products the person is more inclined towards, the political ideologies one believes in¹⁰. In any case that turns up before the court, it is not just the photos, or the posts by the person that can be considered as evidence, in Florida, it is also the mood which is expressed by means of emoticons carries importance¹¹. The Constitution of Florida has an explicit provision providing for the right to privacy if the intrusion takes place by the government authorities. What is missing is the action in case of intrusion by private persons.

A very important facet of right to privacy was brought forth in the case of *Selvi v. State of Karnataka*¹², wherein the SC discussed both the aspects of mental and physical privacy and it linked privacy right to Article 20 (3) of the Constitution¹³.

III. Media Trials and Right to Privacy

The infringement of privacy right has become common and prominent by the media

⁸ Roger Clarke, Privacy and Social Media: An Analytical Framework, 23(1) *Journal of Law, Information and Science* (2014).

⁹ Writ Petition (Civil) No. 494 of 2012

¹⁰ Kuvin Spencer & Silvia Chelsea, Social Media in the Sunshine: Discovery and Ethics of Social Media- Florida's Right To Privacy Should Change the Analysis, 25 ST. THOMAS LAW REVIEW (2013)

¹¹ Ibid.

¹² Criminal Appeal No. 1267 of 2004

¹³ INDIAN CONSTITUTION, art. 20 (3)

persons. Every now and then, the shameful act on the part of media is seen in the manner they intrude in the personal lives of public figures, giving and sharing unnecessary details about them not required to be known. Albeit, people have a Right to Information but not the kind of information the media is seen to be engaged into. Media though has a freedom of speech and expression under Article 19 (1) (a) of the Constitution but it does not have a right to infringe and intrude upon the right of privacy of other individuals.

The photos of celebrities, their children, their private lives are so much stated and published and that too without the consent of the celebrities, thus clearly violating their right of privacy. The photos of Sushant Singh Rajput lying still that got disseminated in the public on various media platforms is really condemning act on part of media persons. People going to the funeral of celebrities are also human beings who are saddened by the demise of the said person; taking photos and all the more trying to interview them during that period is a disgusting and inhuman act on the part of media persons.

Press, though considered to be the fourth pillar of democracy has played a pivotal role during emergency but the way it is expanding its roots in the name of competition, it is losing its importance and credibility. UDHR and International Covenant on Civil and Political Rights (ICCPR) provide for both the freedom of speech and expression as well as recognize the right to privacy. But Indian Constitution has only freedom of speech and expression explicitly recognized in it. In pre independence era, it was through the case of *Nihal Chand v. Bhagwan Dei*¹⁴ that the right to privacy was recognized through customs. But post-independence, it was in Kharak Singh's case that the right to privacy got recognition. In *Sharada v. Dharampal*¹⁵, the apex court has defined the term privacy as the private life of a person being free from any kind of intrusion. In *Hannover v. Germany*¹⁶, the media persons took the photograph of the daughter of Caroline without consent, and that was considered and held to be in violation of Article 8 of European Convention on Human rights. Similar was the case of *Murray v. Express Newspapers Plc*¹⁷.

In the earlier days, getting a camera was a big deal and things used to be published through newspapers but in the contemporary world, the photos reach through social media in milli seconds to the world at large, thereby infringing the privacy rights of the people. There have been many sting operations conducted by media, in the name of public interests; though some of them were of public importance but some were mere intrusions into the privacy rights of the individuals; thereby leading to defamation, an offence under Indian Penal Code.

¹⁴ (1935) A.I.R. S.C. 1002

¹⁵ (2004) L.J.R. 540

¹⁶ (2004) EMLR 379

¹⁷ (2008) WLR 1360

Recently, this happened in the case of Sushant Singh Rajput, wherein the media held its trial, despite the matter under investigation. Because of such media trials, verdicts are passed by the people and media; and a mere suspect in any case who might not be the actual offender is mentally harassed. It may sometimes lead to the consequences of persons committing suicides etc. The principle of criminal law is that one is to be considered innocent until proven guilty but unfortunately these media trials declare a person guilty before he is actually proved to have been committed an offence. The same happened in Jessica Lal Murder case¹⁸ and Arushi Murder case.

