RIGHT TO PRIVACY IN THE DIGITAL AREA

Ms. Chhavi Chauhan[*]

Abstract

In an era where, there are wide, varied, social and cultural norms and more so in a country like ours which prides itself on its diversity, privacy is one of the most important rights to be protected both against State and non-State actors and be recognized as a fundamental right. Right to privacy is a fundamental basic human right under the article 21 of the constitution of India. The right to privacy was declared a fundamental right by the Supreme Court in K.S. Puttaswamy v. *Union of India case, 2017. According to Black's Law dictionary privacy means '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 concerned. It is also recognized as a basic human right under Article 12 of the Universal Declaration of Human Rights Act, 1948.*

[*] Student: B.A.LL.B.(H) @ Amity Law School, Gurugram

INTRODUCTION

Means of communication which is known as 'media', it can be communicated through television, radio, newspapers and the internet, that influence people and make them informative with the happenings of the world. In the world of today, media has become as important as food and clothing. It has played a vital role in strengthening our society. Media is considered as 'mirror' of the society, it shapes our lives. As we are moving towards the modernization of the world, we all are inclining towards the digital way of doing things. Nowadays, everything is online and in the digital format, so now the whole media industry is also in the digital format, which makes it more accessible and connecting more number of people.

ROLE OF MEDIA IN DEMOCRACY

For a healthy democracy, access to information is very important for two reasons. First, it make sure that citizens make responsible, logical and well informed choices and do not act wrong due of misinformation. Secondly, information plays as a "checking function" that make sure that representative which are elected by the people stood up to their oaths of office and carry out the good work for the people. In some societies, an antipathetic relationship between government and media plays a vital and healthy environment of fully functioning democracies. For some people it might create a conflict, and tension-ridden relationship may not be good, but the role of the press to provide the right information is a way of mediating between the state and all civil society remains very important.

In the context of supporting democratic changes, If the media is to have any meaningful role in democracy, then the ultimate goal of media should be to develop a wide range of diverse mediums that are credible, and to create and strengthening the sector that promotes such outlets. Trustable outlets provide citizens to have access to right information that they need to make sensible decisions and to participate in society. Media should be supportive of democracy that has a independency of publishing editorial, is financially capable, has diverse voices, and serves for the public interest. The public interest is defined as representing different types of voices through greater number of channels and through the diversity of views reflected within a single channel.

DIGITAL MEDIA AND DEMOCRACY

Digital media become an integral part of citizens political lives as number of people around the world uses the technology of digital media for information and communication. Digital media

comprises an important platform that people can use to coordinate and connect among like-minded people. Furthermore, the distributing of informative messages, digital media also facilitate socio- political factors that raise concern over the circulation of misinformation, information that divides the people and political separation.

Recent studies on political activism have highlighted that the role of digital media in shaping different forms of political participation and to conduct large-scale social protests around the world. Digital media platform such as Facebook and Twitter provide a platform for affective and behavioral connections that enable people to collectively network among themselves. For instance, digital media provide people with news and mobilizing information and allow them to exchange their opinions with many others, motivating them to engage in public activities. Digital media content can be quickly updated anytime anywhere without wasting of time, money and physical effort, which helps digital media users to be updated for all the activities which is happening around the world.

Freedom is the platform from which digital democracy can evolve. In the history it is the first time that, we have a platform that can questions easily to the governments, make them accountable and bring the required change that people want for which they have voted. For people to rule among themselves, they need to have right and clear information. They also need to communicate to others. Social media platforms make that so much easier. There is a valid point as well. When democracies are functioning in a proper way, then people's challenges and sufferings are not entirely private issues. Social media platforms help us to inform to one another for different problems. In this process, the existence of social media can provide solutions for the required citizens. Whenever we talk about digital or online platform, it raises a lot of concerns. It might have a lot of positive points but one of the major disadvantages will be the concern for privacy, as in the online platform it's difficult to understand whether our data is being compromised or not.

Privacy

We should discuss about right to privacy, it is important to know what is privacy? And why it matters?

According to privacyinternational.org, Privacy is a fundamental right, essential for freedom and the protection of human dignity; serving as the foundation upon which many other human rights are built. Privacy enables us to create boundaries and manage them to protect ourselves from

unwanted interference in our lives, which allows us to negotiate who we are and how we want to interact with the world around us. Privacy helps us to establish boundaries to limit who has access to our identity, places and things, as well as our communications and our information. The privacy protection rules give us the ability to maintain our rights in the face of significant power imbalances.

