Right to Privacy and Data Protection in the Digital Age – Preservation, Control and Implementation of Laws in India

Dr. Neelam Rai[1]

Abstract

The development in the technology has rendered many advantages to the human race. However, the advancement of the technology is now putting lots of our rights at stake. With the start of the digital age and inclusion of data which is routinely collected and traded in the new economy, the right to privacy is becoming an issue. The advancement in the technology has given rise to other criminal acts like Identity theft, pestering, online victimization etc. The personal data submitted by the persons in social media, marketing, communication surveillance companies, Government and private stakeholders and other sites can often be misused. In India there are no specific law for the collection of data, preservation, monitoring, intercepting, obtaining, analysis, using, retaining etc. The present paper is an attempt to study the issues involving right to privacy and data analysis in the digital age. This paper explores the issues of privacy by analyzing the situations wherein the data collected by the people can be misused and sometimes can be used against the person who had disclosed it. The paper is also an attempt to study the efficacy of the Information Technology Act along with other existing laws regarding right to privacy and how far they provide provisions for data protection. Since, the data are collected by the public and private sector equally thus, application of laws to each of these sectors will be studied and compared. Recently, the Ministry of Electronics and Information Technology has appointed experts headed by the former Supreme Court Judge B.N. Srikrishna to draft a data protection law. A draft Bill was made which is called the Personal Data Protection Bill, 2018. However, it could not be introduced thus ultimately on 11th December 2019 the Personal Data Protection Bill 2019 was introduced in the Lok Sabha. The present paper is an attempt to study the Bill and how far it can achieve right to privacy and data protection. It will also compare the Draft Bill of 2018 with the Bill of 2019. Thus, over all the paper aims at analyzing the areas of data protection laws in India, the lacuna and what changes can be brought for the proper implementation of the existing as well as upcoming legislations.

[1]Assistant Professor, Jalpaiguri Law College, Jalpaiguri

I. Introduction

Technological advancements are the driving force for development of any society. It has helped the human race in bringing in change and development in the society at large through its intervention in various fields like health sector, communication sector, banking etc. The 21st Century has seen the boom in the digital revolution and India is not an exception to this new trend. In India too we have maximum number of people who are internet users. Looking into this the Government of India envisaged and recently implemented "Digital India" drive. The "Digital India" drive resulted in processing of personal data through the usages of various electronic devices and applications which has rendered many advantages but is also putting our rights at risk especially the right to privacy. The public and the private sectors are engaged in collecting personal data ceaselessly plus due to the excessive use of internet people too are constantly uploading all their personal information's in various apps, forms etc. from various electronic devices they use. For example: when people file forms/application for services be it Government or private; data input for online marketing; online shopping; posts on social media; uploading Curriculum Vitae in various job sites; buying sim cards or phone connections; usages of electronic devices by children for online gaming etc. All these activities need us to put our major personal information's like the full name, address, contact details, location, friends etc. All this information's which has been put by an individual with his/her consent only for specific purposes can be easily accessible by the advertisers and organized criminals and can misuse these data and information. This not only infringes the right to privacy of an individual through various electronic means but also screams for the laws for data protection.,

II. Right to Privacy and Data Protection

'Right to Privacy' is something which makes a person able to seclude themselves from others. It generally enables a person to whether to share information's regarding themselves to others or not. It basically means the right which able a person to express themselves to selective peoples. It, in fact, gives us the ability to choose which parts can be accessed by others and to control the extend, manner and timing of the use of those parts we choose to disclose. The right prohibits others to public anything concerning the person without his/her consent. If anyone does so then he would be violating the right to the person

concerned and would be liable in an action for damages. The right to privacy is a fundamental rights recognized by International Instruments like Universal Declaration of Human Rights, 1948;[2] International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families;[3] UN Convention on the Protection of Child;[4] and International Covenant on Civil and Political Rights.[5]

