Contemporary Relevance of RTI Act And Right To Privacy

By SHRUTI VERMA

B.B.A. LL.B (Hons.)

AMITY LAW SCHOOL, NOIDA

Contents

1. INTRODUCTION

Right to information (RTI) caters a fundamental right upon the citizens so that it gives them a legal right to access the information held by government bodies or instrumentalities of the government. And simultaneously, Right to privacy allows the individuals to have authority and supervision of the personal information about them that is held by the government and private bodies for instance Aadhar card or bank details. Right to Information and Right to privacy are complementary and supplementary to each other. They are the Two sides of the same coin. They can be rightly called as complementary and supplementary to each other. But contrary to this nature of these two there exit a conflict between them. Right to Information and Right to privacy both have been globally recognised by more than 110 countries have adopted these laws. 50 countries across the globe guarantee right to Information in its constitution.[1]

If we talk about current situation which is prevalent around us it can be witnessed that technologies have taken over lives, and as far as it is concerned with privacy, the privacy of the individual is being increasingly challenged by new technologies and trends in the society and with the introduction of internet the invasion over an individual privacy are quotidian. Sensitive personal data of an individual is very elementary to leak. Public records are disclosed over internet and go viral with an blink of an eye. In response to this it became the necessity of an hour to give the control over their personal information to promote it many countries have incorporated comprehensive laws that give individual certain rights to control over the collection and use of their personal information by public and private bodies. Right to information is a "Sine quo non" of democratic polity which means that right to information cannot exist without a democratic establishment.

[1] Source: Global RTI Rating.

2. RIGHTS DEFINED

2.1 RIGHT TO INFORMATION

"If liberty and equality, as is thought by some are chiefly to be found in democracy, they will be best attained when all persons alike share in the government to the utmost".[2]

The right to information is implicitly guaranteed by the Constitution. To establish a practical regime for securing and safe guarding the information, the Indian Parliament enacted a legislation the Right to Information Act, 2005giving a powerful tool to the citizens to get information from the Government as a matter of right. This law is very comprehensive in nature that is it covers all the aspect and all matters of governance and has the broadest reach, being applicable to Government at all levels Union, State and Local as well as recipients of government grants.[3]

The term "information" means any material in any form, which may include records, documents, memos, e-mails, opinions, advice, press releases, circulars, orders, logbooks, contracts, reports, papers, samples, models, data material held in any electronic and information relating to any private body which can be accessed by a public authority under any other law for the time being in force.

Under RTI the right of access to the information which is held by government bodies is classified as the basic right of the human being. Right to information is derived from the right of freedom of expression to seek and receive information.[4] Under RTI any person who seeks to get some information may make an official request to a body. And that public body gets legally bounded under RTI Act to respond to such requests Right to information or Freedom of

[2] Aristotle.
[3] Guide on RTI Act 2005
[4] See the Universal Declaration of Human Rights (UDHR), art. 19.

Information (FOI) is defined as the universal right to access or seek information held by public bodies.

In a democratic establishment individual have right to seek information. The Right to Information is the bed rock of democracy and paves the way of transparency and accountability in governance of the affairs of the state and ensure effective participation of the people in democratic society.[5] It also promotes good governance. Good Governance is the process of making decision and implementing them.

The right to information is not specifically written in the Constitution of India 1950, it has been interpreted through Articles 14 (right to equality), 19(1)(a) (freedom of speech and expression) and 21 (right to life) and through number of cases such as Bennet Coleman v. Union of India,[6] Tata Press Ltd. v. Maharashtra Telephone Nigam Ltd.,[7] etc. The same Articles were also interpreted in Kharak Singh v.State of U.P.[8], Govind v. State of M.P., and a number of other cases, to include within their scope a right to privacy.

The objective of the act is to establish "the practical regime of right to information for citizens to secure access to information under the control of public authorities, in order to promote transparency and accountability in the working of every public authority, the constitution of a Central Information Commission and State Information Commission and for matters connected therewith and incidental thereto"[9]

2.2 Right to information is not absolute

There is a famous saying that power corrupts and absolute power corrupts absolutely. No right can be absolute in nature. Therefore to have a check and balance between right and power to access it Right to information is not

[5] David Banisar, 2011, The Right to Information and Privacy: Balancing Rights and managing conflicts. Washington. The World Bank.
[6] . Australia Freedom of Information Act, 1982.
[7] Bennet Coleman v. Union of India, AIR 1973 SC 106
[8] 1963 AIR 1295, 1964 SCR (1) 332
[9] The preamble to the RTI Act, 2005

absolute in nature and comes along with certain restrictions. Right to information will always be restricted when it comes to national security and interest .Under Right to Information Act section 8 talks about restrictions that are imposed on right to access the right to information.

Exemptions from disclosure of information are as below: No right is absolute in nature. Right to Information Act provides for certain exemption to hold on to information and not to disclose it. Followings are the situation where government can hold on to access to information:

1) Information which would prejudice International relations, integrity and national security of India.
2) Information which has been expressly forbidden to be publish by court or tribunal or if such disclosure of information leads to contempt of court.
3) Information which is covered by legal / professional privilege.
4) Information including commercial confidence, trade secrets or intellectual property, the disclosure of which would harm the competitive position of a third party.
5) Information which is being seeked out of fiduciary relationship.
6) Information, the disclosure of which would endanger the life or physical safety of any person or identify the source of information or assistance given in confidence for law enforcement or security purposes. For example in case of whistle blower policy.
7) Information which would hinder the process of investigation or apprehension or prosecution of offenders.
8) Information related to cabinet paper and their records.

