SOCIAL MEDIA AND RIGHT TO PRIVACY

Rakesh Kumar Choudhary*

Abstract

If we look back in time, we would have a million reasons to point out the fact that India, being the largest democratic country, was empowered with many fundamental rights for each individual after Independence, including the right to privacy, equality, etc. Having said that, it exists in every Indian individual because without rights, there won't be any duties to perform. The common question that is raised by every layman is, "When rights are violated in a broader sense, then what can be done to prevent that from happening?" This paper deals with the question of whether the right to privacy act can coincide with the ongoing capacities of knowledge organisations to get to and break down essentially everything about a person's life. A significant question is whether the right to protection as a common agreement specialty should be abandoned to strengthen safeguards against assumed psychological oppressor dangers. Furthermore, psychological oppression can be blamed for keeping tabs on the public.

Keywords: *Data Protection, Privacy, Freedom of Speech, IT Act, social media*

* President Oudh Bar Association (Former Additional Advocate General) @ Allahabad High Court, Lucknow Bench; Email: rakeshchaudharyadv@gmail.com; Contact: +91-9415001413

INTRODUCTION

Communication and information technology have reached another level in the past two decades. The world is transforming consistently due to technological advancements. This advancement in technology brings with it the development of social media and social networking sites. Social media has drastically changed the mindset of the people in such a manner that individuals, especially women and children, fall prey to unknown people through these social networking sites. Social networking sites offer privacy policies for every social media application; however, it is important to understand the privacy risks involved while using these applications. The InfoTech Revolution of the 20th Century has put the entire country on fast forward by introducing social media platforms where one can share information in fractions of seconds.[1] Social media platforms such as YouTube, Twitter, and Instagram have greatly impacted the political playing field and often play the role of a deciding factor in elections. The spread of information on social media has impacted political dynamics globally by enabling users to express themselves publicly through social media platforms.[2] The impact of social media is not only limited to politics but has become a part and parcel of people's professional and personal lives. For example, every small or big office in India now has a *WhatsApp* group, which is now mandatory and gives access to people's contact details to a few other people who they don't even know. There are violations of regulations and various laws due to these social media websites, commonly known as "cybercrimes." Regulation of such cybercrimes has not caught up to the speed with which technology has grown and become an inherent part

[1] Ajay Yadav, 'The Legal Complexities of The Digital World' (2012) 18 Lex Witness 1

[2] Wolfgang Danspeckgruber 'Introduction' in Princeton University' (eds.), 'Social Media Revolutions: All Hype or New Reality?' (Spring, 2011)

of the system. It is necessary for the country to legislate new and strict laws to deal with developing technology. The question of paramount importance arises here: Can one maintain his right to privacy while using social media?

RIGHT TO PRIVACY AND SOCIAL MEDIA

Privacy is a fundamental right recognised under Article 21 of the Indian Constitution and is also enshrined in various international instruments. The jurisprudence of privacy laws in India is still developing, but they have taken a sophisticated turn in countries like the UK and the USA. Human dignity was recognised very early on in India through various landmark cases, but it has only been very recently that the right to human dignity has been viewed as intertwined with the right to privacy. The protection of human dignity is critical for any society to function democratically. Jude Cooley explains the right to privacy as synonymous with "the right to be left alone."[3] The right to privacy has been recognised in the eyes of the law and in modern society due to advancements in technology in the global sphere. The collection, storage, and sharing of personal data have changed in unimagined ways with the innovation of technology, which results in breaches of privacy in many spheres of life. This puts an obligation on the state to enact laws for the protection of personal data.[4] Therefore, it can be seen that the right to privacy has always been a fundamental issue and has always been in controversy. In today's world, a person requires a safe private sphere, free from any intervention, be it state or private, to express his or her thoughts

[3] Cooley, Thomas M. "A Treatise on the Law of Torts", 1888, p.29 (2nd ed.)

[4] Human Rights Committee general comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Art. 17) para. 37

and ideas. Then only individual protection could be granted. It needs to go hand in hand with the right to freedom of information and transparency.[5]

REASONABLE RESTRICTION UNDER FREEDOM OF SPEECH

With the enormous workload of the judicial system, the judiciary also has enormous power to deal with it. It is safe to say that every individual's right to speak is protected under Article 19 of the Indian Constitution, but with that protection comes certain reasonable limitations, such as those against India's sovereignty and integrity, the security of the state, friendly relations with foreign states, public order, decency, or morality, or in relation to contempt of court, against defamation or incitement to an offense, which means that any individual is free to speak. The backbone of this article could be based on the landmark case of *Romesh Thappar* v. *State of Madras,*[6] which gives a definitive meaning to the interpretation of Article 19.

