Vol. 2, Issue 2, April - June 2017
ISSN: 2456 - 608X
International Journal of Legal Research and Studies
UGC Approved Online Journal (Sr. No. 1224 & Journal No. 48489)

RIGHT TO PRIVACY IN DIGITAL ERA: A CONSTITUTIONAL PERSPECTIVE

Rekha Kumari
Research Scholar, Department of Law, BPSMV, Sonepat, Haryana, 131305
neely1234@gmail.com

***Abstract*- -Globalization has given acceptance to technology in the whole world. Today we can access any information related to anyone from anywhere at any time but this poses a new threat to private and confidential information i.e. right to privacy. In today's digital world it is very difficult to prevent information to escape into the public domain if someone is determined to put it out without using extremely repressive methods. The right to privacy is recognized in Indian Constitution but its growth and development is entirely left at the mercy of the judiciary.**

This paper aims to establish an independent and effective oversight mechanism with a mandate to monitor all stages of interceptions of communications to ensure they are compliant with India's domestic and international obligations to respect and protect the right to privacy and other human rights in digital era.

Keywords: Surveillance, Privacy, Democracy, Countervailing, Technology, Defamation, Repporteur, interference, liberty.

INTRODUCTION

Digital communications technologies, such as the Internet, mobile smart phones and Wi-Fi-enabled devices, have become part of everyday life. By dramatically improving access to information and real-time communication, innovations in communications technology have boosted freedom of expression, facilitated global debate and fostered democratic participation. By amplifying the voices of human rights defenders and providing them with new tools to document and expose abuses, these powerful technologies offer the promise of improved enjoyment of human rights. As contemporary life is played out ever more online, the Internet has become both ubiquitous and increasingly intimate.

In the digital era, communications technologies also have enhanced the capacity of Governments, enterprises and individuals to conduct surveillance, interception and data collection.

As noted by the Special Rapporteur on the right to freedom of expression and opinion, technological advancements mean that the State's effectiveness in conducting surveillance is no longer limited by scale or duration. Declining costs of technology and data storage have eradicated financial or practical disincentives to conducting surveillance.

The State now has a greater capability to conduct simultaneous, invasive, targeted and broad-scale surveillance than ever before. In other words, the technological platforms upon which global political, economic and social life is increasingly reliant are not only vulnerable to mass surveillance, they may actually facilitate it.[1]

[1] A report of A/HRC/23/40, para. 33

Vol. 2, Issue 2, April - June 2017
ISSN: 2456 - 608X
International Journal of Legal Research and Studies
UGC Approved Online Journal (Sr. No. 1224 & Journal No. 48489)

THE RIGHT TO PRIVACY

Privacy is a fundamental human right, enshrined in numerous international human rights instruments. It is central to the protection of human dignity and forms the basis of any democratic society. It also supports and reinforces other rights, such as freedom of expression, information and association.

Activities that restrict the right to privacy, such as surveillance and censorship, can only be justified when they are prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued.[2]

As innovations in information technology have enabled previously unimagined forms of collecting, storing and sharing personal data, the right to privacy has evolved to encapsulate State obligations related to the protection of personal data. A number of international instruments enshrine data protection principles, and many domestic legislatures have incorporated such principles into national law.

Privacy also has implication for the freedom of opinion and expression. The Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression emphasizes that the "right to privacy is often understood as an essential requirement for the realization of the right to freedom of expression. Undue interference with individual's privacy can both directly and indirectly limit the free development and exchange of ideas."[3]

DOMESTIC LAWS RELATED TO PRIVACY: A CONSTITUTIONAL ASPECTS

The Constitution of India does not specifically guarantee a right to privacy; however through various judgments over the years the Courts of the country have interpreted the other rights in the Constitution to be giving rise to a (limited) right to privacy – primarily through Article 21 – the right to life and liberty. It says "No person shall be deprived of his life and personal liberty except procedure established by law."

This article reminds us one of the famous clauses of the Magna Carta:

"No ma shall be taken or imprisoned, disseized or outlawed, or exiled, or in any way destroyed save…by the law of law."