IV. Online Platforms and Right to Privacy

U.S. Supreme Court has laid emphasis on the concept of reasonable expectation of privacy¹⁹. In the internet era, the user itself disseminates the information, personal photographs, etc. on online platforms, but at the same time while using these platforms provided by various operators and companies, expects that his privacy rights would be respected. Westin, in case of America has identified the Republic of 1790-1820, as the 'modern' system for privacy. According to Westin though American Constitution did not explicitly provide for right to privacy but it had provisions that states, that no search and seizure shall take place unreasonably or a testimony if taken forcefully shall lead to rejection²⁰. In India too, the privacy right has slowly evolved as a concept and has now become an integral part of the Constitution. These social media platforms have led to the more crimes against children and women, thus intruding into their private lives and spaces. The offences like voyeurism is committed online by the voyeurs which is an offence under Section 354-C of Indian Penal Code²¹ (IPC) as well as Section 66-E of I.T. Act²². The person who is being watched by a voyeur has no connection with the voyeur or has no idea, that the activities done in a private space by him are being recorded by someone²³. The punishment for voyeurism was earlier dealt under Information Technology Act and later on it was incorporated through the Amendment in 2013 made to IPC. This particular provision of voyeurism which is incorporated in India has been influenced by U.S. Law dealing with the same, titled, 'Video Voyeurism Prevention Act, 2004'²⁴. If a person who in the reasonable expectation of privacy is doing any act which is captured without any consent and then

¹⁸ *Manu Sharma v. State of Delhi* (NCT) (2010) 6 SCC 1

¹⁹ *Katz v. United States*, 389 U.S. (1967)

²⁰ Henderson & Stephen E., Expectations of Privacy in Social Media, 31 *MISSISSIPPI COLLEGE LAW REVIEW* (2012).

²¹ *Indian Penal Code, 1860*, § 354-C, Act No. 45 of 1860 (India).

²² *Information Technology Act, 2000*, § 66-E, Act No. 21 of 2000, Acts of Parliament, 2000 (India).

²³ Md. Ali Imran & Aman Prakash Singh, A Sneak Peak in Women's Privacy, *MANUPATRA* (Jan. 5, 2022) (last visited on Feb. 18, 2022, 8:15 PM), <https://articles.manupatra.com/article-details/Voyeurism-A-Sneak-Peek-in-Womens-Privacy>.

²⁴ *Video Voyeurism Prevention Act, 2004*, § 1801, Public Law No: 108-495, 2004 (U.S.)

transmitted tends to violate the privacy rights of the person. In a recent Canadian case of *R. v. Jarvis*²⁵, the court has given its interpretation of the term 'reasonable expectation of privacy'. It explained with an example that if, for instance, if a woman is breastfeeding her child, then her expectation of not being viewed becomes unreasonable but the expectation that she would not be recorded for any sexual purpose is reasonable.

During this breach of privacy which takes place online, specifically, when the obscene or objectionable photographs are shared online by anonymous users, the same should be properly inquired into. The role of intermediaries plays a pivotal role in such circumstances. Intermediaries can include the search engines like Google, etc., interactive websites like Facebook, twitter. The definition of intermediary is also provided under I.T. Act²⁶, which states that any person who on behalf of another receives stores and then transmits the information further is termed as intermediary. The famous case of Avnish Bajaj²⁷ is related to the role of intermediary, wherein the Court held the intermediary liable for the sale of an obscene video clip posted on the website. Though the contentions of intermediaries are, that in the vast ocean of information which is posted by others on websites, it is very difficult to analyse, scrutinize and sort all the information posted on the website. In view of this argument by the intermediaries, rules have been brought forth in order to protect the intermediaries²⁸. Further Safe harbor protection was also brought for the intermediaries' protection through the amendment in the I.T. Act²⁹. The problem with the Intermediaries' Rules is that many terms which are used in the Rules are either ambiguous or such which have not been defined in any statute³⁰. The terms like, 'harm minors in any way', 'harassing', 'blasphemous', etc. are no where defined in the I.T. Act, 2000.