CONSTITUTION IN RESCUE OF FUNDAMENTAL RIGHT TO PRIVACY

In the case of *Kharak Singh* v. *State of Uttar Pradesh*[7] Supreme Court recognized for the first time that the citizens of India have the fundamental right to privacy which is a part of the right to liberty in Article 21 as well as right to freedom of speech and expression under Article 19 (1) (a), and of the right to movement under Article 19 (1) (d). However, in the Meneka

[5] *Poorvisha Jindal*, "Right to privacy in India: Its sanctity in India", Available at: Know the Right to privacy in India: Its sanctity in India (ipleaders.in)

[6] AIR 1950 SC 124

[7] (1964) 1 SCR 332

Gandhi[8] and RC Cooper case[9], the Supreme Court modified its approach and held that freedom and liberty is void without Right to Privacy. In today's world, a person requires a safe private sphere free from any intervention be it State or private, to express his/her thoughts and ideas. Then the protection of privacy would be given to one's right only. It needs to go hand in hand with the right to freedom of information and transparency.[10]

After the Judgement of *Justice K.S. Puttaswamy (Retd.) & Anr.* v. *Union of India & Ors.*[11], The right to privacy was given the status of a fundamental right; therefore, every citizen is provided with a right to be left alone and to safeguard its privacy in terms of marriage, education, childbearing, identity, family, motherhood, etc. On the other hand, we have Article 14, which provides freedom of speech and expression. In today's world of globalisation, advanced media, and cutthroat competition, it is becoming next to impossible to balance these two rights provided to citizens. Theoretically speaking, the freedom of the media cannot breach an individual's privacy, but practically there have been many instances where the media has not only breached the individual's privacy but has also acted like an image-building portal. The power that today's media contains and the role it plays are reflected in elections, court decisions, business forums, ad markets, and even the choices made by an individual. Social media in today's world is influential and resourceful; therefore, there is a need to channel the power. Today's problems must be adjudged by a vibrant application of constitutional doctrine and cannot be frozen by a vision

[8] Maneka Gandhi v. Union of India 1978 AIR 597

[9] (1970) 1 SCC 248

[10] Supra note 5

[11] (2017) 10 SCC 1

suited to a radically different society because the television media, newspapers, and technology, along with social media, have completely altered the lives of individuals, and it's no longer as it used to be in the generation when the constitution was drafted. It can be seen from the above paragraphs that the role of the media regarding public figures and matters that are already in the public domain is treated as an exception when it comes to the fundamental right to privacy. Though the media provides an excellent platform for discussing certain issues, there is a need to bridge a gap when privacy and public matters are intertwined. It cannot be overlooked that public figures, like all citizens, have the "right to be left alone," which is a fundamental right included under privacy. If a public figure is accused, the debates and acquisitions on social media draw conclusions before the decision of the court. The unbridled power of the media can become dangerous if check and balance are not inherent in it. The role of the media is to provide the readers and the public in general with information and views that are tested and found to be true and correct. This power should be painstakingly controlled and should accommodate an individual's major right to security.[12]

PRIVACY VIOLATION BY SOCIAL MEDIA

Have you at any point saw that anything you looked for and wished to purchase not many hours prior, their promotions begin jumping out on the web-based entertainment applications or while riding the net amazingly? What is your take, is that a fortuitous event each time? The solution to this question is not a solitary time, it is an occurrence. That is called Online Entertainment Promoting and Systems administration done by different

[12] *PJS* v. *News Group Newspapers Ltd*, (2016) U.K.S.C. 26

organizations to arrive at new clients by in a roundabout way attacking our protection.

To understand how right to privacy is violated while using social media, one must understand what social media is. Social media is nothing, but a form of communication based on the internet. Blogs, Social Media Applications, social Networking Sites, Widgets, YouTube, are some examples of Social Media Platforms. But in the past few years Facebook, Whatsapp, Instagram, Twitter have become voguish. Modern obsessions with privacy are rooted in the past century.[13] Dissemination of information on social media websites impacts user's personal privacy. Social networking sites like Facebook, Twitter, Whatsapp, Instagram have default privacy settings which enables other users to see a person's private information until the settings are actively changed. Merely failing to change their privacy settings, can make personal information of the user accessible to the public.[14] Technology aware users who change their default privacy settings also fall prey to this kind of violation as most of their personal information is available to their friends on social media.