It means that no member of executive shall be entitled to interfere with the liberty of a citizen unless he can support his action by some provision of law.[4]

In 2015, this interpretation was challenged and referred to a larger Bench of the Supreme Court (the highest Court in the country) in the writ petition Justice *K.S Puttaswamy & Another vs. Union of India and Others*[5], the case is currently pending in the Supreme Court.

[2] Universal Declaration of Human Rights Article 29; General Comment No. 27, Adopted by The Human Rights Committee Under Article 40, Paragraph 4, Of The International Covenant On Civil and Political Rights, CCPR/C/21/Rev.1/Add.9, November 2, 1999; See also Martin Scheinin, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism," 2009, A/HRC/17/34.

[3] 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)

[4] Basu, Dr. Durga Das, Introduction to the Constitution of India, Wadhwa Publications, 2007, p.n. 108.

[5] (2014) 6 SCC 433

Vol. 2, Issue 2, April - June 2017
ISSN: 2456 - 608X
International Journal of Legal Research and Studies
UGC Approved Online Journal (Sr. No. 1224 & Journal No. 48489)

The constitutional right to privacy in India is subject to a number of restrictions. These restrictions have been culled out through the interpretation of various provisions and judgments of the Supreme Court of India:

• The right to privacy can be restricted by procedure established by law which procedure would have to be just, fair and reasonable *(Maneka Gandhi v. Union of India)*[6];

• Reasonable restrictions can be imposed on the right to privacy in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence; (Article 19(2) of the Constitution of India, 1950)

• The right to privacy can be restricted if there is an important countervailing interest which is superior (*Gobind v. State of M.P.*)[7];

• The right to privacy can be restricted if there is a compelling state interest to be served (*Gobind v. State of M.P.*)[8];

• The protection available under the right to privacy may not be available to a person who voluntarily thrusts her/himself into controversy (*R. Rajagopal v. Union of India*)[9].

• Like most fundamental rights in the Indian Constitution, the right to privacy has been mostly interpreted as a vertical right applicable only against the State, as defined under Article 12 of the Constitution, and not against private citizens. (*Zoroastrian Cooperative Housing Society v. District Registra*r).[10]

India does not have comprehensive privacy legislation and limited data protection standards can be found under section 43A and associated Rules in the Information Technology Act 2000.

INTERNATIONAL OBLIGATIONS

India has ratified the International Covenant on Civil and Political Rights ('ICCPR'). Article 17 of the ICCPR provides that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence or to unlawful attacks on his honour and reputation". The Human Rights Committee has noted that states party to the ICCPR has a positive obligation 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 right [privacy]."

While other nations should not localize servers as that may balkanise the Internet, the U.S. has to do more to show that it is not infringing on the rights of global citizens.[11]

Much has happened in the last six months, in different parts of the world, after the global surveillance programme of the United States National Security Agency (NSA) was revealed by Edward Snowden, a former NSA contractor. In the U.S., there was a lot of noise made by privacy and liberty groups — such as American Civil Liberties Union, Center for Democracy and Technology, and Electronic Frontier Foundation among others — and some Senators and Congressmen.

[6] (1978) 1 SCC 248
[7] (1975) 2 SCC 148
[8] Ibid.
[9] (1994) 6 SCC 632 (popularly known as Auto Shanker's case)
[10] AIR 1997 Guj 136.
[11] An article on 'The Right to Privacy in Digital Age', Published in 'The Hindu' on January 11, 2014.

Vol. 2, Issue 2, April - June 2017
ISSN: 2456 - 608X
International Journal of Legal Research and Studies
UGC Approved Online Journal (Sr. No. 1224 & Journal No. 48489)

Even U.S. President Barack Obama raised some questions on the propriety of such a massive surveillance programme. He set up a committee under the chairmanship of Richard Clarke, former National Coordinator for Security, Infrastructure Protection, and Counter-terrorism for the U.S., to review the programme for recommendations to scale it down so as to be less intrusive in the lives of Americans and others. Within three months, the committee submitted its report to President Obama — on December 12, 2013 to be precise. In the months leading up to the submission of this report, there were strong reactions from the European Union, especially Germany and France. Angela Merkel's personal mobile phone was kept under surveillance by the NSA. She was put on a par with the Brazilian President Dilma Rousseff, whose phone gave away several governance and economic secrets to the Americans.[12]