Unlike the International Instruments right to privacy in India is not a separate right. It is in fact enshrined under Article 21[6] of the Constitution of India and was developed as a right through series of Supreme Court decisions starting with R. Rajagopal v. State of Tamil Nadu[7]famously known as "Auto Shankar's Case."In this case Auto Shankar who was at that time one of the prisoner in jail for committing several murders, had written his autobiography wherein he mentioned his relationships with various IAS, IPS and other police officials. Some of these were partners in his crimes. In this instant case the editor of the Tamil magazine "*Nakkheeran*" filed a writ petition restraining the government officials who were interfering with the rights of the publishers to publish the said autobiography. While deciding the case the Supreme Court held that the right to privacy is not available to government officials so far as the matter regarding their public duties is concerned even if the publication is based on untrue facts and statements. Thus, it was held that the State or its officials have

[2]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."
[3]Article 14: "No migrant worker or member of his or her family shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home correspondence or to other communications, or to unlawful attacks on his or her honour and reputation. Each migrant worker and member of his or her family shall have the right to the protection of the law against such interference or attacks."
[4]Article 16.1: "No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation."
[5]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 and reputation."
[6]Article 21: "No person shall be deprived of his life or personal liberty except according to the procedure established by law."
[7](1994) 6 SCC 632

no authority in law to impose prior restraint on publication of defamatory matter. The officials can take action only after the publication is found to be false.

Right to privacy is, thus, an intrinsic part of the right to life and personal liberty enshrined under Article 21 of the Constitution of India. However, the right to privacy in India is not an absolute right. It is subject to number of restrictions like by procedure established by law wherein the procedure would have to be just, fair and reasonable; if it is in the interest of the sovereignty and integrity of India; in case if there is an important countervailing interest which is superior; in states interest; not available to persons who voluntarily thrusts her/himself into controversy; and if it's against the interest of private citizens.

Coming to the protection of data. Let us first define what do we understand by the term 'data'? Section 2(1)(o) of the Information Technology Act 2000defines "data." It provides us in fact the process of data collection which can be laid down as follows –

It says data is -

(a) a representation of information, knowledge, facts, concepts or instructions;
(b) which are being prepared; or
(c) have been prepared in a formalized manner in a computer system or computer network.

It also further provides that such data may be presented in any forms such as computer printouts, magnetic or optical storage media, punched cards, or punched tapes) and can also be stored internally in the memory of the computer.

With the digital drive in India, extensive use of internet and various applications in the devices for various purposes, there has been increase in the amount of data generated. There is no denying the fact that the data generation has been advantages to the people and has increased the efficiency of people as well as the development of the society. However, the data generated is not protected and often get misused which results in the infringement of right to privacy of an individual. This issue was recently raised before the Supreme Court in the case of K.S.Puttaswamy (Retd.) v. Union of India.[8] The case was brought by retired

[8](2015) 8 SCC 735.

High Court Judge Puttaswamyin 2012 wherein he challenged the constitutional validity of the "Aadhaar Card Scheme" of the UPA Government which required the people to submit their biometric data for the identity card which would be mandatory for access to government services and benefits. It was contended that the Aadhar Card Scheme infringes the rights of the people. It was brought before a Bench of three judges which passed an order that a Bench of appropriate strength must examine the said case and also to examine the correctness of the decisions of the Court in M.P. Sharma v. Satish Chandra, District Magistrate, Delhi[9] and Kharak Singh v. State of Uttar Pradesh.[10]This matter was first placed before a 5 Judge Bench but subsequently, the matter was referred to a 9 Judge Bench on 18th July 2017. The Supreme Court in its unanimous decision held that the Constitution guaranteed the right to privacy as an intrinsic part of the right to life and personal liberty under Article 21. Thus, right to privacy may give rise to two inter-related protections i.e. against the world at large (right to choose that what personal information is to be released into the public space) and against the state (necessary concomitant of democratic values, limited government and limitation on power of State). The nine judge bench in Justice K.S. Puttaswamy (Retd) v. Union of India[11]decided over the matter whether the "Aadhar Card Scheme" which is the scheme introduced by the UPA Government of India wherein collecting and compiling the demographic and biometric data of the residents of this country is to be used for various purposes is violative of the "right to privacy"?