The main purpose of social media platforms is to establish a relationship between the real and virtual world. The fault is ours to allow the entry of the virtual world in our real life because of which our privacy has been compromised. From IP address to online transactions, to mobile registration personal details, we make ourselves prone to the dangerous risk of cybercrime using the internet. All these sites instantly record personal

[13] Andrew T. Kenyon & Megan Richardson (eds.), 'New Dimensions in Privacy Law' (Reprint, Cambridge University Press 2007) 1

[14] Helen Anderson, 'A Privacy Wake-Up Call for Social Networking Sites?' (2009) 20 Entertainment Law Review 7, 245

details like in the case of Amazon.[15] This happens because more personal information leads to more potential advertisers. The giant advertising companies and websites with this personal information can track every step of the user on the internet when he is unaware and is choosing his preferential habits and lifestyles. One example could be how Facebook shows adds to a user's based on his internet surfing history. Have we given too much importance to this question as to how Facebook exactly knows what we were shopping from other websites? Probably this question would become problematic after many years in India when people will realize the importance of their privacy rights, but the UK Government recently imposed heavy penalty on Facebook for invasion of privacy of its citizens. A user's data is collected by these companies using an electronic trail which the user leaves behind every time a user logs into the internet. The information so collected is then used for marketing purposes targeting a particular individual. These pop-up messages will then appear in social media pages of the user. From this, it can be concluded that somewhere or the other, personal information of the user is being shared by these social networking sites just for the purpose of earning revenues.

Another problematic means adopted by social media applications and websites is permanent availability of user's information to others. For example, even if a person permanently deletes his Facebook account, the application does not delete complete information of the user. This is because of its data-use policy which clearly states that it typically takes about one month to delete an account. Thus, some information may remain for up to 90 days in logs or backup. Your friend may still have a message you

[15] Karnika Seth, "Computers, internet and new technology laws" 276 (1st Ed. 2012)

sent, even after you delete your account.[16] Moreover, pictures captured during video calls are automatically saved in Google's social media platform and the user remains unaware about it. The automatic saving and its permanent availability without the consent of the user is a gross violation of right to know and right to privacy. Even if you delete the Google account, the pictures will not be deleted as per the Google privacy policy. As a result, cases of identity thefts, sexual predators, unintentional fame, cyber stalking, Phishing, and defamation have started to increase.

Scams like KOOBFACE stealing personal information of FACEBOOK users, Version 5 HTML code providing personal details of the users to advertising companies, Twitter scanning phone contacts of their users and importing this information to their website database, are increasing daily and ironically, there is no remedy to all these scams as there is no law to curb the same.

INDIAN LEGISLATION ON SOCIAL MEDIA AND DATA PROTECTION

Keeping up with satisfactory network safety estimates in the present super advanced computerized climate is vital and the most ideal way to shield the IT foundation of the associations. Besides the fact that these dangers hurting are the organizations, yet in addition government specialists. Starting digital protection estimates by the public authority of India will help keep a digital secure climate and moderate the dangers related with the danger. The quantity of digital protection occurrences has expanded throughout the long term. Mr. P. P. Choudhary, clergyman of state for hardware and IT

[16] Facebook, 'Data Policy' (Facebook, 30 January 2015) <https://www.facebook.com/about/privacy/yourinfo>

expressed that 44679, 49455, 50362 network safety occurrences occurred in India during the years 2014, 2015 and 2016, as expressed by the data gathered by India's PC crisis reaction group (CERT-in). Albeit the public authority has taken certain network protection drives as talked about underneath, more forceful measures are expected to address the difficulty.

The current legal regime that regulates and protects privacy of citizens in India is under-developed and highly lacking to combat such sophisticated problems. Till now, we do not have any legislation dedicated to crimes on social media and data protection. In fact, cyber-bullying has also taken a concrete form, but the legislature is yet to mull on such issues. However, there are different laws which will be applicable in different situations broadly. The one and only statute which accounts for the media privacy issues to an extent is the Information Technology Act, 2000 (herein referred to as the IT Act, 2000) which is used in the present time to counter the challenges posed by information technology. The IT Act, 2000 does not capture the essence of privacy as a concept but only as a literal interpretation. It is self-explanatory as to how much this legislation can regulate given the fact that it was enacted nearly two decades ago, a point from which technology has exponentially grown multiple folds.