The EU leaders condemned the NSA; the American ambassadors in various European cities were summoned and asked to explain their government's actions. Threats were held out that the safe harbor extended to the U.S. for EU data flows would be withdrawn. Although the Brazilian President sent a strong signal by cancelling her visit to the White House, she was sought to be pacified through the offer of ICANN CEO Fadi Chehadé for holding a conference in April, 2014, in Brazil to consider or establish a new governance framework for ICANN, which currently governs the Internet under the exclusive control of the U.S. government. In the meantime, Brazil and Germany had moved a resolution in the UN for nations to agree on privacy protection for citizens in cyberspace, which was passed by the General Assembly on December 18, 2013, as 'Right to Privacy in the Digital Age'[13].

It was sponsored by more than 50 countries, including India, and approved unanimously by the 193 members. The resolution upholds the right to privacy for everyone when billions of innocent individuals around the world have been victims of the sweeping mass surveillance conducted by the U.S. and the United Kingdom from their domestic soil. It reaffirms the human rights core principle that individuals cannot be denied human rights simply because they live in a country different from the one that is placing them under surveillance. The resolution calls upon states to end violations of privacy by ensuring that national legislation complies with obligations under international human rights law, and "to review their procedures, practices and legislation regarding the surveillance of communications, their interception and collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law."

The Clarke Committee in its report, titled "Liberty and Security in a Changing World", observes that advances in ICT continue along with increased globalization of trade, investment and information flows, as also the national security threats. Information collection by intelligence cannot distinguish between 'domestic' and 'foreign', leading to violation of the privacy of American citizens and foreigners. Even strategic relationships with allies get into difficulties because of pursuing "multiple and competing goals at home and abroad". These goals include: protecting the nation against threats to national security, foreign policy interests, the right to privacy, democracy, civil liberties, the rule of law promoting prosperity, security, and openness in a networked world. But the recommendations do not suggest that bulk data of U.S. persons or non-U.S. persons should not be collected.[14]

[12] Ibid.
[13] A/HRC/23/40, para. 33.
[14] Section 702 of the Foreign Intelligence Surveillance Act (FISA).

Vol. 2, Issue 2, April - June 2017
ISSN: 2456 - 608X
International Journal of Legal Research and Studies
UGC Approved Online Journal (Sr. No. 1224 & Journal No. 48489)

While it does make some recommendations on 'probable cause' for U.S. citizens to be shown to the Foreign Intelligence Surveillance Court (FISC), there is no such concession for non-U.S. persons. It is interesting that the committee acknowledges, albeit indirectly, that the U.S. government is undermining encryption standards, and subverting or weakening commercial encryption software, by advising the government not to do so. Likewise, it recommends that surveillance of foreign leaders should be done after due consideration of possible reactions by concerned countries, if it ever becomes public. The committee does not recommend that bulk data collection, in the form of meta-data of phone calls, under Section 215, be stopped. Instead it should be held by a private entity, and made available to the NSA after a judicial order by the FISC. There are several other recommendations, some of which will cause discomfort in the intelligence community.

No wonder, in the congressional hearings, both the NSA and the Director, National Intelligence, have strongly urged that the surveillance programme should be allowed to continue in its present form, since it is essential for its counterterrorism operations. The committee reiterates the position of the U.S. government on the Internet for global agreements, namely freedom of expression, Internet governance through multi-stakeholderism, use of the mutual legal assistance treaty process for gaining access to electronic communications, not engage in espionage to steal trade secrets through surveillance, not to sabotage financial systems. In a clear message to the Brazilian President, it recommends that countries should not try to locate servers in their territories, or prevent data trans-border data flows. While other nations should not localise servers as that may balkanise the Internet, the U.S. has to do more to show that it is not infringing on the rights of global citizens or undermining the sovereignty of nations. Will the U.S. review its laws, procedures and practices regarding the mass surveillance of communications, their interception and collection of personal data to uphold the right to privacy by ensuring the full and effective implementation of its obligations under international human rights law, as per the UN resolution, to which it was a party?[15]

AREAS OF CONCERN OR ISSUES RELATING TO RIGHT TO PRIVACY IN THE DIGITAL AGE

COMMUNICATIONS SURVEILLANCE

Broad and fragmented standards for surveillance

Communication surveillance in India is primarily regulated by two different statutes, the Telegraph Act, 1885[16] and the Information Technology Act, 2000.[17]