2.2 Section 8(1) (j) of Right to Information Act

Section 8(1)(j) of The Right to Information is read as “information which relates to personal information the disclosure of which has no relationship to

any public activity or interest, or which would cause unwarranted invasion of the individuals privacy unless the Central Public Information Officer or the State Public Information Officer or the appellate authority as the case may be, is completely satisfied that the larger public interest justifies the disclosure of such information is involved in the matter. Provided that the information, which cannot be denied to parliament or a state legislature shall not be denied to any person".[10]

With respect to each and every activity the Right to Information is not vested absolutely. With respect to certain areas the disclosure of information can be denied to a person by giving cogent reasons. Section 8(1)(j) protects the personal information of an individual against disclosure under RTI Act.When it is read whole it is apparent that personal information does not mean information pertinent to information seeker since the question of invasion of privacy does not arise in his own case. Therefore when a citizen seeks information about his own case and as long as the information sought is not exempt in terms of other provisions of section 8 of RTI Act. This section is not applicable to deny the information. The document submitted by individuals applicants contain a lot of information as personal detail, income , PAN , source of funds , partnership detail plan to learn dealership, affidavit etc, which are personal document and contain a lot of confidential information submitted by third parties that are not to be given.

2.3 Section 11 of Right to Information Act

Where the CPIO or SPIO intends to disclose any information or record on request made under this Act, which relates to and was supplied by a third party, it shall be within five days of the receipt of such request, given a written notice to such third party inviting her to make submission in writing or orally regarding whether such information should be disclosed, and such submission shall be

[10] Section 8(1)(j) of The Right to Information Act,2005.

kept in view while taking decision regarding the disclosure of such information.[11]Though there is an exception in case of Trade or commercial secrets protected by law. In such cases disclosure is allowed only if public interest outweighs the non-disclosure in importance any possible harm or injury to the third party.

If the information seeker request an information, document or records which are in relation to the third party and it has been treated confidential by that party, then the CPIO or SPIO can serve a notice to a third party as an opportunity given to make representation against the proposed disclosure within 10 days.

3. RIGHT TO PRIVACY

Right to Privacy is an integrated part of Article 21 of the Constitution of India. The Supreme court has stated that Article 21 is the heart of the Fundamental Rights provided in the part III of the constitution of India. The Constitution of India does not specifically guarantee a "right to privacy". However, through various judgments, Indian courts have interpreted the other rights in the Constitution as giving rise to a right to privacy primarily through Article 21, the right to life and liberty. In the year 1963 in the case of Kharak Singh v. State of U.P.[12], AIR 1963 SC 1295: (1963) 2 Cri LJ 329, the Supreme Court had consider the scope of Right to Privacy when the power of surveillance conferred on the police by the provisions of the U.P. Police Regulations came to be challenged as it was voilative of Articles 19 and Article 21 of the Constitution. The Court repelled the argument of infringement of freedom guaranteed under Article 19(1)(*d*) of the Constitution, and asserted that the movements of an individual was held not to be an infringement of any

[11] Section 11 of RTI Act 2005.
[12] AIR 1963 SC 1295: (1963) 2 Cri LJ 329

fundamental right. The judgement emphasized on the need for recognition of right to privacy was essential for the personal liberty of an individual.

In Black's Law Dictionary Right to Privacy is defined as "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 the public is not necessarily concerned". Though Right to Privacy is not just confined to this definition it also includes rights such as protection from trespassers into family and home life, control of sexual and reproductive rights and communications secrecy (Doctor-patient communication, Lawyer-client privileges).

Privacy is essential for the development of an individual's ideas and their personal relationship with other individual and society. The Right to Privacy is a recognised legal in almost national constitution worldwide. It is also included in major international human rights treaties, for example the Universal Declaration of Human Rights,[13] the International Covenant on Civil and Political Rights,[14] the European Convention on Human Rights,[15] International bodies, including the European Court of Human Rights and the United Nations (UN) Human Rights Committee, have also given rulings on Right to privacy.[16]
The Court has implied the right of privacy from Article 21of the constitution by interpreting it in accordance with Article 12 of the Universal Declaration on Human Rights and Article 17 of the International Covenant on Civil and Political Rights, 1966. Both of these international documents provide for the right of privacy and many countries look up to these document and exercise the right to privacy in conformity with these two major document.

[13] UDHR,Art. 12.
[14] Ibid. ,Art. 17.
[15] Ibid.,Art. 8.
[16] For example, see Netherlands—CCPR/C/82/D/903/1999 [2004] UNHRC 60 (November 15, 2004), http://www1.u mn.edu/humanrts/undocs/html/903-1999.html

4. DEVELOPMENT OF PRIVACY IN INDIA

1. Kharak Singh v. The State of U.P.(1962: In this case before the Supreme Court, a minority opinion recognised the right to privacy as a fundamental right but this was not the majority opinion. The minority Judges located the right to privacy under both the right to personal liberty as well as freedom of movement.

2. Govind v. State of M.P (1975): In this case The Supreme Court established that the right to privacy is a fundamental right. It derived the right to privacy from both the right to life and personal liberty as well as freedom of speech and movement. The right to privacy was said to encompass and protect the personal intimacies of the home, the family marriage, motherhood, procreation and child rearing. However, the right to privacy is subject to "compelling state interest".

3. R.Rajagopal v. Union of India (1994): Another case of the Supreme Court determined that the right to privacy is a part of the right to personal liberty guaranteed under the constitution. It was acknowledged that the right to privacy can be a tort (actionable claim) as well as a fundamental right. A citizen has a right to safeguard his own privacy, his family, marriage, procreation, motherhood, child-bearing and education among other matters and nobody can publish anything regarding the same unless:

- he consents or voluntarily thrusts himself into controversy,
- the publication is made using material which is in public records (except for cases of rape, kidnapping and abduction),
- he is a public servant and the matter relates to their discharge of official duties.