While discussing the right to information and privacy in today's world the Hon'ble Mr. Justice D.Y. Chandrachud placed his opinion on "informational privacy." According to him in this informational age right to privacy of a person is at stake not only at the hands of the state but also from some non-state actors. Thus, he recommends that before such application the Union Government should examine and put into place a robust regime for data protection wherein a striking balance between the individual interests and legitimate concerns of the state is made. He also said that in order to achieve such balance it is necessary that the Union Government while designing such scheme should also consider the legitimate aims of the states which may include protecting the national

[9]AIR 1954 SC 300.
[10]AIR 1963 SC 1295.
[11](2017) 10 SCC 1.

security, prevention and investigating crimes, national security etc. In this case, all the nine judges unanimously observed that 'right to privacy' is protected under Article 21 of the Constitution of India and the 'Aadhaar Card Scheme' without any robust regime for data protection does infringe this right of the citizens. Although this right protected under Article 21 is not absolute and must meet its threefold requirement of (i) legality; (ii) the need for a legitimate aim; and (iii) proportionality.

III. Data Mining and Misuse of Collected Data

Data mining is the process through which the raw data is collected and useful information from that data is extracted for use. Thus, we can say that it is the process through which usable data is extracted from the raw data. In this age of internet every single activity of any individual can result in the data generation. The e-commerce has made it possible to collect, organize and process the personal information of any individual. There are many sources through which data can be collected which are as follows: -

(a) the marketing and the retail companies which collect the data of its customers which can later be used for targeting customers for particular purposes/marketing, predict the new marketing campaigns, helps in identify the customer response, helps in implementing the profit making policies for the growth of the business, to understand the behavior and habits of their customers;

(b) the finance or banking companies collect the data from their customers which helps the financial institutions with information about the loan information and credit reporting, it helps them in determining the good and bad loans, helps bank to detect fraudulent credit card transactions or debit card transactions, and also helps us in understanding the purchases, exchanges, banking, stock etc;

(c) the Government agencies/departments too are collecting information from people who are filling up forms for job interviews in government department. This helps the government agencies to build pattern and gain information about the money laundering and other aspects of forgery by the government officials/servants;

(d) the data collected by the medical fields too helps us in understanding the effects of certain epidemic in any place, in knowing the views of the patients, in implementing advanced treatment methodology, improve the communication between doctor and the patient, and the most important of all is to enhance health facilities;

(e) the data is collected through surveillance videos and pictures too for the purpose of safety of people or a particular locality by tracking the movement of people in the said locality and observing the pattern of their day to day life; it also helps the law enforcers to prevent any crime;

(f) the data is also collected through online games in computers, tablets or phones. The gaming sites collects the personal data of the consumers and use the data in knowing what the gamer wants. The online gaming makes it possible for even the strangers to exchange information about each other.

(g) the digital medias like digital camera, scanner, desktop video cameras as well as the video chatting too helps in collecting the personal data of the person who is using those;

(h) the personal data of an individual is also collected from social media like Facebook, twitter, WhatsApp etc. The individual himself provide the information in the social media.

However, there is no doubt that the information collected has been helpful in developing a nation as well as made our life easy. The information are available at our hands with the help of all the necessary information's stored in our devices and all the documents which are almost linked with each other. But it cannot be denied too that such data extractions like address, account details via KYC, phone number, workplace etc. through various applications as well as self-posts in social media and status of WhatsApp and other such applications has been also pitfall in data mining and imposes dangers to the person these data belong. The streaming of data is so much that it is practically impossible to have control over its collection, distribution, use and misuse. These collected data can be used for beneficial purposes but the unregulated and arbitrary use of such data can raise grave concern regarding the protection of privacy and individual's security. The people's information can be hacked by the hackers like the bank details, address and other personal information and can be used by criminal

organizations or criminal minded persons with criminal motive as well as the marketing companies. With the expansion of social networks, e-commerce, forms, blogs and other such things the personal information is collected and can be used in an unethical way which can result in violation of the privacy of a person along with lack of safety and security. Generally, the personal information collected by the business companies can be sold or leaked. This imposes the lack of safety and security as the information can be misused.