Before 1996, the state authorities relied upon the provisions of the Telegraph Act to carry out interception of phone calls. The Act allows any authorized public official to intercept communications on the occurrence of any public emergency or in the interest of public safety. Communications can be intercepted under the Telegraph Act during "public emergencies" or in the interest of "public safety" provided that such interception is in the interests of certain other grounds, namely, the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order and for preventing the incitement of offences. Such broad and vague justifications for surveillance have become a

[15] www.thehindu.com/opinion/op-ed/the-right-to-privacy-in-the-digital-age/article5563151.

[16] "Telegraph Act", which deals with interception of calls.

[17] ("IT Act"), which deals with interception of electronic data.

Vol. 2, Issue 2, April - June 2017
ISSN: 2456 - 608X
International Journal of Legal Research and Studies
UGC Approved Online Journal (Sr. No. 1224 & Journal No. 48489)

feature of many jurisdictions. The concept of national integrity or security are usually defined very broadly and are vulnerable to misuse as a means to target certain kinds of actors and propagate unnecessary secrecy around law enforcement measures, thus, having an adverse impact on transparency and accountability.

However, in 1996 the Supreme Court noticed the lack of procedural safeguards in the provisions of the Telegraph Act and laid down certain guidelines for interceptions. These guidelines formed the basis of the Rules defining the procedures of interception that were codified by introducing Rule 419A in the Telegraph Rules in 2007. These guidelines were, in part also reflected in the Rules prescribed under the IT Act in 2009.

Section 69 of the IT Act allows for the interception, monitoring and decryption of digital information in the interest of the sovereignty and integrity of India, of the defense of India, security of the State, friendly relations with foreign nations, public order, preventing the incitement to the commission of any cognizable offense relating to the above, and for the investigation of an offense. While this provision is similar to interception provision under the Telegraph Act mentioned above, it is noteworthy that it dispenses with the sine qua non of "the occurrence of public emergency of the interest of public safety", thus dramatically broadening the ambit of powers. The rules framed under Section 69 and 69B10 [18](the "IT Interception Rules") include safeguards stipulating who may issue directions of interception and monitoring, how such directions are to be executed, the duration they remain in operation, to whom data may be disclosed, confidentiality obligations of intermediaries, periodic oversight of interception directions by a Review Committee under the Indian Telegraph Act, the retention of records of interception by intermediaries and to the mandatory destruction of information in appropriate cases. Rule 3 allows the "competent authority" to issue directions for monitoring for any of a number of specified purposes related to cyber security.

Access to stored data is also potentially addressed theoretically, under section 91[19], law enforcement agencies in India can access stored data. Section 92 of the Cr.P.C. also allows District Magistrates and Courts to issue directions requiring document, parcel or "things" within the custody of any postal or telegraph authority to be produced before it if needed for the purpose of any investigation, inquiry, trial or other proceeding under the Code. There is little judicial clarity on the subject but it may be argued that it is possible to interpret the provisions in a way that even private ISPs can be considered as postal or telegraph authorities and thus become subject to interception under this section.
Although there is broad symmetry between the legislations, there are still important differences as to when surveillance can be undertaken under the Information Technology Act, 2000 vis-à-vis the Indian Telegraph Act, 1885.

In 2012, a group of experts was appointed by the government to identify privacy issues and prepare a paper to inform a Privacy legislation in India.11 As part of their report, the Group of Experts undertook a

[18] The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.
[19] Section 91 of the Code of Criminal Procedure, 1973 "Cr.P.C." which states that a Court in India or any officer in charge of a police station may summon a person to produce any document or any other thing that is necessary for the purposes of any investigation, inquiry, trial or other proceeding under the Cr.P.C.