4. People's Union for Civil Liberties v. Union of India(1996): This case of the Supreme Court extended the right to privacy to communications. In doing so, the Court laid down guidelines that form the backbone for checks and balances in interception provisions in India such as:

- At both the Central and State government Interception orders to be issued only by Home Secretaries.
- Before making the decision to approve interception two things should be considered which are whether there is the necessity of the information and whether it can be acquired by other means.
- The addresses and the persons whose communication has to be intercepted should be specified in the order.

5. Selvi and others v. State of Karnataka and others (2010): The Supreme Court recognised the distinction between physical privacy and mental privacy. The scheme of criminal and evidence law makes it mandatory interference with the right to physical and bodily privacy in certain circumstances, but the same cannot be used to compel a person "to impart personal knowledge about a relevant fact". This case also established the intersection of the right to privacy with Article 20(3) (self-incrimination). An individual's decision to make a statement is the product of a private choice and there should be no scope for any other individual to interfere with such autonomy. Subjecting a person to techniques such as narco analysis, polygraph examination and the Brain Electrical Activation Profile (BEAP) test without his or her consent violates the subject's mental privacy.

6. Unique Identification Authority of India and another v. Central Bureau of Investigation(2014) : In this case, the Central Bureau of Investigation sought access to the database of the Unique Identity Authority of India for the purposes of investigating a criminal offence. However, the Supreme Court in an interim order held that the Unique Identity Authority of India should not transfer any biometric information of any person who has been allotted an Aadhaar number to any other agency without the written consent of that person.

7. Justice K.S.Puttuswamy (Retd.) & Another v. Union of India : In this case Supreme Court ordered that the issue of privacy was discussed in light of the Unique Identity Scheme. The question before the court was whether such a right is guaranteed under the Constitution, and if it is, the source of this right, given

that there is no express provision for privacy in the Indian Law. The Attorney General of India argued that privacy is not a fundamental right guaranteed to Indian citizens. Ultimately, the Court left the question to be deliberated by a larger constitutional basis since the earlier judgments that denied the existence of the right to privacy were given by larger benches than the cases where the right to privacy was accepted as a fundamental right. This lead to unresolved controversy, leading the Court to refer the matter to a larger bench to be settled.

8. REGIONAL AND INTERNATIONAL CONVENTIONS

India is party to two international instruments containing privacy protections. These are The Universal Declaration on Human Rights (Article 12) and The International Covenant on Civil and Political(Article 17).

9. CONCEPT OF DATA PROTECTION

In the era where there is a speedy growth in the technologies have led to raise privacy issues relating to the collection, use and circulation of personal data in information systems. Now which information can be termed as personal information, many international treaties have interpreted the term personal information. Personal information is single piece of the set of information by which a person's identity can be revealed. For example individual's name, address, nationality, Phone number, date of birth or a facial image. Vehicle registration plate numbers, credit card numbers, fingerprints, a computer's IP address, CCTV video footage, or health records can also constitute as personal information.

9.1. What is Data Protection?

"Data protection is commonly defined as the law designed to protect your personal information which is collected processed and stored by automated

means or intended to be part of a filing system.[17] Data Protection acts like an instrument which can be used by a citizen or consumer to have a means to exercise the Right to Privacy and to protect themselves and their information against any abuse. Where Government, Organisations, Public or private bodies collect and uses your personal information for any reason for example census, implementing new policies, requirement for app usage whatever the case may be the comes under the obligation to use and handle such data in accordance with The Data Protection Laws. This law is based on principles. There are eight principles which are enumerated as below :

- There should be strict check on the limit of collection of personal data. Such data should be obtained by lawful and fair means with the consent of the individual.
- The personal information should be accurate and relevant and should be used for the stated purpose.
- The purposes should be specified at the time of collection of data without any ambiguity.
- The information must be secured and protected. Data collector must insure the safety of the information and reasonable safeguard.
- There should be no secrecy while collecting data. The purpose of collecting data must be made clear, stating for what purpose their information is being collection, where it will be used, whether they will retain the information or not. Etc.
- Organization will be held liable in case of any abuse of their data and personal information.
- Each individual have right to be involved. An individual have right to access to his/her information and change it. Can also ask that information to be deleted from the database also its rectification or completion.

[17] Privacy International[GB], https://www.privacyinternational.org/node/44

- Information must be collected in good faith. The intention behind collecting the information should be bona fide. One's information should not be used against them or to harm other.

The rules and regulations of Data Protection are enforced by authority called information privacy commissioner. Such authority have power to conduct an investigation, process the complaint, held the party liable and impose fine when there is breach of law.

9.2. What is considered as personal information under data protection laws?

Personal information can be defined as any kind of information (which may include a single piece of information or a set of information) that can personally identify an individual or single them out as an individual. The obvious examples are somebody's name, address, national identification number, date of birth or a facial image. A few examples of personal information include vehicle registration plate numbers, credit card numbers, fingerprints, a computer's IP address, CCTV video footage, or health records. You can be singled out from other people even if your name is not known; for example online profiling companies assign a unique number and use tracking techniques to follow you around the net and build a profile of your behaviour and interests in order to present you with advertisements. Some personal information is considered more sensitive than other, and therefore subject to stricter rules; this includes your racial or ethnic origin, political views, religion, health, and sex life. Such information cannot be collected or used at all without your specific consent.

9.3. Are data protection laws the same in all countries that have them?

No, it is not true to say that data protection laws are same in all countries and somehow increasingly this is part of the problem. As our information travels

around the world to every corner through borderless networks, which might result our data ending up in a country where they have different laws on data protection of varying strength or no law at all, thereby we would be left with no remedies if our rights are abused. In essence, depending on what services you use, different pieces of your data will be in various countries.