As a result, privacy is an indispensable way we seek to protect ourselves and our society against arbitrary and unjustified use of power[1], by reducing what can be known about us and can be done to us, while protecting us from others who might wish to control. As a human beings Privacy is essential to whom we are, and we make decisions about it every single day. It gives us a space to be ourselves without judgement, allows us to think freely without any discrimination, and is an important tool by giving us control over who knows what about us.

Why does it matter?

In today's society, the negativity around privacy is a debate about modern freedoms. As we consider how we establish and protect the boundaries around the people, and the ability of the individual to have a say in what happens to him or her, we are equally trying to decide:

- the morals of modern life;
- the rules governing the conduct of commerce; and,
- the restraints we place upon the power of the state.

Technology has always been twisted with this right. For an illustration, our capabilities to protect privacy are greater in today's world than ever before, yet the capabilities that now exist for surveillance are without authentic permission.

It is now possible for companies and governments to monitor every conversation we conduct, each commercial transaction we undertake, and every location we visit. These capabilities may lead to negative effects on individuals, groups and even society as it initiates discriminations and violence among the people. They also affect how we think about the relationships between the individual, markets, society, and the state. If the situation arises where able to peer into our histories, observe all our actions, and predict our future actions, even greater power imbalances will emerge where individual autonomy in the face of companies, groups, and governments will effectively disappear and any deemed aberrant behavior identified, excluded, and even quashed.

[1] Available at: https://privacyinternational.org/explainer/56/what-privacy

Perhaps the most crucial challenge to privacy is that the right can be compromised without the individual being aware. Moreover, we aren't being informed about the surveillance we are placed under, and do not have the capabilities to raise question about these activities. Now, it's time to take the matter of privacy more seriously and to fill the loopholes as much as possible. We have to concerned about our privacy it's not just about our dignity but it's our right too. Right to privacy is now our fundamental right.

RIGHT TO PRIVACY

On 24 August 2017, the Supreme Court of India in a historic judgement declared the right to privacy as a fundamental right protected under the Indian Constitution. In declaring that this right stems from the fundamental right to life and liberty, the Court's decision has far-reaching consequences.

A nine-judge bench of the Supreme Court in the case of K.S. Puttaswamy vs. Union of India [2]2has declared that the right to privacy is a fundamental right protected under Part III of the Constitution of India. While primarily focused on the individual's right against the State for violations of their privacy, this landmark judgement will have repercussions across both State and non-State actors and will likely result in the enactment of a comprehensive law on privacy. The Supreme Court confirmed that the right to privacy is a fundamental right that does not need to be separately articulated but can be derived from Articles 14, 19 and 21 of the Constitution of India. It is a natural right that subsists as an integral part to the right to life and liberty.

As we can see that right to privacy is defined in our constitution and in the upcoming future many judgements will be made on the basis of this landmark judgement which will make a major change. We as the people of this country should make sure our privacy is being protected and if in any way our right is infringed then we should take the needful action, and by implementing this our society will get more aware of their rights.

IMPACT OF DIGITALIZATION ON PRIVACY AND FUNDAMENTAL RIGHTS

We are in a period of profound societal change and dislocation, almost a consequential shift, brought on by the rapid amplification of digital communication infrastructure and exponential enactment of digital technology. Digital technology has entered into the means through which human rights are violated around the globe.

[2] K.S. Puttaswamy v. Union of India (2007) 10 SCC 1

Several questions are raised that- to whom does all these data or information belongs to? Who will be able to approach it? What, if any, are the conditions on the use of this information? The law pays for catch-up as it does in all thing's technology. Jurists around the globe combat to combine traditional law ideas and the absurdly protruding moments in which we find ourselves. Several governments demanding and seeking access to information from their people and corporations complicate this stance further. On the other side, what are the privacy limitations? Can information be requested for fundamental services, travel or even advantages from the government? Is national security overriding all privacy issues? Article 21 of the Indian Constitution offers that "No person shall be deprived of his life or personal liberty except according to procedure established by law". The Supreme Court ruled on 24 August 2017 that the right to privacy is a fundamental right guaranteed by Part III of the Indian Constitution. This decision on the legislation and regulations will have very severe consequences. New regulations will be implemented on the same parameters on which the laws that violate personal freedom are tested in accordance with Article 21 of the Indian Constitution. The right to privacy is now unambiguously accessible–its contours and boundaries are the issue that remains exceptional. India has no extensive data protection and privacy legislation. As of now, in addition to other sectoral legislation, the appropriate regulations of the Information Technology Act, 2000 and its regulations govern the collection, processing and use of' private information' and' delicate private data or information by a corporate body in India.