THE INFORMATION TECHNOLOGY ACT, 2000

- **Section 66 A of the IT Act, 2000** - Widely used for Offences in social media- Held unconstitutional by the Hon'ble Supreme Court in the case of *Shreya Singhal* v. *Union of India*.[17]

- **Section 66 C of the IT Act, 2000 -** Punishment for Identity Theft[18]

[17] (2015) 5 SCC 1

- **Section 66 E of the IT Act, 2000 -** One of the most important provisions - Punishment for violation of privacy without the consent of the user.[19]

- **Section 66 F of the IT Act, 2000 -** Punishment for cyber-Terrorism

- **Section 67 of the IT Act, 2000 -** Punishment for transmitting and publishing any obscene material.

- **Section 67 A of the IT Act, 2000 -** Punishment for transmitting material containing sexually explicit acts.

- **Section 69 of the IT Act, 2000 -** Power of Central or State Government to issue directions for interpretation of information in the interest of sovereignty or integrity of India.

- **Section 79 of the IT Act, 2000 -** Liability for intermediary. This section gives closest reference to social media. It states that the intermediary on which any data or information is hosted, like Facebook, Twitter, etc is not liable for any content given by the third party.

---

[18] "Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh."

[19] "Whoever, intentionally or knowingly captures, publishes, or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

"The intermediaries like Facebook, Twitter, Instagram, Google, etc have to remove any objectionable content hosted on their page when complaints to remove them have been received." - Shreya Singhal Case. These guidelines if implemented can protect privacy of individuals but in the practical world it is not possible. The issue which should be addressed is the usage of data and how these intermediaries get access to it.

THE IT (PROCEDURE AND SAFEGUARDS OF INTERCEPTION, MONITORING AND DECRYPTION OF INFORMATION) RULES, 2009

The Central Government in exercise of its power under section 87 (2) (y) of the IT Act, 2000 framed these rules to lay down procedure and to safeguard, monitor and collect data or information. Relevant rules in this regard are as follows:

- **Rule 4 -** An agency of the Government will carry out the functions of monitoring, safeguarding, and collecting data.
- **Rule 13 -** Intermediary will provide facilities and will cooperate for monitoring or decryption of information.

THE IT (PROCEDURE AND SAFEGUARDS FOR BLOCKING FOR ACCESS OF INFORMATION BY PUBLIC) RULES, 2009

The Central Government in exercise of its power under section 87 (2) (z) of the IT Act, 2000 framed these rules to lay down procedure and to safeguard for blocking of access by the public. Relevant rules are as follows:

- **Rules 3 to 8 -** Method for requesting the Nodal Officer to block the concerned organization. Approval necessary from the IT

Department of the central government after which the blocking will be done by the Nodal Officer.

- **Rule 9 -** Power to the Nodal Officer to decide regarding blocking
- **Rule 10 -** The Court can direct the Nodal Officer regarding blocking of any information and the information be given to the IT Department.
- **Rule 13 -** Every intermediary shall appoint a person to handle directions for blocking of information.

THE INFORMATION TECHNOLOGY (INTERMEDIARIES GUIDELINES) RULES, 2011

Enacted under section 79 of the IT Act, 2000. The intermediaries to claim exemption from liability must follow some rules regarding blocking of certain content.

- **Rule 3 -** Intermediaries should inform the users not to display, upload any information which is objectionable.
- **Rule 3 (4) -** Intermediary shall remove the objectionable content within 36 hours.

THE INDIAN PENAL CODE, 1860

- **Section 153 A -** Punishment for class hatred
- **Section 292 -** Offence of Obscenity

- **Section 295 A -** Punishment for insult to religion and to religious beliefs.

- **Section 499 -** Offence of Defamation

- **Section 505 -** Offence to incite any community against another.

THE CRIMINAL PROCEDURE CODE, 1973

- **Section 166 A -** Letter of request for investigation at any place in or outside India

- **Section 4 -** Trial of offences under any law

- **Section 188 -** Regarding offences committed outside India

THE PERSONAL DATA PROTECTION BILL

Following the debates in the year 2019, the personal data protection bill was tabled in the Lok Sabha in December 2019. Relevant provisions are as follows:

- **Section 26 -** It defines "Social Media intermediary" - Service that facilitates transaction between two users to convey information.

- **Section 28 (3) -** Users to get account verification mechanisms by the intermediaries.

- Data Protection Authority (DPA) to be set up to resolve issues relating to intermediaries.