Data protection law has become not only a means for protecting citizens and consumers, it has became a gateway to trade. Various international conventions and guidelines have been established in order to ensure that information can be circulated around the world without causing too much damage to 'data subjects' and that operative business do not base themselves in countries with the weakest laws. The OECD Guidelines on the Protection of Privacy, first agreed in 1980 and revised in 2013, were the pioneer in establishing the data protection principles, adopted by many countries in their legislation. A driving motivation for the OECD Guidelines was to enable protection of privacy while enabling data to flow across borders, and opening up markets.

The international instrument with most teeth however is the Council of Europe 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data. This has the force of law for the countries that have signed up to it.

10. DATA PROTECTION AND PRIVACY IN INDIA

10.1. Definition of personal data

Under the Privacy Rules and Data protection laws the term 'personal information' has been defined as any information that relates to a natural person, which either directly or indirectly, in combination with other information that is available or likely to be available to a corporate entity, is capable of identifying such person.

10.2. Definition of sensitive personal data

The Privacy Rules define 'sensitive personal data or information' to include the following information relating to[18]:

- password
- financial information. For example: bank account/credit or debit card or other payment instrument details.
- physical, physiological and mental health condition
- sexual orientation
- medical records and history
- biometric information
- any detail relating to the above clauses as provided to a corporate entity for providing services
- any of the information received under the above clauses for storing or processing under lawful contract or otherwise.

Biometrics technologies means the technologies that measure and analyse human body characteristics, such as 'fingerprints', 'eye retinas and irises', 'voice patterns', 'facial patterns', 'hand measurements' and 'DNA' for authentication.

However, any information that is freely available in the public domain is exempt from the above definition.

10.3. Law

In India there is no specified legislation for privacy and data protection. However, the Information Technology Act, 2000 contains specific provisions intended to protect electronic data (including non-electronic records or information that have been, are currently or are intended to be processed electronically).

[18] Source: https://www.dlapiperdataprotection.com.

India's IT Ministry adopted the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (Privacy Rules). The Privacy Rules, which took effect in 2011, require corporate entities collecting, processing and storing personal data, including sensitive personal information to comply with certain procedures. It distinguishes both 'personal information' and 'sensitive personal information'.

In August 2011, India's Ministry of Communications and Information issued a 'Press Note' Technology (Clarification on the Privacy Rules), which provides that any Indian outsourcing service provider/organisation providing services which involves collection, compilation, storage, dealing/handling or accessing of sensitive personal information or personal information under contractual obligation with any legal entity located within or outside India is not subject to collection and disclosure of information requirements, including the consent requirements discussed below, provided that they do not have direct contact with the data subjects (data subject refers providers of information) when providing their services.

10.4. Data Protection Officer

Every organization that collects sensitive personal information must appoint a Grievance Officer to address complaints relating to the processing of such information, and to respond to data subject access and correction requests in an expeditious manner but within one month from the date of receipt of grievance.

There is no specific requirement that the data protection officer must be a citizen of or resident of India, nor are they any specific enforcement actions or penalties associated with not appointing a data protection officer correctly. However, appointment of a data protection officer is part of the statutory due diligence process and it is thus imperative that such an officer should be appointed.

10.5. Collecting And Processing

Under the Act, if a corporate entity that possesses, manages or handles any sensitive personal information in a computer resource that it owns, controls or operates, is negligent in implementing and maintaining compliance with the Privacy Rules, and its negligence causes wrongful loss or wrongful gain to any person, the corporate entity shall be liable for damages to the person(s) affected.

The Privacy Rules state that any corporate entity or any person acting on its behalf, which is collecting sensitive personal information, must obtain written consent (through letter, email or fax) from the providers of that information. However, the August 2011 'Press Note' issued by the IT Ministry clarifies that consent may be given by any mode of electronic communication.

The Privacy Rules also mandate that any corporate entity (or any person, who on behalf of such entity) collects, receives, possess, stores, deals or handles information, shall provide a privacy policy that discloses its practices regarding the handling and disclosure of personal information including sensitive personal information and ensure that the policy is available for view, including on the website of the corporate entity (or the person acting on its behalf). Specifically, the corporate entity must ensure that the person to whom the information relates is notified of the following at the time of collection of sensitive personal information or other personal information:

- 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 that is collecting the information and the agency that will retain the information.

Further, sensitive personal information may only be collected for a lawful purpose connected with a function or purpose of the corporate entity and only if such collection is considered necessary for that purpose. The corporate entity must also ensure that it does not retain the sensitive personal information for longer than it is required, and should also ensure that the same is being used for the purpose for which it was collected.

An organization or any person acting on its behalf is obligated to enable the providers of information to review the information they had so provided and also to ensure that any personal information or sensitive personal information that is found to be inaccurate or deficient is corrected upon request. Further, the provider of information has to be provided a right to opt out even after consent has been provided. However, the corporate entity will not be held responsible for the authenticity of the personal information or sensitive personal information given by the provider of information to such corporate entity or any other person acting on its behalf.

10.6. Data security

A organization possessing, dealing or handling any sensitive personal information in a computer resource which it owns, controls or operates is required to implement and maintain reasonable security practices and procedures to secure the sensitive personal information. The reasonable security practices and procedures may be specified in an agreement between the parties.

Further, the Privacy Rules provide that in the absence of such agreement ‘reasonable security practices and procedures’ to be adopted by any Organization to secure sensitive personal information are procedures that comply with the IS/ISO/IEC 27001 standard or with the codes of best practices for data protection as approved by the Federal Government. Presently, no such codes of best practices have been approved by the Federal Government.

10.7. Breach

The Government of India, has established and authorised the Indian Computer Emergency Response Team (Cert-In), to collect, analyse and disseminate information on cyber incidents, provide forecast and alerts of cyber security incidents, provide emergency measures for handling cyber security incidents and coordinate cyber incident response activities.

The Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (Cert-In Rules) mandates the notification requirements on service providers, intermediaries, data centres and corporate bodies, upon the occurrence of certain 'cyber security incidents'.

Cyber security incidents have been defined which includes any real or suspected adverse events, interrelated to cyber security, that violate any explicitly or implicitly applicable security policy, results in[19]:

- unauthorised access, denial or disruption of service
- unauthorised use of a computer resource for processing or storage of information
- Changes to data, information without authorisation.
- The occurrence of the following types of cyber security incidents, trigger the notification requirements under the Cert-In Rules:
- Targeted scanning/ probing of critical networks/ systems
- Compromise of critical information/ system
- Unauthorized access of IT system/ data
- Defacement of websites or intrusion into website & unauthorized changes such as inserting malicious codes, links to external websites
- Malicious code attacks such as spreading virus, worm/ Trojan/ spyware

[19] See Privacy International India.

- Attacks on servers such as Database, Mail and DNS & Network devises such as Routers
- Identity theft, Spoofing and phishing attacks
- Denial of service (DoS) & Distributed Denial of service (DDoS) attacks
- Attacks on critical infrastructure , SCADA(Supervisory control and Data acquisition) systems and wireless networks
- Attacks on Application such as E-governance and E-commerce etc.

Upon the occurrence of any of the aforementioned events, companies are required to notify the Cert-In within reasonable time, so as to leave scope for appropriate action by the authorities. However, it is important to follow "breach notice obligation", which depends upon the "place of occurrence of such breach", and whether or not Indian customers have been targeted. The format and procedure for reporting of cyber security incidents have been provided by Cert-In on its official website.

10.8. Enforcement

Civil penalties of up to EUR 694,450 for failure to protect data including sensitive personal information may be imposed by an Adjudicating Officer; damages in a civil suit may exceed this amount.

Criminal penalties of up to 3 years imprisonment or a fine up to EUR 6,950, or both for unlawful disclosure of information.

11. COMPLEMENTARY ROLES OF RTI AND PRIVACY

Right to information and Right to privacy often play complementary roles. Both are focused on ensuring the accountability of powerful institutions to individual in the information era.

Several cases have laid down that these two rights overlap and complement each other. Right to Information and Right to privacy both provides an individual access to their own personal information from government bodies,

In many cases, the two rights overlap in a complementary manner. Both rights provide an individual access to his or her own personal information from government bodies. They also mutually enhance each other: privacy laws are used to obtain policy information in the absence of an RTI law, and RTI laws are used to enhance privacy by revealing abuses.

In the famous case Peoples Union for Civil Liberties v. Union Of India[20] held that true democracy cannot exit unless the citizens have a right to participate in the affair of the policy of the country. The right to participate in the affair of the country is meaningless unless the citizen are well informed on all sides of issue in respect of which they are called upon to express their view. Unilateral information, disinformation, misinformation and non-information all equally create uniformed citizens which makes democracy a farce when medium of information is monopolised either by a partisan central authority or by private individual or an organisation. This is particularly so in a country like ours where 65% of the population is illiterate.

Privacy gives the right to control about who knows what about a person, and under what conditions, thereby controlling the intimacies of life. It is all about secrecy, and the right to determine for oneself if and to what extent personal information is disseminated. The right to privacy is the protection against having a society in which the government completely controls the people's lives, and requires the government to protect individuals from privacy invasion by other people[21]. Right to privacy ensures that personal emails, bank details and medical records are safe and secure. This is essential to human dignity and autonomy in all societies around the globe.

Privacy is a fundamental right and most governments around the world have sought to protect their citizens in their beliefs, emotions, sensations and

[20] AIR 2003 SC 2363.

[21] David Banisar, 2011, The Right to Information and Privacy: Balancing Rights and managing conflicts. Washington. The World Bank.

thoughts. A person has the right to determine what kind of information is taken about them, and the purpose of that information. This helps in protecting individuals from exploitation.

Right of privacy prevents unlawful exposure of personal information. People have to right to review their information, ask for any necessary corrections and be informed on any disclosures. This is significant as it contributes to the security of the involved persons. Privacy provided by financial institutions to their customers helps on safeguarding the information collected from their customer offering security to their finances.

The constitutions should protect people from unreasonable searches and seizures. The right to privacy is most often guarded by constitutional law. For instance, In United States, the health information portability and accountability act protects a person's health information while the federal trade commission guarantees the right to privacy in various private statements and policies.

The controversy on the extent of privacy protection has forced many governments to make certain clarifications by amending the constitutions. These amendments have been used in determining the right to personal liberty. For example, in United States, the principle underlying the fourth and the Fifth Amendment is the protection against the invasion of the sanctity of a person's home and the privacy of life.[22]

Its the right of every human being to protect it privacy from the intrusion by corporations and governments. Privacy should be cherished by individuals, protected by the governments and cherished by all corporations. It is imperative for the government as well as other people to respect a person's right to keep some things to themselves.

In NAACP v. Alabama (357 U.S. 449)[23] was the landmark case in which the U.S. Supreme Court formally recognized the freedom of association as a

[22] See fourth and fifth amendment of US Constitution.
[23]377 U.S.288.84 S. Ct. 1302. 12L. Ed.2d 325 (1964)

right protected by the First Amendment**.** The Supreme Court of the United States held the demand of Alabama's unconstitutional that the NAACP reveal the names and addresses of addresses of all of its members and its agent.