IV. Data Protection and Laws in India

With the explosion in the internet and data generation through various means due to it, India is facing problems relating to various kinds of cyber-crime. Matters relating to credit card/debit card theft, identity theft, money laundering, infringement of privacy, fraud, etc.Till now there is no specific law in India which deals with data protection and right to privacy of an individual. However, we cannot say that there is no law to protect citizens from it. There are few legislations which mitigate against private concerns and national security concern and to some extent deal with the problem regarding the data protection.

"Right to privacy" is protected under Article 21 of the Constitution along with reasonable restriction for the right for the freedom of speech and expression provided under Article 19(1)(a). However, it has to be admitted that currently India does not have any specific law which deals with the issues of data protection. In the absence of any specific laws on data protection we rely on the Information Technology Act 2000 and the Indian Contract Act 1872 for the same.

The Information Technology Act 2000 under Section 43A provides compensation for failure to protect data. The sole objective of this provision is to protect the personal data and privacy. It provides rights to compensation to any person from a body corporate who possess, deals or handles sensitive data or information which are stored in computers or other such means and have caused infringement to the persons whose data and information they are holding by being negligent or not maintaining reasonable security practices and procedures. The Explanation (ii) to Section 43A provides that for the purpose of this provision "*reasonable security practices and procedures*" means security practices and procedures which were designed to protect such data and

information from unauthorized access, damage, use, modification, disclosure or impairment, as part of the agreement enforceable between the parties or which are specified in the laws which are time being in force. In the absence of any specific agreement it should be as per the security practices and procedures which are prescribed by the Central Government.

Explanation (iii) to Section 43A provides the meaning of "*sensitive personal data or information*" as such personal information which are prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal data or Information) Rules, 2011 provides what are included under the "sensitive personal data or information"? It provides that the sensitive personal data or information of a person which means things like password; information regarding Bank accounts or credit cards or debit cards; health condition which includes physical, physiological and mental health; sexual orientation of a person; biometric information; medical records; or any details provided to a body corporate.[12]However, it also provides that wherein any information is available freely and is accessible in public domain or is furnished under the Right to Information Act, 2005 or any other law for the time being in force then those information or data will not be regarded as sensitive personal data or information.

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal data or Information) Rules, 2011 also provides that the body corporate which collects, receives, possess, stores, deals or handle information of provider of information is under a duty to provide a privacy policy for handling of or dealing in personal information including sensitive personal data or information. In its policy a body corporate should also ensure that the information and data provided by the people should be available for them to view under lawful contract. Such policy shall be published by the body corporate in their websites. The said policy shall be clear and should state its practices and policies clearly which is easily accessible by the persons who will be furnishing their details. It should also consist of the type of personal and

[12]Rule 3, The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal data or Information) Rules, 2011

sensitive data which are collected; the purpose of collection and usage of such information; disclosure of information including sensitive personal data or information as provided in Rule 6 and reasonable security practices and procedures as provided under Rule 8.[13] Rule 6 of the The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal data or Information) Rules, 2011 provides that sensitive personal data or information can be done by a body corporate to any third party only with prior permission from the provider of such information. The Information Technology Act, 2000 also provides punishment for disclose of information in breach of lawful contract with imprisonment for a term which may extend to three years, or with fine which may extend to Rs.5 lakh, or with both.[14]

Apart from the above legislation, measures are taken by the Telecommunication Companies. Lots of data is collected by the telecommunication companies too by way of getting phone connection, buying sim card for mobile phones, conversations, phone tapping etc. For all these matter the Telecommunication industries are governed by the Indian Telegraph Act 1885 which allows the Government to take possession of licensed telegraphs and intercept messages in case of any public emergency for the purpose of public safety and in the interest of the sovereignty and integrity of India. TRAI too controls the telecom and internet services (TSPs) in India and requires all of them to ensure compliance of the terms and conditions of the license regarding the confidentiality of information of subscribers and privacy of communications. Recently, in Karmanya Singh Sareen v. Union Of India[15]matter relating to WhatsApp user's 'right to privacy' came into question. WhatsApp is being used by the people for communicating with their dear and near ones and more preferred over the other Apps because of its privacy policy. On 19th February 2014 Facebook announce to have acquired ownership over WhatsApp. On 26th August 2016 WhatsApp announced changes in privacy policy which included that the account information of users including their phone number and contact details will be shared with the Facebook which is more public platform than the WhatsApp. The said new privacy policy will come into effect after 25th September 2016.