The Supreme Court first esteemed whether the 'right to privacy' is a basic right in the case of M. P. Sharma and Ors. v. Satish Chandra[3], District Magistrate, Delhi and Ors where the warrant granted for search and seizure was questioned pursuant to Sections 94 and 96(1) of the Criminal Code of Procedure. The Supreme Court ruled that the search and seizure authority was not contrary to any constitutional provision. The Court also refused to recognize the right to privacy as a basic right guaranteed by India's Constitution.

Thereafter, in the case of Kharak Singh v State of Uttar Pradesh and Ors.[4], the Court regarded whether it would be an abuse of the right guaranteed under Article 21 of the Constitution of India to monitor an accused's home visits at night, thus raising the question of whether Article 21 included the right to privacy. The Supreme Court ruled that, in reality, such monitoring was contrary to Article 21. Moreover, the majority judges held that Article 21 did not expressly

[3] M. P. Sharma and Ors. v. Satish Chandra (1954) 1 SCR 1077
[4] Kharak Singh v. State of Uttar Pradesh and Ors. 1963 AIR 1295

provide for a provision of privacy, and therefore the right to privacy could not be interpreted as a fundamental right.

After a while, in the case of Gobind v. State of M.P.[5] Police's right to housekeeping was questioned to be incompatible with the right to privacy enshrined in Article 21 of the Indian Constitution. The Supreme Court ruled that the laws of the police did not comply with the principle of private liberty and also acknowledged the right to privacy as a basic right guaranteed by the Indian Constitution, but supported the development of the right to privacy on a case-by-case basis and denied it as an absolute right.

This issue was once again raised before the Supreme Court in the case of K. S. Puttaswamy (Retd.) v. Union of India, in that case, the Aadhaar Card Scheme was questioned on the ground that the collection and compilation of population and biometric information of citizens of the nation to be used for different reasons infringed the basic right to privacy enshrined in Article 21 of the Indian Constitution. Given the ambiguity surrounding the constitutional status of the right to privacy from previous judicial precedents, the Court referred the matter to a constitutional panel composed of nine (nine) judges.

The Supreme Court ruled that the right to privacy is inherent to the human element and the core of human dignity and is inseparable from it. Accordingly, privacy was kept to have both beneficial and negative content. The adverse content functions as an embargo on the State by intruding into a citizen's life and private freedom, and its beneficial content imposes a duty on the State to take all needed steps to safeguard the individual's privacy.

Therefore, the constitutional protection of privacy may give rise to two inter-related protection:

- Against the world at large, to be respected by all including the State: the right to choose what personal information is to be released into the public space, and
- Against the State: as necessary concomitant of democratic values, limited government and limitation on power of State.

As a consequence of this judgement, the right to privacy has become more than just common law and more solid and sacrosanct than any statutory right. Thus, an invasion of privacy must now be justified in the context of Article 21 of the Constitution on the grounds of a law stipulating a fair, just and sensible procedure.

[5] Gobind v. State of M.P. (1975) 2 SCC 148

CURRENT ISSUES

The Supreme Court set a threefold necessity to interfere with fundamental rights by the state. While the State may intervene to safeguard the lawful interests of the State:

- There must be a law in place to justify an infringement of privacy which is an express requirement of Article 21 of the Constitution;
- The nature and content of the law imposing the limitation must fall within the reasonableness area prescribed by Article 14; and
- The means taken by the legislatures.

Therefore, any regulations aimed at infringing an individual's right to privacy would have to satisfy the proportionality and reasonableness criterion. It will take a couple of years for jurisprudence to settle momentarily what constitutes sensible and proportionate state interference.

In contrast to today's consent-based model, it is often asserted that India should embrace rights-based information privacy models. The information controller is free to process, use and share the information with any third party under the consent-based model once the user's consent has been acquired. In the above judgments, the Supreme Court's judgment empowers Indian citizens to seek judicial relief in the event of infringement of their data privacy rights. This could have an effect on India's tech companies' privacy and security policies. Not only can consumers increase allegations based on torture, they can also invoke their fundamental right to privacy.

CONCERNS AND DIFFICULTIES

Nature of data protected by the Indian legislature: Since India lacks an extensive data protection mechanism, the primary act dealing with data protection is the IT Act and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011. Under the IT Act and the IT Rules, what is primarily intended to be protected are personal data and sensitive personal data or information, i.e. password-related information, financial information such as bank account or credit card or debit card or other payment tool details, physical, physiological and mental health condition, sexual orientation, medical records and history.