Synopsis of Rule of Law: In the realm of acute liberties of speech, press, or association, curtailment of such rights, even though unintentional, may unavoidably follow from different forms of governmental action. Disclosure of affiliation with groups engaged in advocacy may result in an effective restrain on freedom of association

Facts: The Respondent, Alabama (Respondent), demanded that the Petitioner, the NAACP (Petitioner), provide a list of all of the Alabama NAACP members based on the state's foreign corporation registration law made in the course of an injunction action brought to stop the Petitioner from conducting activities in the state. Respondent moved for the production of a large number of the Petitioner's records. The Petitioner produced almost all the requested data except for membership lists. The trial court adjudged the petitioner and imposed fine. The issue were whether compelled disclosure of membership lists is in violation of the Petitioner's members' rights of freedom of association? Whether Respondent has demonstrated an interest in obtaining the membership lists, which is sufficient to justify the deterrent effect which releasing this lists would have on the free exercise of the constitutionally protected right of association?

The answer of the first question was affirmative. "Yes, the Judgment of the lower court reversed. In the domain of indispensable liberties, whether of speech, press, or association, curtailment of such rights, even though unintentional, may inevitably follow from different forms of governmental action. Compelled disclosure of affiliation with groups engaged in advocacy may constitute an effective restraint on freedom of association. There is an important relationship between freedom to associate and privacy in one's associations. This order must be regarded as entailing the likelihood of a

substantial restraint upon the exercise by the Petitioner's members of their freedom of association. Further, it is apparent that forced disclosure would result in adversely affecting the members to pursue their collective effort to foster beliefs, which they have the right to advocate. Therefore, disclosure of membership lists is in violation of the Petitioner's freedom of association.

No. Judgment of the lower court reversed. The Petitioner has not objected to divulging the identity of its members who are employed or hold office positions. There is no justification for the interest of obtaining membership lists."[24]

This case holds that disclosure of the membership lists is unconstitutional partly based on the "chilling effect" that it would have on the freedom of association. NAACP v. ALabama advances the concept of associational privacy. Yet the case has been a precedent for the right to privacy in what are clearly decisional and informational privacy cases[25]. some as progressive as Griswold v. Conneuicut[26] and Roe v. Wade[27].

12. PERSONAL INFORMATION

The word personal means appertaining to the person; belonging to an individual; limited to the person; having the nature or partaking of the qualities of human beings, or of movable property[28].

Personal Information under the Act, would be an information, that pertains to a person. It takes into its fold possibly every kind of information relating to the person. Now, such personal information of the person may, or may not be related to any public activity, or to public interest. At the same time,

[24] Allen, Anita L., "Associational Privacy and the First Amendment: NAACP v. Alabama, Privacy and Data Protection" (2011). Faculty Scholarship. Paper 507.
[25] Allen, Anita L., "Associational Privacy and the First Amendment: NAACP v. Alabama, Privacy and Data Protection" (2011). Faculty Scholarship. Paper 507.
[26] 381 U.S. 479 (1965)
[27] 410 U.S. 113(1973)
[28] See Black's Law Dictionary, Sixth Edition.

such personal information may, or may not, be private to the person. So the determination as to what constitute personal information is very crucial.

In the case **Union Public Service Commission v. R.K. Jain,** Delhi high court[29], the applicant invoked the provision of RTI Act and sought from the Public Information Officer for inspection of all records, note sheets, manuscripts, etc; on the disciplinary action taken against Shri G.S. Narang IRS, Central Excise and custom Service Officer along with final decision taken regarding imposition of penalty/ disciplinary action and the decision of UPSC.

The Delhi High Court has tried to distinguish private information and personal information by stating that personal information is a broader concept which covers all private information like family, marriage, motherhood, an employee is primarily a matter of employer-employee known as personal information that is governed by service rule.

Personal Information has also been interpreted to mean identity details of public servants like date of birth, identification numbers etc. The court also established certain considerations to be followed in order to have a balance between information and privacy rights when personal information of public officials submitted to public agencies is requested.

They are as follows :

1) Whether the information is deemed to comprise the individual's private information unrelated to the person's position in the organization.
2) Whether the disclosure of personal information is with the aim to check the proper performance of the duties and tasks assigned to him as an officer of the organization.
3) Whether the discloser will furnish information required to establish accountability and transparency in the use of public resource.

[29] W.P.(C) 1243/2011 & C.M. NO.2618/2011.

The personal information cannot be that of a "public authority". No public authority can claim that any information held by it is personal to it. There is nothing "personal" about any information held by a public authority in relation to itself. The expression "personal information" used in Section 8(1) means information personal to any "person", that the public authority may hold. For instance, a public authority may in connection with its functioning require any other person to provide information which may be personal to that person. It is that information, pertaining to that other person, which the public authority may refuse to disclose, if the information sought satisfies the conditions set out in clause (j) of Section 8(1) of the Act, i.e., if such information has no relationship to any public activity (of the person who has provided the information, or who is the source of the information, or to whom that information pertains), or to public interest, or which would cause unwarranted invasion of the privacy of the individual (unless larger public interest justifies disclosure). The use of the words "invasion of the privacy of the individual", instead of "an individual", shows that the legislative intent was to connect the expression "personal information" with the word "individual".

Merely because information that may be personal to a third party is held by a public authority, a querist does not become entitled to access it, unless the said personal information has a relationship to a public activity of the third person (to whom it relates), or to public interest. If it is private information (i.e. it is personal information which impinges on the privacy of the third party), its disclosure would not be made unless larger public interest dictates it. Therefore, for example, a querist cannot seek the personal or private particulars provided by a third party in his application made to the passport authorities in his application to obtain a passport, merely because such information is available with the passport authorities, which is a public authority under the Act. The querist must make out a case (in his application under Section 6 of the Act)

justifying the disclosure of the information sought on the touchstone of clause (j) of Section 8(1) of the Act.