[13]Rule 4, The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal data or Information) Rules, 2011
[14]Section 72A, The Information Technology Act, 2000
[15]233 (2016) DLT 436

This new privacy policy was challenged by Karmanya Singh and Shreya Sethi who filed a writ petition in the Delhi High Court. In their petition they contended that when WhatsApp was introduced in 2010 they had declared a privacy policy wherein they promised complete safety against sharing of any details of the users along with complete security and protection of privacy to tis users. But the change in the privacy policy infringes the right to privacy of its users. However, the Delhi High Court gave partial relief to the petitioners by stating that the information, data and details of non-existing members as on 25th September 2016 shall be deleted and will not be shared. Thus, it left a choice upon the users whether to continue using the said App or not. Aggrieved by the decision of the Delhi High Court the petitioners filed a Special Leave Petition at the Supreme Court on 17th December 2016.[16]The main issues which are raised in this Special Leave Petition are: -

(a) whether the change in the privacy policy of WhatsApp after 25th September 2016 violates the 'right to privacy' of its users?
(b) Whether the internet messaging services through which users exchange messages via text, audio, video, calls/video calls constitute "Telecommunication" services? And whether the same can be regulated by the relevant telecommunication authorities or not?
(c) Whether WhatsApp can provide an option to the users 'not to share' data with Facebook?
(d) There are many users in our country who cannot read/understand the terms of the privacy policy provided by the App. Hence, the manner of seeking consent who are unable to read or understand the terms amounts to misleading, deceptive and unlawful?

At present the case is pending before the Hon'ble Supreme Court.

With respect to data protection and right to privacy in the Banking sectors we have certain laws like the Credit Information Companies Regulations 2006; Circulars of RBI including KYC circulars; Master Circulars on Credit Cards etc.; Master Circulars on Customer Services; Code of Banks Commitment to

[16]SLP (C) 804/2017

customers. In the field of Medicine and Health care Sector there are laws like the Clinical establishments (Central Govt) Rules 2012; Indian Medical Council (Professional Conduct, Etiquette, and Ethics) Regulation 2002 which speaks for data protection and right to privacy. Date protection law should be equally applicable on the public and private sector. Government offices also hold personal information.

V. The Personal Data Protection Bill in India

Although in India the legislations do exists for the purpose of data protection but the complexity, dynamism and all-encompassing reach of the digital revolution requires a far more comprehensive regulatory regime to mitigate the concerns that are ever present. Thus, the Government of India constituted a Committee consisting of 10 members which was chaired by Supreme Court Judge B.N. Srikrishna(Retd) in August 2017 by the Ministry of Electronics and Information Technology to design and draft data protection laws for India. The Committee after a year of deliberations and public consultations has released a draft bill titled "The Personal Data Protection Bill, 2018." This Bill contains provisions regarding the processing and collection of personal data and information of individuals by government and private entities incorporated in India and abroad. Along with it the Bill also contains provision for the protection of processing personal data of children such as age verification, parental consent etc. The bill also speaks about appointment of Data Protection Officers for carrying out functions like ensuring compliance to this Act, monitoring data processing activities, establishing grievance redressal of data principals. It also contains provision for transfer of data outside the country. It can be done only after meeting certain conditions. The Bill also has certain exemptions wherein data protection is not available. It also speaks about the establishment of Data Protection Authority of India (DPAI)by the Central Government and its power. It makes the following as an offense:-

- Obtaining, transferring or selling of personal data as well as sensitive personal data contrary to the Act;
- Re-identification and processing of de-identified personal data;
- It provides for special procedures to deal with Offences by Companies, Central or State Governments.

The Personal Data Protection Bill, 2019 with few changes was introduced in Parliament on 11th December 2019. The Bill has been referred to a Joint Parliamentary Committee to examine it and submit its report. The essence of the Bill 2019 is to provide protection of personal data of the individuals and establish a Data Protection Authority. However, it does differ from the Draft Bill 2018 on the following grounds: -

(i) With respect to the definition of "Personal data" the Bill 2019 retains the definition provided under the Draft Bill 2018.