The information freely available in the public domain, however, is not considered within the scope of sensitive personal data or information. In addition, the regulations deal only with a corporate body collecting and disseminating data.

Who can collect the personal data?

Rules 5 of the IT Rules stipulate that no corporate body or individual on its behalf shall gather delicate private data or information unless:

- The information is obtained for a legitimate purpose related to the function or activity of the corporate body and
- It is deemed appropriate to obtain such information for that purpose.

In addition, the person sharing the information must be made aware of the fact that the information is being collected, the purpose for which the information is being collected, the intended recipients of the information, the name and address of the agency collecting the information and the agency retaining the information.

Duration of storing the personal data: Any company or persons holding sensitive personal data or information on their behalf cannot maintain it for longer than is necessary for the reasons for which the information may be legally used or is otherwise needed for the time being under any law and such information may only be used for the purpose for which it is gathered. Further the body corporate or any person on its behalf collecting the information, prior to the collecting of information, is required to provide an option to the provider of the information to not to provide the data or information sought to be collected. The data supplier has the choice to withdraw its permission provided previously, whenever the services are available or otherwise.

Extend to which personal data can be shared with third parties: The corporate body receiving the information may disclose sensitive personal data or information to any third party, provided that prior authorization has been received from the provider of such information, or such disclosure has been agreed in the contract between the recipient and the information provider, or where disclosure is necessary to comply with a legal obligation.

However, no such approval from the information supplier is needed if the information is shared with government organizations mandated by legislation to acquire information including sensitive private data or information for identity verification purposes, or to prevent, detect, investigate, including cyber occurrences, prosecute, and punish offenses.

Furthermore, in accordance with Rule 4 of the IT Rules, the employer, being a corporate body that gathers, receives, possesses, shops, and employee data, is needed to have a privacy policy in place to handle or distribute such private data. The employer is also required to provide employees with the privacy policy for review and publish the same on their website.

E-GOVERNANCE AND CYBER SECURITY: A NEW PANDORA'S BOX

Electronic governance or e-governance is adopted by countries across the world. In a fast-growing and demanding economy like India, e-governance has become essential. The rapid growth of digitalization has led to many governments across the globe to introduce and incorporate technology into governmental processes. Electronic governance or e-governance can be defined as the usage of Information and Communication Technology (ICT) by the government to provide and facilitate government services, exchange of information, communication transactions and integration of various standalone systems and services.

In other words, it is the use of technology to perform government activities and achieve the objectives of governance. Through e-governance, government services are made available to citizens and businesses in a convenient, efficient and transparent manner. Examples of e-governance include Digital India initiative, National Portal of India, Prime Minister of India portal, Aadhaar, filing and payment of taxes online, digital land management systems, Common Entrance Test etc.

The objectives of e-governance can be listed down as given below:

- To support and simplify governance for government, citizens, and businesses,
- To make government administration more transparent and accountable while addressing the society's needs and expectations through efficient public services and effective interaction between the people, businesses, and government,
- To reduce corruption in the government,
- To ensure speedy administration of services and information,
- To reduce difficulties for business, provide immediate information and enable digital communication by e-business.

While e-governance provides the advantages of convenience, efficiency, and transparency, it also has problems associated with it. They are as follows:

- Lack of computer literacy: India is still a developing country and a vast majority of the citizens lack computer literacy which hinders the effectiveness of e-governance,
- Lack of accessibility to the internet or even computers in some parts of the country is a disadvantage to e-governance[6],
- E-Governance results in a loss of human interaction. As the system becomes more mechanized, lesser interaction takes place among people,
- It gives rise to the risk of personal data theft and leakage,
- E-Governance leads to a lax administration. The service provider can easily provide excuses for not providing the service on technical grounds such as "server is down" or "internet is not working", etc.

Cyber-attacks are very much threat for the e-governance, several countries have begun exploring options for strengthening their offensive capabilities in cyberspace, and many have already done so. This is a dangerous escalation. Almost all societies have become heavily dependent on the internet, the world's most important piece of infrastructure and also the infrastructure upon which all other infrastructure relies. It will be not so late when there will be "Internet of Everything" and our current era is not a Fourth Industrial Revolution, but it is the beginning of the digital age.

Cyber-attacks in India jeopardize national security by accessing sensitive Government infrastructure. Cyber-crime against government is a major threat to citizen, government properties, government -plans and society. Some cybercrime risk factors on e-governance are spoofing, reproduction, disclosure of e-governance information, denial of service and elevation of privilege.