More recently, the Government has released the draft Information Technology (Intermediary Guidelines and Digital Media Ethics Code) 2021³¹, wherein it provides for the regulation of social media as well as OTT platforms along with digital news media³².

Thus, there are many lacunas that need to be rectified and the right to privacy which is being violated on such a large scale in the internet age need to be strictly regulated. Also,

²⁵ MANU/SCCN/0010/2019

²⁶ *Information Technology Act*, 2000, § 2 (w), No. 21 of 2000, Acts of Parliament, 2000 (India).

²⁷ Bail Appl. No. 2284 of 2004

²⁸ Information Technology (Intermediaries Guidelines) Rules, 2011

²⁹ *Information Technology Act*, 2000, § 79, No. 21 of 2000, Acts of Parliament, 2000 (India).

³⁰ Intermediaries users and the law- Analysing Intermediary Liability and the IT Rules, REPORT BY SOFTWARE FREEDOM LAW CENTRE, (Feb. 17, 2022, 6:15PM), <https://sflc.in/sites/default/files/wp-content/uploads/2012/07/eBook-IT-Rules.pdf>.

³¹ Information Technology (Intermediary Guidelines and Digital Media Ethics Code), 2021, (Feb. 14, 2022, 4:30 PM), https://www.meity.gov.in/writereaddata/files/Intermediary_Guidelines_and_Digital_Media_Ethics_Code_Rules-2021.pdf.

³² Mehab Quershish & Kazim Rizvi, The Evolution of Right to Privacy in India: A Look at Past, Present & Future, THE QUINT (Nov. 23, 2021), (Last visited on Feb. 14, 2022, 10:57PM), <https://www.thequint.com/tech-and-auto/the-evolution-of-right-to-privacy-a-look-at-the-past-present-and-the-future#read-more>.

Watsapp-Facebook has been in news for a long time, since its Privacy policy violated the right to privacy of individuals³³.

V. Pegasus: An intrusion into Privacy

Pegasus is a Greek word, which means a horse that is winged and is immortal. But in reference to privacy rights, this 'Pegasus' is a spyware that was developed by an Israeli technology firm, NSO. This spyware basically made politicians, heads of the State, journalists, etc. as its targets. If this spyware is actually true, then it is said to hack the phone numbers of various persons. The prominent feature of this spyware is that unlike other spywares, it does not require any kind of interaction with the targeted person; only a missed call or a simple message at the phone number of the targeted person is enough to extract all the possible information stored in the phone. Moreover, studies conducted have found that until and unless any forensic investigation is done, it is really difficult to detect the attack of a spyware in a device³⁴.

In the contemporary times, the spyware and ransomware attacks have become common phenomenon intruding the privacy of the users, thereby stealing the data.

VI. Right to be Forgotten

This has become an important issue when everything is put on social media and published. Some individuals demand that certain information which has become futile and if continued to remain posted, it can malign the reputation of a person; therefore, they demand that information to be removed from the websites. This right of getting the information which is of no use now, erased, is termed as right to be forgotten. Justice B.N. Srikrishna Committee's Report also recommended to include right to be forgotten as one of the principle to right to privacy. It states that as soon as the purpose for which the information was taken is over, the information needs to be removed or prevented to be displayed³⁵.