13. PUBLIC ACTIVITY,PUBLIC INTEREST AND PRIVACY AS RIGHT

13.1. PUBLIC ACTIVITY

Public Activity qua a person are those activities which are performed by the person in discharge of a public duty, i.e. in the public domain. There is an inherent public interest involved in the discharge of such activities, as all public duties are expected to be discharged in public interest. Consequently, information of a person which is related to, or has a bearing on his public activities, is not exempt from disclosure under the scheme and provisions of the Act, whose primary object is to ensure an informed citizenry and transparency of information and also to contain corruption. For example, take the case of a surgeon employed in a Government Hospital who performs surgeries on his patients who are coming to the government hospital. His personal information, relating to discharge of his public duty, i.e. his public activity, is not exempt from disclosure under the Act. Such information could include information relating to his physical and mental health, his qualifications etc., as the said information has a bearing on the discharge of his public duty, but would not include his other personal information such as, his taste in music, sport, art, his family, his family background etc., which has no bearing/relation to his act of performing his duties as a surgeon.

13.2. PUBLIC INTEREST

Public interest is also a ground for taking away the exemption from disclosure of personal information. Therefore, a querist may seek personal information of a person from a public authority in public interest. The second half of the first part of clause (j) of Section 8(1) shows that when personal

information in respect of a person is sought, the authority concerned shall weigh the competing claims i.e., the claim for the protection of personal information of the concerned person on the one hand, and the claim of public interest on the other, and if "public interest" reasonably justifies the disclosure, i.e., the public interest weighs more that the need for protection of personal information, the authority concerned can disclose the information by providing that how the public interest is involved in the matter.

Public interest does not mean that which is interesting as gratifying curiosity or love of information or amusement; but that in which a class of the community have a pecuniary interest, or some interest by which their rights or liabilities are affected. The expression "public interest" is not capable of a precise definition and has not a rigid meaning and is elastic and takes its colors from the statute in which it occurs, the concept varying with the time and the state of the society and its needs[30].

The second part of clause (j) of Section 8(1) appears to deal with the scope of defence founded on the right of privacy of an individual. The tussle between the right of privacy of an individual and the right of others to seek information which may impinge on the said right of privacy, is what the said clause seeks to address.

The right to privacy means the right to be left alone and the right of a person to be free from unwarranted publicity. Black Law Dictionary says that the terms “right to privacy” is a generic term encompassing various rights recognized to be inherent in concept of ordered liberty, and such rights prevent government interference in intimate personal relationships or activities, freedoms of individual to make fundamental choices involving himself, his family, and his relationship with others and A man has the right to pass through this world, if he wills, without having his picture published, his business enterprises discussed, his successful experiments written for the benefit of

[30] See Advanced Law Lexicon, Third Edition

others, or his eccentricities commented upon by any means or mode. It is based on the theory that everyone has the right of inviolability of the person.

13.3. PRIVACY AS RIGHT

Privacy is a qualified, fundamental human right. The right to privacy is articulated in all of the major international and regional human rights instruments, including the following :

United Nations Declaration of Human Rights (UDHR) 1948, Article 12: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

International Covenant on Civil and Political Rights (ICCPR) 1966, Article 17: "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour or reputation. 2. Everyone has the right to the protection of the law against such interference or attacks."

The right to privacy is also included in:

- Article 14 of the United Nations Convention on Migrant Workers;
- Article 16 of the UN Convention on the Rights of the Child;
- Article 10 of the African Charter on the Rights and Welfare of the Child;
- Article 4 of the African Union Principles on Freedom of Expression (the right of access to information);
- Article 11 of the American Convention on Human Rights;
- Article 5 of the American Declaration of the Rights and Duties of Man,
- Articles 16 and 21 of the Arab Charter on Human Rights;
- Article 21 of the ASEAN Human Rights Declaration; and
- Article 8 of the European Convention on Human Rights.

Over 130 countries have constitutional statements regarding the protection of privacy, in every region of the world[31].

- An important element of the right to privacy is the right to protection of personal data. While the right to data protection can be inferred from the general right to privacy, some international and regional instruments also stipulate a more specific right to protection of personal data, including:
- the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,
- the Council of Europe Convention 108 for the Protection of Individuals with Regard to the Automatic Processing of Personal Data,
- a number of European Union Directives and its pending Regulation, and the European Union Charter of Fundamental Rights,
- the Asia-Pacific Economic Cooperation (APEC) Privacy Framework 2004, and
- the Economic Community of West African States has a Supplementary Act on data protection from 2010.

14. PRIVATE INFORMATION OF A PUBLIC OFFICIAL

Some of the most common problems regarding section 8(1)(j) come up when discussing information (personal or otherwise) regarding public officers. The issue comes up because an argument can be made that certain information such as income tax details, financial details, medical records, etc. of public officials should be disclosed since it has a bearing on their public activities and disclosure of such information in case of crooked officers would serve the interests of transparency and cleaner government (hence serving a larger public interest). Although section 8(1)(j) does not make any distinction between a private person and a public servant, a distinction in the way their personal

[31] See Privacy International.At: https://www.privacyinternational.org/node/54

information is treated does appear in reality due to the inherent nature of a public servant. Infact it has sometimes been argued that public servants must waive the right to privacy in favour of transparency.[32] However this argument has been repeatedly rejected by the Courts, [33] just because a person assumes public office does not mean that he/she would automatically lose their right to privacy in favour of transparency.

If personal information regarding a public servant is asked for, then a distinction must be made between the information that is inherently personal to the person and that which has a connection with his/her public functions. The information exempted under section 8(1)(j) is personal information which is so intimately private in nature that the disclosure of the same would not benefit any other person, but would result in the invasion of the privacy of the third party.[34] In short, the Courts have concluded that there can be no blanket rule regarding what information can and cannot be disclosed when it comes to a public servant, and the disclosure (or lack of it) would depend upon the circumstances of each case.