- **Section 35 -** Central Government has powers to exempt any agency from its obligations relating to processing of personal data of users.

RECENT CASES AND EXAMPLES

Hacking in today's world has become common. A user knows that his account is being hacked, but he cannot do anything about it because he has shared relevant information. Nowadays, hackers look for people who visit harmful sites. Hackers use short URLs, and they inject viruses into the computers of those who open these URLs. They also tend to use apps, with the help of which they can see the screen of the user's phone on their phone. These kinds of spyware give the hacker information about the user's passwords and credentials for the accounts from which you do online transactions.

Shreya Singhal Case [20]

In the case of Shreya Singhal v. Union of India, the Supreme Court of India established important guidelines for intermediaries to follow. According to these guidelines, Facebook, Twitter, Google, Instagram, and YouTube have an obligation to remove any objectionable content displayed on their respective platforms after they receive complaints to do so. These guidelines were set to protect the privacy of individuals, but there is no proper implementation of them. In this regard, the real issue must be addressed, i.e., the usage of data by these intermediaries and how they gain access to it.

Brief Facts- Two young ladies, Shaheen Dhada and Rinu Srinivasan, were captured by the Mumbai police in 2012 for communicating their dismay at a bandh following Shiv Sena boss Bal Thackery's passing. The ladies posted their remarks on Facebook. The captured ladies were later delivered, and it was decided to strip the crook bodies of evidence against them, but the

[20] Supra note 17

captures sparked widespread public outrage. It was felt that the police have abused their power by summoning Segment 66A, inter alia, and that this disregards the right to speak freely and articulate.

Whatsapp - Facebook Privacy Case[21]

The actions of one private party to enter a contract with another private party was constitutionally challenged before the court. According to the latest privacy update, WhatsApp's analytics and data will be sent to Facebook. The data includes important credentials and details of the WhatsApp account holder. The catch here is that the user is unaware that his data will be sent to some other social media platform as the users are not informed about EULA.[22] This is a gross violation of the user's right to privacy because the WhatsApp update is deceptive.

As this case needed serious constitutional interpretation, it was referred to a constitutional bench. The bench observed: "There are 3 zones of privacy". They are:

- Intimate Zone - Sexuality, Physical privacy, etc.
- Private Zone - PAN Card Number, ATM Number, etc.
- Public Zone - Big Data Analytics, etc.

The Hon'ble Supreme Court ruled that the first two zones are out of the bounds of Facebook and Whatsapp, while the public zone requires deliberations on a case-to-case basis.

[21] *Karmanya Singh Sareen* v. *Union of India*, (2017) 10 SCC 638
[22] WhatsApp's End User License Agreement

Bois Locker Room Case

Few guys of XI-XII standard in Delhi allegedly made certain remarks in a group named 'Bois Locker Room'.[23] These sexually colored remarks were made on underaged girls and objectified them too. Some even went to an extent of discussion of raping them. The offences relevant to this scenario are:

- Section 292 of IPC, 1860 - Offence of Obscenity
- Section 66 of IT Act, 2000 - transmitting gross offensive information
- Section 503 of IPC, 1860 - Criminal Intimidation
- Section 509 of IPC, 1860 - Raging Modesty of a woman
- Section 499 of IPC, 1860 - Defamation
- Section 354 D of IPC, 1860 - Stalking
- Provisions of POCSO Act
- Section 79 of IT Act, 2000 - Liability of Intermediary

Eventually the Cyber Cell Delhi arrested those juveniles, and it turned out that one of the juveniles was the fake ID made by a girl who started the conversation by sending a picture of hers.

[23] Sparsh Sharma, "Bois Locker Room Controversy And The Law Related To The Liability For Sharing Obscene Material In A Group Chat" http://www.legalserviceindia.com/legal/article-2286-bois-locker-room-controversy-and-the-law-related-to-the-liability-for-sharing-obscene-material-in-a-group-chat.html

Twitter case

Twitter itself has admitted that they have scanned contacts of its users and have imported them to their database to know more about their users.

CONCLUSION

It's high time we make ourselves prepared for the tech boom which will hit us in the coming years. Stringent Laws shall be made in the wake of increasing technology and invasion of privacy at the same time. Theory of Protection of Privacy shall be applied in the real world and shall be given practical use. The developers of the application should change their approach from data centric to consumer trust centric. The users should be given an option whether to share their information or not. The principle of data minimization should be adopted. Information Technology Act, 2000 should be redrafted along with its rules and regulations so that it can be applied in today's world in the 21st century.