India is in the final stages to clear a National Cybersecurity Strategy in the wake of growing Cyber-attacks and threats from nation-state actors against the country, national cyber security coordinator Lt. Gen. (Retd.) Rajesh Pant has stressed. There are about 4 million malware that are detected every day and India is one of the most cyber attacked nations in the world.

[66] Available at: https://cleartax.in/s/e-governance

One of the reasons for that is that we have a large attack surface with 1.15 billion phones and more than 700 million Internet users, Pant said during the third edition of 'Expert Speak', a curated dialogue series by Microsoft with industry experts.

What we require now is a National Cybersecurity Strategy6, which we have been working on over the last two years and is in the cabinet for the final stamp. The first thing we need is the cybersecurity of the nation, Pant stressed.

That is the first thing we have to tackle, because the difference between a policy and a strategy is that a strategy is an action-oriented plan with a timeline. The pandemic has taught countries that cybercrime is now an essential service, just like the police and fire departments.

NEW MEDIA REGULATION IN DIGITAL AGE

Rapid and extensive development of digital technology has led to the rethinking of the media concept. Even before digital technology, the impact of technology on the media was substantial. All media were once new, and the academic and professional public discussed about the possible impact the new technologies would have on media sphere. Changes caused by the new technology have also brought about changes in society: electronic media have increased mass audiences and led to an increase in media power which influence people in a better way.

The new media that are emerging thanks to digital technology are making a dramatic change: all content can be represented in the same digital code, on the same device. Traditional media are changing with the emergence of new media formats and they can present their content on digital platforms). There is an active audience that posts blogs, tweets, records videos, and reports on disasters. Participatory journalism 7is born, where ordinary citizens act as journalists from the standpoint of witnesses of certain events, while professional journalists and professional media count on them in these situations. A new genre called live blog has been created, in which journalists and amateurs cover an ongoing event. Social media, Twitter above all, are becoming significant journalistic sources. For getting current happenings of the world, we don't have to wait for the newspaper every morning; everything is just a click away from our electronic devices.

The new media regulation in this digital age comes up with its own set of issues. One of the key reasons that these issues are so difficult to untangle is that social media is fundamentally different from traditional media (that is, newspapers, radio, and broadcast

networks)[7] — and so traditional approaches to regulation have largely fallen short. There are a few key dimensions worth considering,

First, traditional cable news (and to a lesser extent, other traditional news media) are defined by limited bandwidth. There are a limited number of news media networks, and a limited number of primetime windows and headline slots with which to influence as large an audience as possible. In contrast, social media platforms offer essentially infinite bandwidth, with millions of accounts that can each target much narrower audiences.

Second, traditional news content is produced with editorial oversight: A set of producers with executives above them determine the personalities and viewpoints to be broadcasted across their networks or given envied publication space. This means that it's easier for companies to supervise the content that is shared on their platforms, and it's also easier for third parties to hold companies accountable.

Finally, in general, viewers and readers of traditional news media must proactively choose the content they consume — whether that's a show they choose to watch or a column they choose to subscribe to. Social media users, on the other hand, have almost no control over the content they see. Instead, platforms use complex algorithms to serve content they think will keep users scrolling, often exposing them to more radical posts that they may never have sought out on their own. Also, the information that people are rely on are not thoroughly investigated and sometimes the source is unknown.

People have to be very choosy when it comes to reading of news, yes, it's true that due to the new digital age the media is almost accessible to all but people have to make sure that whatever we are reading it should be from a reliable source and in which people can trust. The media and the news companies are sharing irrelevant content to their viewers for getting more ratings and becoming more profitable.

This new scenario for public communication in the digital era should not be understood in a catastrophic way, but it should be looked as the opportunity to redefine the role of media for the people, the professional challenges, and to make it more authentic and impactful in our lives.

CONCLUSION

[7] Available at: https://hbr.org/2021/01/are-we-entering-a-new-era-of-social-media-regulation

From above, it is obvious that the need for the hour is an extensive legislature governing the collection and dissemination of private information. There are no extensive laws governing the handling of private data that are not private data or information that is per se sensitive. Personal information protection is inextricably related to privacy, i.e. every person's right to enjoy his life and freedom without arbitrary interference with his private life, family, home or correspondence, etc. In contrast to the public, the term private must be grasped. Therefore, in the current obtrusive era of information technology, the right to be let alone and its security is highly essential. Since there is no single law that governs data protection in India comprehensively, it is necessary to derive the legal clauses regulating the same from multiple legislative acts.