Although the earlier thinking of the CIC as well as various High Courts of the country was that information regarding disciplinary proceedings and service records of public officials is to be treated as public information in order to boost transparency, however this notion was changed in 2012 after the decision of the Supreme Court in Girish Ramchandra Deshpande v. Central Information Commissioner, and now the prevailing principle is that such information is personal information and should not be disclosed unless a larger public interest is would be served by the disclosure.

It would also be helpful to look at a list of the type of information regarding public servants which has been disclosed in the past, gleaned

[32] Vijay prakash v. Union of India,2009(82)AIC 538 (Del)
[33] Secretary General, Supreme Court of India v Subhash Chandra , Delhi High Court- full bench, LPA no.501/2009, dated 12-01-2010.
[34] See canara bank vs. Chief information commissioner,2007(58) AIC ker 667.

from various cases, to get a better understanding of the prevailing trends in such cases:

1. Details of postings of public servants at various points of time, since this was not considered as personal information;[35]
2. Copies of posting/ transfer orders of public servants, since it was not considered personal information;[36]
3. Information regarding transfers of colleagues cannot be exempted from disclosure, since disclosure would not cause any unwarranted invasion of privacy and non disclosure would defeat the object of the RTI Act;[37]
4. Information regarding the criteria adopted and the marks allotted to various academic qualifications, experience and interview in selection process for government posts by the state Public Service Commission;[38]
5. Information regarding marks obtained in written test, interview, annual confidential reports of the applicant as well as the marks in the written test and interview of the last candidate selected, since this information was not considered as personal information;
6. Information relating to the appointment and educational certificates of teachers in an educational institution (which satisfies the requirements of being a public authority) was disclosed since this was considered as relevant to them performing their functions.

The performance of an employee or officer in an organization is a matter between the employee and the employer and normally those aspects are governed by the service rules which fall under the expression "personal information", the disclosure of which has no relationship to any public activity or public interest. To understand this better below is a brief list of the type of

[35] Girish Ramchandra Deshpande v. Central Information Commissioner, 2010(119) AIC 105 (Sc).
[36]Girish Ramchandra Deshpande v. Central Information Commissioner, 2012 (119) AIC 105 (SC).
[37] Canara Bank v. Chief Information Commissioner, 2007 (58) AIC Ker 667.
[38] Haryana Public Service Commission v. State Information Commission, AIR 2009 P & H 14.

information that has been considered by the Courts as personal information which is liable to be exempt from disclosure under section 8(1)(j):

(i)

(a) Salary details,

(b) show cause notice, memo and censure,

(c) return of assets and liabilities,

(d) details of investment and other related details,

(e) details of gifts accepted,

(f) complete enquiry proceedings,

(g) details of income tax returns[39]

(ii) All memos issued, show cause notices and orders of censure/punishment etc. are personal information. Cannot be revealed unless a larger public interest justifies such disclosure.[40]

(iii)Disciplinary information of an employee is personal information and is exempt under section 8(1)(j).[41]

(iv) Medical records cannot be disclosed due to section 8(1)(j) as they come under "personal information" unless a larger public interest can be shown meriting such disclosure.[42]

(v) Copy of personnel records and service book (containing Annual Confidential Reports, etc.) of a public servant is personal information and cannot be disclosed due to section 8(1)(j).[43]

(vi) Information regarding sexual disorder, DNA test between an officer and his surrogate mother, name of his biological father and step father, name of his mother and surrogate step mother and such other aspects were denied by the

[39] Girish Ramchandra Deshpande v. Central Information Commissioner, 2012 (119) AIC 105 (SC).
[40] Girish Ramchandra Deshpande v. Central Information Commissioner, 2012 (119) AIC 105 (SC).0
[41] R.K. Jain v. Union Public Service Commission, Delhi High Court, LPA No. 618 of 2012, dated 12-11-2012.
[42] Secretary General, Supreme Court of India v. Subhash Chandra, Delhi High Court - Full Bench, LPA no.501/2009, dated 12-01-2010.
[43] Srikant Pandaya v. State of M.P., AIR 2011 MP 14.

Courts as such information was considered beyond the perception of decency and was an invasion into another man's privacy.[44]

It is not just the issue of disclosure of personal details of public officials that raises complicated questions regarding the right to information, but the opposite is equally true, i.e. what about seemingly "public" details of private individuals. A very complicated question arose with regard to information relating to the passport details of private individuals**.**

15. CONCLUSION

The Paper discusses The Right to Information and Right to Privacy and also the various important aspects such as Data protection . It can be alleged that Right to Information and protection of an individual's Privacy is paramount and helpful for an individual to exist in today's scenario where technologies have taken over our lives, where everybody is a tech savvy.

These two Right should exist together. The simple solution for harmonizing these to right can be through sanctioning crystal clear definition in legislation, regulations, guidelines and implementing it in the system. Determination of public interest of Public Interest Test should be adopted in case of Right to Information and Right to Privacy as in the Supreme Court case of Girish Ramchadra deshpande in 2012, which concerned with the issue of service details of public officials .Supreme court gave a strong interpretation of Right to Privacy and held that such information is out of the ambit of RTI unless a larger public interest is involved in the disclosure can be proven.

Now the legal boundaries of a person's privacy should be specified strictly as determined in Supreme Court case R. Rajagopal vs State of Tamil Nadu.

[44] Paardarshita Public Welfare Foundation v. Union of India and others, AIR 2011 Del 82. It must be mentioned that this case was not exactly under the procedure prescribed under the RTI Act but was a public interest litigation although the courts relied upon the provisions of the RTI Act.

Finally there should be institutional organization to ensure the harmony between Right to Information and Right to Privacy, and resolving the conflict between these two rights .The loopholes that still exist in these two laws of Right to Information and Right to Privacy must be filled. This can be achieved through airtight legislation for Right to Information, Right to Privacy and Data Protection Laws.

.....