Google Spain case is a landmark case of European Courts in respect to right to be forgotten³⁶. This right is incorporated in Article 17 of EU GDPR, which gives the right to the data subject to have the data erased by the Controller without any unreasonable delay³⁷. Similarly Section 20 of the Indian Data Protection Bill is a provision incorporated regarding

³³ *Karmanya Singh Sareen v. Union of India*, MANU/SCOR/38389/2017

³⁴ Mansi Katyar & Akshita Singh, Pegasus- An Ominous Privacy Breach (Jan. 21, 2022), (last visited on Feb. 20, 2022, 7:07PM), <https://articles.manupatra.com/article-details/Pegasus-An-Ominous-Privacy-Breach>.

³⁵ *Aditya Verma, Right To Privacy, REPORT*, (Feb. 8, 2022, 8:15 P.M.), <https://cic.gov.in/sites/default/files/Right%20to%20Privacy%20and%20RTI%20by%20Aditya%20Verma%20%20%281%29%20%281%29.pdf>

³⁶ *Google Spain SL v. Agencia Espanola de Proteccion de Datos*, Case C-131/12, decided on May 13, 2014

³⁷ Article 17, EU General Data Protection Bill, 2018; Also see: Everything you need to know about the "Right To Be Forgotten" (Feb. 17, 2022, 6:40 PM), <https://gdpr.eu/right-to-be-forgotten/>

the same. In *V. v. High Court of Karnataka*³⁸, the right was recognized by the High Court of Karnataka. Moreover, Supreme Court in Puttaswamy judgment held right to be forgotten as part of right to life incorporated under Article 21 of Constitution³⁹.

Very recently, actor Ashutosh Kaushik, the winner of 2007 MTV Roadies show and Big Boss, is fighting for his right to be forgotten, for a mistake committed by him a decade ago. He was fined for drink and drive case and due to which his photos of the act became viral and which still can be found posted, of which he demands to be erased⁴⁰.

VII. EU GDPR v. Data Protection Bill of India

The EU General Data Protection Regulation (EU GDPR) is considered to be a comprehensive law concerning right to privacy related to protection of data. It came into force on 25th May, 2018. On the other hand, the Data Protection Bill of India is still waiting for it to be turned into an Act. Though many aspects of the Bill and EU GDPR are similar but they differ at various points. For example, in case of breach cases in EU GDPR law, the authority needs to be informed within 72 hours of the breach and accordingly the users can decide and take necessary steps regarding the protection of data. On the contrary, the time limit in India though remains same, but whether the users need to be informed or not regarding the breach shall be decided by the Data Protection Authority first and then the users can decide upon the steps for the data protection. Also, under GDPR, the punishment is fine upto 20 million Euros and if it is an undertaking then it may have to pay a fine upto 4 percent of the total turnover in the last fiscal year. But in case of breach in India, the person can be imprisoned upto 3 years or fine of Rs. 2 lakh can be charged⁴¹. The important thing to note is that the Bill does not apply to journalists, which means there is no restriction on the freedom of press⁴². Similarly, considering the importance and relevance of data in the present scenario, different countries have adopted and enacted privacy laws as per their requirements⁴³.

VIII. Conclusion and Suggestions

Right to Privacy has become an integral part in the life of individuals and now been

³⁸ 2017 SCC OnLine Kar 424

³⁹ Sanjay Vashishtha, The Evolution of Right To be Forgotten In India, SCC BLOG (Jan. 27, 2022), (last visited on Feb. 20, 2022, 8:50 PM), <https://www.sconline.com/blog/post/tag/right-to-be-forgotten/>

⁴⁰ Geeta Pandey, Ashutosh Kaushik: Indian Actor fighting for 'the right to be forgotten', BBC NEWS, (Feb. 17, 2022), (last visited on Feb. 20, 2022, 9:48 PM), <https://www.bbc.com/news/world-asia-india-60373229>

⁴¹ Aashish Aryan, Explained: How India's data protection Bill compares with EU regulation, THE INDIAN EXPRESS (Dec. 18, 2021), (last visited on Feb. 16, 2022, 11:40 PM), <https://indianexpress.com/article/explained/data-protection-india-versus-european-union-7678664/>