Vol. 2, Issue 2, April - June 2017
ISSN: 2456 - 608X
International Journal of Legal Research and Studies
UGC Approved Online Journal (Sr. No. 1224 & Journal No. 48489)

review of the Telegraph Act and Information Technology Act noting that that there were clear inconsistencies with regards to: "permitted grounds,", "type of interception," "granularity of information that can be intercepted," the degree of assistance from service providers, and the "destruction and retention" of intercepted material. The report of the Group of Experts concluded that these discrepancies "have created an unclear regulatory regime that is non-transparent, prone to misuse, and that does not provide remedy for aggrieved individuals."[20]

LACK OF DATA PROTECTION STANDARDS FOR THE PUBLIC SECTOR

Section 43A and associated Rules apply only to "body corporate", thus not extending the same requirements to the public sector. The lack of a comprehensive data protection policy that is applicable to the public sector is particularly concerning giving the numerous government led data driven initiatives which have already been implemented and others that are emerging in India including Digital India, the Unique Identity Scheme, and the National Population Register. The intent of these schemes is to register all residents of the country and provide them with unique identifiers,[21] seeding of different databases (feeding information into the database) with unique identifiers,[22] and enable the implementation of large e-governance projects,[23] all of which will involve collection of vast amount of personal data. The absence of any regulation governing the collection, use and sharing of such data leads to serious privacy concerns.

RECOMMENDATIONS

We recommend that the Government of India:

• Harmonize the legal framework which regulate communications surveillance in India to ensure that the law is accessible and clear, and meets India's international human rights obligations;

• Establish an independent and effective oversight mechanism with a mandate to monitor all stages of interceptions of communications to ensure they are compliant with India's domestic and international obligations to respect and protect the right to privacy and other human rights;

• Establish independent accountability mechanisms and clear standards for India's security and intelligence agencies to ensure they are subject to independent oversight mechanisms and guarantee transparency of their mandate and operations in accordance with international human rights standards;

• Review and reform the regulations regarding export and import of surveillance technologies to and from India;

• Review all licensing agreements which impose obligations on the private sector to facilitate and/or conduct communication surveillance, and take the necessary measures to ensure that the private sector – in both policy and practice – comply with international human rights law and standards;

• Review the proportionality of data retention requirements placed on telecommunications companies;

• Adopt and enforce a comprehensive data protection legal framework that meets international standards, applies to both the private and public sector, and establish an independent data protection authority that is appropriately resourced and has the power to investigate data protection breaches and order redress.[24]

[20] "Report of the Group of Experts on Privacy", Planning Commission of India, 7: 19, p. 60-61, October 16, 2012, http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf

[21] : https://uidai.gov.in/beta/about-uidai/about-uidai/vision-mission.html

[22] https://uidai.gov.in/images/aadhaar_seeding_june_2015_v1.1.pdf

[23] http://www.digitalindia.gov.in/

[24] The Report on "The right to Privacy in India", submitted by Centre for Internet and Society India and Privacy International, October, 2016.

Vol. 2, Issue 2, April - June 2017
ISSN: 2456 - 608X
International Journal of Legal Research and Studies
UGC Approved Online Journal (Sr. No. 1224 & Journal No. 48489)

CONCLUSION

Privacy is a basic human right and computer systems contain large amount of data that may be sensitive. Chapters IX and XI of the Information Technology Act define liabilities for violation of data confidentiality and privacy related to unauthorized access to computer, computer system, computer network or resources, unauthorized alteration, deletion, addition, modification, destruction, duplication or transmission of data, computer database, etc. The data protection may include financial details, health information, business proposals, intellectual property and sensitive data.

However, today we can access any information related to anyone from anywhere at any time but this poses a new threat to private and confidential information. Globalization has given acceptance to technology in the whole world. As per growing requirement different countries have introduced different legal framework like DPA (Data Protection Act), 1998 UK, ECPA (Electronic Communications Privacy Act of 1986) USA, etc. from time to time. In USA some special privacy laws exist for protecting student education records, children online privacy, individual's medical records and private financial information. In both countries self-regulatory efforts are facilitating to define improved privacy surroundings.

The right to privacy is recognized in Indian Constitution but its growth and development is entirely left at the mercy of the judiciary. In today's connected world it is very difficult to prevent information to escape into the public domain if someone is determined to put it out without using extremely repressive methods. Data protection and privacy has been dealt with in the Information Technology Act, 2000 but not in an exhaustive manner. The IT Act needs to establish setting of specific standards relating to the methods and purpose of assimilation of right to privacy and personal data. We may conclude by saying that the IT Act is facing the problem of protection of data and a separate legislation is much needed for data protection striking an effective balance between personal liberties and privacy.