(ii) Unlike the Draft Bill 2018, the Bill of 2019 removes 'passwords' from the term of sensitive personal data. It also provided power to the Central Government (in consultation with the Data Protection Authority) to categorize any personal data as sensitive personal data. As per the Draft Bill 2018 this power was vested on the Data Protection Authority.

(iii) Wherein the rights of the individual (data principal) is concerned the Draft Bill 2018 provided that rights such as obtaining confirmation on whether their data has been processed, seeking correction, transfer or restriction on continuing disclosure of their data vested on the data principal. The Bill 2019 has added one more right to the rights of the individual i.e. right to erase the personal data.

(iv) As per the Draft Bill 2018 the personal data can be processed without obtaining the consent of the individual on certain grounds which includes functions of Parliament or State legislatures, wherein the individual will benefit out of such steps by the state and for any reasonable purposes specified by the authority to detect fraud, for recovery of the debt etc., however, the Bill 2019 removes the provision on functions of Parliament or State legislatures for non-consensual processing of personal data. The Bill 2019 provides that the Authority may allow 'operation of search engines' as a reasonable purpose for which non-consensual processing of personal data.

(v) The Bill 2019 provides definition for 'social media intermediary' which enables online interaction between the users and allows them to share information. Thus, we find that social media intermediary

is a significant data fiduciaries and must provide a voluntary user verification mechanism for all users in India. The Draft Bill 2018 does not mention this at all.

(vi) Although we know that the data are collected by the Government agencies also but they were exempted from the provisions by the Draft Bill 2018. However the Bill 2019 do bring them within the purview of the provisions but provide certain reasonable reasons wherein they are exempted like if it concerns the national integrity of the nation or for preventing incitement to commission of any cognisable offence.

(vii) Small entities were also kept outside the purview of the provisions under the Draft Bill 2018. The Bill 2019 do retain the exemption but has proviso to it that if the Authority thinks that their annual turnover has exceeded the prescribed limit then they can be brought under the purview of the provisions.

(viii) As per the Draft Bill 2018 it was provided that with respect to the transfer of personal data outside the country one serving copy of all personal data will be kept in India. The Bill 2019 has removed the mandatory storage of all personal data and provides that only sensitive personal data should be stored.

(ix) With respect to the composition of the Data Protection Authority of India, Bill 2019 has changed its composition of selection Committee of the Data Protection Authority of India.

(x) Under the Draft Bill 2018 offences like obtaining, disclosing, transferring or selling personal data in contravention of the Act; re-identification and processing of de-identified personal data without consent are punishable with imprisonment. However, under the Bill 2019 only the re-identification and processing of de-identified personal without consent if punishable with imprisonment.

(xi) With respect to the use of non-personal data collected by the Government for formulation of policies for digital economy, growth and security the Draft Bill 2018 states that no provisions will apply. The Bill 2019 retains it but further provides that the Government may direct the data fiduciaries to provide them non-personal data and anonymised personal data for the purpose of better targeting of the services and formulation of evidence-based policy.

VI. Conclusion

With the digitalization and processing of data in almost every sphere it is difficult to safeguard one's personal data which might land into wrong hands it becomes essential to revamp the existing laws as well as enact the law for protecting the personal data at the earliest. Enacting laws will not be sufficient until and unless effective machinery is not there to protect the rights of the individuals, thus, it becomes essential to have Special courts to deal with the problems relating to the data protection and other intellectual property right other than the Data Protection Authority which both the Bill of 2019 speak of. Data protection and right to privacy goes hand in hand and despite being a significant right of an individual with reasonable restrictions right to privacy still covered under the concept of right to life and personal dignity under Article 21. Hence, there is a need for Constitutional amendment to make right to privacy as separate provision for the protection of individual rights. Incorporation of comprehensive policy is essential which shall consist of EU's General Data Protection Information Technology principles so that several agencies which are performing cyber security operations in India such as the National Technical Research Organization, the National Intelligence Grid and the National Information Board perform their duties properly. Apart from all these it is essential that we as an individual while interacting in the digital sphere be fully cautious especially where personal details are to be put, so that we may not be the victims of various kinds of cyber threats, frauds and theft of our personal data and information.