⁴² Kurt Wimmer, Comparison: Indian Data Protection Bill 2019 v. GDPR, (last visited on Feb. 20, 2022, 5:20 PM), https://iapp.org/media/pdf/resource_center/india_pdpb2019_vs_gdpr_iapp_chart.pdf

⁴³ U.K., Data Protection Act, 2018, (last visited Feb. 15, 2022, 4:20 PM), <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>

declared as Fundamental Right by the Courts as enshrined under Article 21 of the Indian Constitution. The Right is violated in various manners as discussed in the above sections but the question still remains that in the era of internet and technology, do the individuals really able to exercise the right to privacy? The Data Protection Bill which though was introduced in 2019 is yet to become a Law. And even if the same is implemented and brought into force, will the privacy right be cent percent ensured to the individuals. What is required is more number of experts in the field who can work on this and bring a possible solution.

The role of the organizations storing the information of large number of users need to be very strict and not indulge in any data sharing with third parties without the user knowing and consenting for the same. The information shared with one educational institute to take admission is shared with others at such a wide scale that people get numerous unnecessary calls and that too at any odd hours, this is a clear violation of privacy rights taking place and which needs a strong regulation and policy to curb such activities. Many people are not even aware of their right to privacy and those of them aware do not know if they will actually succeed in a privacy breach case or some even don't know how to proceed with things and who to apply in case of violation takes place. It therefore, becomes indispensable to make people aware of the importance and existence of privacy rights. There should be some principles and guidelines for the press and media as well so that they exercise their freedom in a regulated and controlled manner. The punishment for people involved in the case of breach of privacy should be very strict and offences need to be made cognizable and non-bailable; only then the situation can be taken in some control.

EDITORIAL POLICY

PROLOGUE

The Journal of the Faculty of Law aims at giving opportunities to all those who want to write on current and burning issues which carry socio-legal significances. It seeks to promote original and diverse legal scholarship in a global context. It is an annual peer-reviewed journal, **first published in 2009**, multi-disciplinary, aiming to communicate high quality original research work, reviews, short communications and case report that contribute significantly to further the knowledge related to the field of law. The Editorial Board of the Journal of The Faculty of Law (**ISSN: 2347-758X**) solicits submissions for its **Volume 11 issue in this year.**

SUBMISSION GUIDELINES

- Submissions must be made in Microsoft Office (doc./docx.) formats only.
- The submission must be the original work of the authors and should be free from all grammatical and spelling errors.
- The manuscript body must be in the font 'Times New Roman,' font-size 12, line spacing 1.5, and the text should be justified.
- All footnotes must be in Font 'Times New Roman', font size 10, line spacing 1.5, and justified.
- All submissions must follow the Bluebook (20th Edition).
- All the articles must carry an abstract of not more than 250 words.
- The article may be of 5000 words to 10,000 words.
- Since it's a peer reviewed Journal, the decision of the reviewers would be final.
- Article should contain a disclaimer to the effect that the submitted paper is original and is not been published or under consideration for publication elsewhere. The signed document must be e-mailed/posted to the The Editor along with manuscript.

Editor

Mailing address:

Prof. Satish C. Shastri

Chief Editor

Dean, School of Law

Mody University of Science and Technology

Lakshmangarh – 332311, Distt. Sikar (Rajasthan) India

Phone: +91-1573-225026, 09414047320

E-mail: dean.sol@modyuniversity.ac.in; satishshastri9@yahoo.co.in

U.G.C. Approved Journal No. 62469 (Till 2019)



MODY
UNIVERSITY

OF SCIENCE AND TECHNOLOGY

LAKSHMANGARH • RAJASTHAN

A Leading Women's University

Mody University of Science and Technology

Lakshmangarh - 332311, Distt. Sikar (Rajasthan) India

Phone: +91-1573-225026, 09414047320

E-mail: dean.sol@modyuniversity.ac.in,
satishshastri9@yahoo.co.in

